Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

O Teorema de Nichols-Zöeller

Dissertação de Mestrado

LEONARDO DUARTE SILVA

Porto Alegre, 31 de Março de 2016

Dissertação submetida por Leonardo Duarte Silva[1] , como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professora Orientadora:
Profª. Dra. Bárbara Seelig Pogorelsky

Banca examinadora:
Prof. Dr. Antonio Paques (IM - UFRGS)
Prof. Dr. Wagner de Oliveira Cortes (IM - UFRGS)
Profª. Dra. Carolina Noele Renz (UNISINOS)
Profª. Dra. Bárbara Seelig Pogorelsky (IM - UFRGS, ORIENTADORA)

[1]Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)

Agradecimentos

Agradeço aos meus pais Miguelina e Geraldo, ao meu irmão Lucas, à minha namorada Juliana e também à sua família, por todo incentivo e carinho que sempre recebi, bem como compreensão e paciência em alguns momentos. O apoio de vocês é essencial para mim.

Ao meu amigo Everton, o irmão que adotei.

Aos meus amigos e colegas da pós-graduação, pelos momentos dentro e fora da universidade. Em especial à Grasi e à Dani, que contribuíram muito na construção desta dissertação.

À minha orientadora Bárbara, por ter me aceitado como orientando, dado liberdade em meus estudos e acreditado em minha capacidade. Espero ter retribuído sua confiança e que este trabalho lhe tenha sido tão satisfatório quanto foi a mim.

Aos amigos e professores da UFPel, que sempre acreditaram em mim, deram todo suporte e oportunidade para iniciar esta etapa. Em especial aos professores: Alexandre Athayde, Alexandre Molter, Cícero, Janice, Lisandra e meu orientador Giovanni.

Ao professor Paques pela sugestão desta dissertação e também por aceitar me orientar no doutorado.

Aos professores e funcionários do Programa de Pós-Graduação em Matemática da UFRGS, pela oportunidade. E à CAPES pelo apoio financeiro.

Agradeço também aos professores que aceitaram participar da banca.

Resumo

Este trabalho tem por objetivo estudar todos os pré-requisitos e demonstrar o Teorema de Nichols-Zöeller. Para isso é realizado um estudo preliminar em tópicos selecionados da Teoria de Anéis e Módulos, visando o Teorema de Krull-Schmidt, e também da Teoria de Álgebras de Hopf, principalmente os resultados para dimensão finita.

Abstract

The purpose of this work is to study all prerequisites and to prove the Nichols-Zöeller Theorem. For this we conducted a preliminary study on selected topics of Module and Ring Theory, aiming at the Krull-Schmidt Theorem, and also Hopf Algebras Theory, specially results for finite-dimensional case.

Índice

Introdução

Em 1975, Irving Kaplansky [5] listou 10 conjecturas em álgebras de Hopf. Desde então, a busca de respostas para estas conjecturas foi um grande foco de pesquisa na área. A primeira destas conjecturas trata da relação de uma álgebra de Hopf e suas subálgebras de Hopf. Já era sabido que toda álgebra de Hopf é um módulo sobre qualquer uma de suas subálgebras de Hopf. Contudo, não se sabia quando uma álgebra de Hopf era livre sobre suas subálgebras de Hopf. Assim, a primeira conjectura de Kaplansky foi que "toda álgebra de Hopf H é livre como um B-módulo, para qualquer subálgebra de Hopf B de H". Rapidamente Oberst e Schneider em [14] mostraram um contra-exemplo e a conjectura se mostrou falsa, ao menos no caso de uma álgebra de Hopf de dimensão infinita. O caso finito, entretanto, permaneceu aberto por 14 anos. Em 1985, Martha Bettina Zöeller, sob orientação de Warren Nichols, mostrou em sua tese de doutorado que o resultado era verdadeiro quando B é uma álgebra de grupo semissimples. Resultado este publicado posteriormente em [20]. No artigo subsequente de Nichols e Zöeller [13] foi mostrado, utilizando métodos mais técnicos, que o resultado era válido quando B era uma álgebra de grupo qualquer. Finalmente, em 1989 no artigo [12], Nichols e Zöeller mostraram, utilizando técnicas ainda mais sofisticadas, o resultado mais geral, o caso em que H é uma álgebra de Hopf de dimensão finita qualquer, assegurando então que a conjectura de Kaplansky é verdadeira no caso em que a álgebra de Hopf H tem dimensão finita.

O principal teorema do artigo [12] é hoje em dia conhecido como "Teorema de Nichols-Zöeller", e afirma então que toda álgebra de Hopf H de dimensão finita é livre como B-módulo para qualquer subálgebra de Hopf B de H. Este teorema foi muito importante para o desenvolvimento da pesquisa em álgebras de Hopf, sendo por exemplo, um resultado fundamental para o estudo de classificação de álgebras de Hopf.

Uma consequência imediata interessantíssima do referido teorema é que ele generaliza para o caso de álgebras de Hopf o famoso Teorema de Lagrange para grupos finitos. Sabemos que os grupos se generalizam naturalmente para álgebras de Hopf, já que para um grupo G, a álgebra de grupo $\Bbbk G$ é uma álgebra de Hopf, e para cada H subgrupo de G, $\Bbbk H$ é subálgebra de Hopf de $\Bbbk G$. Dado um grupo finito G e H um subgrupo de G, o Teorema de Nichols-Zöeller afirma então que $\Bbbk G$ é livre como

$\Bbbk H$-módulo, e disto segue que $\dim_{\Bbbk}(\Bbbk H) | \dim_{\Bbbk}(\Bbbk G)$, e já que $\dim_{\Bbbk}(\Bbbk H) = |H|$ e $\dim_{\Bbbk}(\Bbbk G) = |G|$, segue que $|H| \Big| |G|$.

Neste trabalho iremos provar o Teorema de Nichols-Zöeller, tendo como principal referência o artigo [12]. Nesta demonstração, o Teorema de Krull-Schmidt, que é um teorema clássico da Teoria de Anéis e Módulos, tem uma importância fundamental. Por conta disso, colocamos como apêndice um estudo completo deste teorema, com todos seus detalhes, seguindo principalmente a referência [6]. Devido a este resultado ser um clássico, outras referências fazem a construção do mesmo, seguindo outros caminhos. Por conta disso, em alguns momentos foi interessante fazer a abordagem de resultados preliminares conforme outras referências, tais como [10], [4] e [2].

O primeiro capítulo desta dissertação é dedicado às álgebras de Hopf, e se estende quase que linearmente até chegarmos ao fato que toda álgebra de Hopf de dimensão finita H é injetiva como um H-módulo. O motivo de nos estendermos até este resultado é que ele, juntamente com o Teorema de Krull-Schmidt, são fundamentais para o entendimento dos resultados desenvolvidos por Nichols e Zöeller em [12]. Na primeira seção deste capítulo, apresentamos a definição e resultados básicos sobre a estrutura de álgebras de Hopf, e apresentamos brevemente a dualidade entre álgebras e coálgebras. Na segunda seção, construímos os módulos de Hopf e nos estendemos até o Teorema Fundamental dos Módulos de Hopf que será importante na seção seguinte. Na terceira seção, fazemos um breve estudo sobre as integrais de uma álgebra de Hopf, culminando no Teorema de Larson-Sweedler. Este importante teorema afirma que a antípoda de uma álgebra de Hopf de dimensão finita é bijetora, e além disso o espaço das integrais tem dimensão 1 sobre $\Bbbk$. Como consequência dele, provamos que quando H é uma álgebra de Hopf de dimensão finita, então H e H^* são isomorfos como H-módulos. Na quarta e última seção do capítulo 1, resgatamos um pouco a teoria clássica de módulos, visando principalmente resultados sobre módulos injetivos. Boas referências para a Teoria de Álgebras de Hopf são [3], [18], [1] e [11].

O segundo e principal capítulo desta dissertação trata dos resultados desenvolvidos por Nichols e Zöeller no artigo [12]. Optamos por dividí-lo em duas seções, apresentando na primeira seção alguns resultados preliminares e na seção seguinte culminando no Teorema de Nichols-Zöeller.

Por fim, é importante salientar que esta dissertação tem o intuito de ser auto-suficiente, na medida em que tentamos adotar um caminho linear para a prova do Teorema de Nichols-Zöeller, onde todos resultados preliminares são devidamente provados. Porém, devido ao conteúdo desenvolvido, exigimos do leitor um conhecimento básico sobre a Teoria de Anéis e Módulos. Por conta disso, nos permitimos definir aplicações cujo domínio é um produto tensorial, simplesmente indicando a lei da função em seus geradores, e admitimos sua boa definição, desde que a verificação disto é um simples cálculo, onde se faz uso da Propriedade Universal que caracteriza os produtos tensoriais.

Capítulo 1

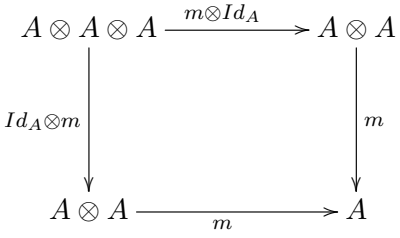
Álgebras e Módulos de Hopf

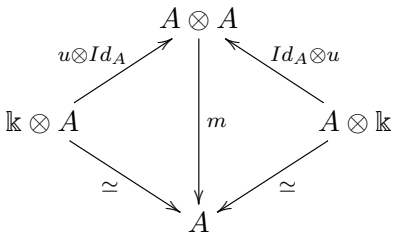
Neste capítulo damos as definições básicas sobre álgebras de Hopf, bem como algumas propriedades importantes. Além disso, desenvolvemos a teoria até chegarmos a um resultado importante sobre álgebras de Hopf de dimensão finita, a saber, que toda álgebra de Hopf de dimensão finita H é injetiva como um H-módulo.

1.1 Álgebras de Hopf

Notação 1.1.1. *Ao longo de todo este trabalho, $\Bbbk$ denotará um corpo qualquer, fixado. Se V, W são dois $\Bbbk$-espaços vetoriais, denotamos o produto tensorial de V e W sobre $\Bbbk$, $V \otimes_{\Bbbk} W$, simplesmente por $V \otimes W$. Além disso, chamamos de* twist *a seguinte aplicação $\tau : V \otimes W \longrightarrow W \otimes V$ dada por $\tau(a \otimes b) = b \otimes a$, que é um isomorfismo.*

Definição 1.1.2. *Uma* álgebra sobre um corpo $\Bbbk$*, ou simplesmente uma $\Bbbk$-álgebra, é um $\Bbbk$-espaço vetorial A munido de duas aplicações $\Bbbk$-lineares, multiplicação $m : A \otimes A \longrightarrow A$ e unidade $u : \Bbbk \longrightarrow A$, tais que os seguintes diagramas são comutativos:*





Em outras palavras, o primeiro diagrama nos dá a relação

$$m \circ (m \otimes Id_A) = m \circ (Id_A \otimes m)$$

e o segundo diagrama

$$[m \circ (u \otimes Id_A)](1_{\Bbbk} \otimes a) = a = [m \circ (Id_A \otimes u)](a \otimes 1_{\Bbbk}),\ \forall a \in A.$$

Notação 1.1.3. *Denotemos a imagem de um elemento $a \otimes b \in A \otimes A$ pela aplicação m simplesmente por $m(a \otimes b) := ab$. A imagem de $1_{\Bbbk}$ via a aplicação u será denotada por $u(1_{\Bbbk}) = 1_A$.*

Em alguns contextos, esta definição de álgebra é também chamada de *álgebra associativa e unitária*, visto que essas são as duas propriedades que são garantidas pelos diagramas da definição.

Notemos primeiro que, pelo segundo diagrama, 1_A é realmente a unidade em A, isto é, 1_A satisfaz $1_A a = a = a1_A$, para todo $a \in A$. De fato, o lado esquerdo do segundo diagrama garante que $[m \circ (u \otimes Id_A)](1_{\Bbbk} \otimes a) = a$, mas $[m \circ (u \otimes Id_A)](1_{\Bbbk} \otimes a) = m(u(1_{\Bbbk}) \otimes a) = m(1_A \otimes a) = 1_A a$. Assim, $a = 1_A a$. Analogamente, o lado direito nos garante que $a = a1_A$.

Além disso, vejamos que o primeiro diagrama se traduz como a associatividade do produto. Visto que $m \circ (m \otimes Id_A) = m \circ (Id_A \otimes m)$, então para qualquer $a \otimes b \otimes c \in A \otimes A \otimes A$, temos que valem as seguintes igualdades:

$$\begin{aligned}
[m \circ (m \otimes Id_A)](a \otimes b \otimes c) &= [m \circ (Id_A \otimes m)](a \otimes b \otimes c) \\
m([m \otimes Id_A](a \otimes b \otimes c)) &= m([Id_A \otimes m](a \otimes b \otimes c)) \\
m(m(a \otimes b) \otimes Id_A(c)) &= m(Id_A(a) \otimes m(b \otimes c)) \\
m(ab \otimes c) &= m(a \otimes bc) \\
(ab)c &= a(bc)
\end{aligned}$$

Vejamos agora que se $A \neq \{0\}$, então a aplicação u é injetora. De fato, sejam $\alpha, \beta \in \Bbbk$ tais que $u(\alpha) = u(\beta)$. Do fato que u é $\Bbbk$-linear, temos $\alpha \cdot u(1_{\Bbbk}) = \beta \cdot u(1_{\Bbbk})$, ou seja, $\alpha \cdot 1_A = \beta \cdot 1_A$, e portanto $(\alpha - \beta) \cdot 1_A = 0_A$. Note que $(\alpha - \beta) \in \Bbbk$ e $1_A = u(1_{\Bbbk}) \in A$. Como A é um $\Bbbk$-espaço vetorial, $\alpha - \beta = 0_{\Bbbk}$ ou $u(1_{\Bbbk}) = 1_A = 0_A$. Vimos na observação anterior que $a = 1_A a$, $\forall a \in A$, assim, se $1_A = 0_A$, temos que $a = 1_A a = 0_A a = 0_A$, para todo $a \in A$, ou seja, $A = \{0\}$, o que é um absurdo. Logo $\alpha - \beta = 0_{\Bbbk}$ e portanto $\alpha = \beta$, donde segue que u é injetora.

Assim, temos que a aplicação u nos permite ver $\Bbbk$ dentro de A, isto é, para $\alpha \in \Bbbk$, podemos escrever $\alpha \in A$, via a aplicação injetora u. Quando $\alpha \in \Bbbk$ e escrevermos $\alpha \in A$, entendemos que estamos considerando $\alpha := u(\alpha) = \alpha \cdot u(1_{\Bbbk}) = \alpha \cdot 1_A \in A$.

Além disso, do segundo diagrama temos a compatibilidade entre a ação de $\Bbbk$ em A e o produto dos elementos de $u(\Bbbk)$ com um elemento qualquer de A. Em outras palavras, para $\alpha \in \Bbbk$ e $a \in A$, temos que $\alpha \cdot a = (\alpha \cdot 1_A)a = a(\alpha \cdot 1_A)$, onde denotamos a ação do escalar $\alpha \in \Bbbk$ em um elemento a do $\Bbbk$-espaço vetorial A por $\alpha \cdot a$. De fato, pelo primeiro lado do segundo diagrama, temos que para quaisquer $\alpha \in \Bbbk$ e $a \in A$, temos que $[m \circ (u \otimes Id_A)](\alpha \otimes a) = \alpha \cdot a$, já que $\alpha \otimes a = 1_{\Bbbk} \otimes \alpha \cdot a$. Mas note que $[m \circ (u \otimes Id_A)](\alpha \otimes a) = m(u(\alpha) \otimes a) = m((\alpha \cdot u(1_{\Bbbk})) \otimes a) = m((\alpha \cdot 1_A) \otimes a) = (\alpha \cdot 1_A)a$. Ou seja, $\alpha \cdot a = (\alpha \cdot 1_A)a$. Utilizando o outro lado do diagrama, concluímos que $\alpha \cdot a = a(\alpha \cdot 1_A)$.

Com isso, escreveremos indistintamente αa para significar tanto $\alpha \cdot a$ quanto $a(\alpha \cdot 1_A)$ ou $(\alpha \cdot 1_A)a$.

A seguir, vamos começar a construção de um importante exemplo ao longo de toda dissertação, a saber, a álgebra de grupo.

Exemplo 1.1.4. *Seja G um grupo com elemento neutro e, e considere as somas formais*

$$\Bbbk G = \left\{ \sum_{i=1}^{n} \alpha_i g_i | \alpha_i \in \Bbbk, g_i \in G, n = 1, 2, ... \right\}.$$

Para um elemento $g \in G$, escrevemos também $g \in \Bbbk G$ para significar $1_\Bbbk g$. Assim, definimos $m : \Bbbk G \otimes \Bbbk G \longrightarrow \Bbbk G$ por $m(g \otimes h) = gh$ e $u : \Bbbk \longrightarrow \Bbbk G$ por $u(1_\Bbbk) = e$ e estendidas linearmenente.

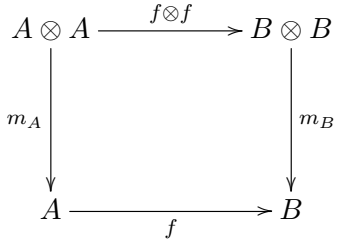
Em outras palavras, $\Bbbk G$ é o $\Bbbk$-espaço vetorial com base indexada por elementos de um grupo G, com a multiplicação dada pela operação do grupo e a unidade é o próprio neutro do grupo. Além disso, é claro que $\dim_\Bbbk(\Bbbk G) = |G|$.

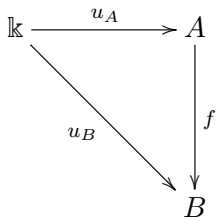
É de fácil constatação que as aplicações m e u acima definidas satisfazem os diagramas, tornando $\Bbbk G$ uma $\Bbbk$-álgebra.

É uma simples verificação que se (A, m_A, u_A) e (B, m_B, u_B) são duas $\Bbbk$-álgebras, então $A \otimes B$ também é uma $\Bbbk$-álgebra com multiplicação dada por $m_{A\otimes B} = (m_A \otimes m_B) \circ (Id_A \otimes \tau \otimes Id_B)$ e unidade dada por $u_{A\otimes B} = (u_A \otimes u_B) \circ \varphi$, onde $\tau : B \otimes A \longrightarrow A \otimes B$ é o isomorfismo *twist* dado por $\tau(a \otimes b) = b \otimes a$ e $\varphi : \Bbbk \longrightarrow \Bbbk \otimes \Bbbk$ é o isomorfismo canônico dado por $\varphi(1_\Bbbk) = 1_\Bbbk \otimes 1_\Bbbk$.

Em termos de elementos, para quaisquer $a \otimes b, a' \otimes b' \in A \otimes B$, temos que $u_{A\otimes B}(1_\Bbbk) = 1_A \otimes 1_B$ e $m_{A\otimes B}((a \otimes b) \otimes (a' \otimes b')) = aa' \otimes bb'$.

Definição 1.1.5. *Sejam A e B duas álgebras com multiplicações m_A e m_B e unidades u_A e u_B, respectivamente. Uma aplicação $f : A \longrightarrow B$ é um* homomorfismo de álgebras *se os seguintes diagramas são comutativos:*





Assim, $f : A \longrightarrow B$ é um homomorfismo de álgebras se valem

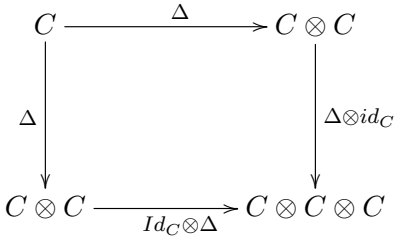
$$m_B \circ (f \otimes f) = f \circ m_A \qquad e \qquad f \circ u_A = u_B.$$

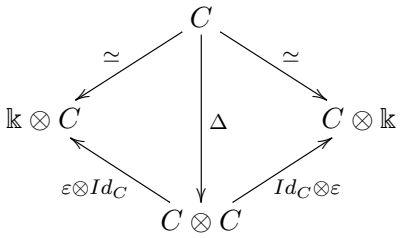
Em termos de elementos, temos que para quaisquer $a, b \in A$, valem

$$f(ab) = f(a)f(b) \quad e \quad f(1_A) = 1_B.$$

A definição de álgebra por diagramas como dada anteriormente, nos permite definir coálgebra de uma maneira intuitiva, sendo um $\Bbbk$-espaço vetorial com duas aplicações $\Bbbk$-lineares que satisfazem aos mesmos diagramas de uma álgebra, mas com as setas invertidas. Precisamente, temos:

Definição 1.1.6. *Uma* coálgebra sobre um corpo $\Bbbk$, *ou simplesmente uma coálgebra, é um* $\Bbbk$*-espaço vetorial* C *munido de duas aplicações* $\Bbbk$*-lineares, comultiplicação* $\Delta : C \longrightarrow C \otimes C$ *e counidade* $\varepsilon : C \longrightarrow \Bbbk$, *tais que os seguintes diagramas são comutativos:*





Em outras palavras, temos as relações:

$$(\Delta \otimes Id_C) \circ \Delta = (Id_C \otimes \Delta) \circ \Delta,$$

$$(\varepsilon \otimes Id_C)(\Delta(c)) = 1_{\Bbbk} \otimes c \quad e \quad (Id_C \otimes \varepsilon)(\Delta(c)) = c \otimes 1_{\Bbbk}, \, \forall c \in C.$$

Observação 1.1.7. *Observamos que a imagem de um elemento* $c \in C$ *pela aplicação* Δ *é da forma*

$$\Delta(c) = \sum_{i=1}^{n} c_{i_1} \otimes c_{i_2}, \quad onde \quad c_{i_1}, c_{i_2} \in C, i = 1, ..., n.$$

Notação 1.1.8. ***(Notação de Sweedler)*** *Para denotar a imagem de um elemento* $c \in C$ *pela aplicação* Δ, *usaremos a seguinte e já bem conhecida notação, chamada de* notação de Sweedler *ou* notação sigma*:*

$$\Delta(c) = \sum_{i=1}^{n} c_{i_1} \otimes c_{i_2} := c_1 \otimes c_2$$

Algumas vezes, também manteremos o símbolo de somatório, isto é, denotaremos

$$\Delta(c) = \sum_{i=1}^{n} c_{i_1} \otimes c_{i_2} := \sum c_1 \otimes c_2$$

Traduzindo os diagramas em termos de elementos, e utilizando a notação de Sweedler, temos que para todo elemento c em uma coálgebra C, vale pelo primeiro diagrama que

$$\begin{aligned}
[(\Delta \otimes Id_C) \circ \Delta](c) &= [(Id_C \otimes \Delta) \circ \Delta](c) \\
[\Delta \otimes Id_C](\Delta(c)) &= [Id_C \otimes \Delta](\Delta(c)) \\
[\Delta \otimes Id_C](c_1 \otimes c_2) &= [Id_C \otimes \Delta](c_1 \otimes c_2) \\
\Delta(c_1) \otimes Id_C(c_2) &= Id_C(c_1) \otimes \Delta(c_2) \\
(c_1)_1 \otimes (c_1)_2 \otimes c_2 &= c_1 \otimes (c_2)_1 \otimes (c_2)_2
\end{aligned}$$

Neste caso, estendemos nossa notação e denotamos por $c_1 \otimes c_2 \otimes c_3$ para significar tanto $(c_1)_1 \otimes (c_1)_2 \otimes c_2$ quanto $c_1 \otimes (c_2)_1 \otimes (c_2)_2$, já que são iguais.

Além disso, da segunda parte do segundo diagrama, temos que para um elemento qualquer $c \in C$, vale que $[(Id_C \otimes \varepsilon) \circ \Delta](c) = c \otimes 1_{\Bbbk}$. Como temos

$$[(Id_C \otimes \varepsilon) \circ \Delta](c) = [Id_C \otimes \varepsilon](\Delta(c)) = [Id_C \otimes \varepsilon](c_1 \otimes c_2) = Id_C(c_1) \otimes \varepsilon(c_2) = c_1 \otimes \varepsilon(c_2)$$

concluímos então que $c_1 \otimes \varepsilon(c_2) = c \otimes 1_{\Bbbk}$. Desde que $\varepsilon(c_2) \in \Bbbk$, e o produto tensorial está sobre $\Bbbk$, da última igualdade, obtemos que $c_1\varepsilon(c_2) \otimes 1_{\Bbbk} = c \otimes 1_{\Bbbk}$, ou seja $(c_1\varepsilon(c_2) \otimes 1_{\Bbbk}) - (c \otimes 1_{\Bbbk}) = 0$, e portanto $(c_1\varepsilon(c_2) - c) \otimes 1_{\Bbbk} = 0$. Agora, como $1_{\Bbbk} \neq 0$, obtemos que $c_1\varepsilon(c_2) - c = 0$, ou seja, $c_1\varepsilon(c_2) = c$.

Analogamente, a primeira parte do segundo diagrama nos dá que $\varepsilon(c_1)c_2 = c$. Lembremos apenas que $\varepsilon(c) \in \Bbbk$ para qualquer $c \in C$, e portanto pelo que vimos é indiferente escrever $c_1\varepsilon(c_2)$ ou $\varepsilon(c_2)c_1 = c$.

Vimos no Exemplo 1.1.4 que quando G é um grupo, $\Bbbk G$ é uma álgebra. Vamos dar agora a $\Bbbk G$ uma estrutura de coálgebra.

Exemplo 1.1.9. *Definimos em $\Bbbk G$ as aplicações $\Bbbk$-lineares comultiplicação $\Delta : \Bbbk G \longrightarrow \Bbbk G \otimes \Bbbk G$ dada por $\Delta(g) = g \otimes g$ e counidade $\varepsilon : \Bbbk G \longrightarrow \Bbbk$ dada por $\varepsilon(g) = 1_{\Bbbk}$, e estendidas linearmente.*

Também é de fácil verificação que com estas aplicações $\Bbbk G$ é uma coálgebra.

Também conseguimos a partir de duas coálgebras uma nova coálgebra.

Sejam $(C, \Delta_C, \varepsilon_C)$ e $(D, \Delta_D, \varepsilon_D)$ duas $\Bbbk$-coálgebras, então $C \otimes D$ também é uma $\Bbbk$-coálgebra com comultiplicação $\Delta_{C\otimes D} = (Id_C \otimes \tau' Id_D) \circ (\Delta_C \otimes \Delta_D)$ e com counidade $\varepsilon_{C\otimes D} = \varphi' \circ (\varepsilon_C \otimes \varepsilon_D)$, onde $\tau' : C \otimes D \longrightarrow D \otimes C$ é o isomorfismo *twist* dado por $\tau'(c \otimes d) = d \otimes c$ e $\varphi' : \Bbbk \otimes \Bbbk \longrightarrow \Bbbk$ é o isomorfismo canônico dado por $\varphi'(1_{\Bbbk} \otimes 1_{\Bbbk}) = 1_{\Bbbk}$.

Em termos de elementos, e utilizando a notação de Sweedler, para qualquer $c \in C, d \in D$, temos que $\Delta_{C\otimes D}(c \otimes d) = c_1 \otimes d_1 \otimes c_2 \otimes d_2$ e $\varepsilon_{C\otimes D}(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d)$, onde $\Delta_C(c) = c_1 \otimes c_2$ e $\Delta_D(d) = d_1 \otimes d_2$.

Antes de prosseguir, é interessante observar que assim como em uma álgebra, onde a associatividade se generaliza para uma quantidade finita de elementos, isto é, dada uma lista finita de multiplicações, podemos associar os elementos como quisermos, também em uma coálgebra existe essa noção, ao qual é chamada de *coassociativadade generalizada*. Em nosso estudo, precisaremos apenas de um caso particular desta propriedade mais geral, o qual enunciaremos como lema a seguir. Para o caso geral, o leitor interessado pode consultar qualquer referência indicada.

Lema 1.1.10. *Seja (C, Δ, ε) uma coálgebra. Então temos que*

$$(Id_C \otimes \Delta \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta = (\Delta \otimes Id_C \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta.$$

Demonstração. Sejam (C, Δ, ε) uma coálgebra e $x \in C$ um elemento qualquer. Notemos inicialmente que

$$(Id_C \otimes \Delta \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta = (Id_C \otimes [(\Delta \otimes Id_C) \circ \Delta]) \circ \Delta \tag{1.1}$$

De fato, temos que

$$\begin{aligned}[(Id_C \otimes \Delta \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta](x) &= [Id_C \otimes \Delta \otimes Id_C](x_1 \otimes (x_2)_1 \otimes (x_2)_2) = \\ &= x_1 \otimes ((x_2)_1)_1 \otimes ((x_2)_1)_2 \otimes (x_2)_2\end{aligned}$$

Por outro lado, temos

$$\begin{aligned}[(Id_C \otimes [(\Delta \otimes Id_C) \circ \Delta]) \circ \Delta](x) &= [Id_C \otimes ([\Delta \otimes Id_C] \circ \Delta)](x_1 \otimes x_2) = \\ &= x_1 \otimes ([\Delta \otimes Id_C]((x_2)_1 \otimes (x_2)_2) = \\ &= x_1 \otimes ((x_2)_1)_1 \otimes ((x_2)_1)_2 \otimes (x_2)_2\end{aligned}$$

Logo, vale a igualdade(1.1). Pela definição de coálgebra, temos que $(\Delta \otimes Id_C) \circ \Delta = (Id_C \otimes \Delta) \circ \Delta$, e com isso temos que $(Id_C \otimes [(\Delta \otimes Id_C) \circ \Delta]) \circ \Delta = (Id_C \otimes [(Id_C \otimes \Delta) \circ \Delta]) \circ \Delta$, donde concluímos que vale a igualdade

$$(Id_C \otimes [(\Delta \otimes Id_C) \circ \Delta]) \circ \Delta = (Id_C \otimes [(Id_C \otimes \Delta) \circ \Delta]) \circ \Delta \tag{1.2}$$

Notemos agora que

$$(Id_C \otimes [(Id_C \otimes \Delta) \circ \Delta]) \circ \Delta = (Id_C \otimes Id_C \otimes \Delta) \circ (\Delta \otimes Id_C) \circ \Delta \tag{1.3}$$

De fato, temos que

$$\begin{aligned}[(Id_C \otimes [(Id_C \otimes \Delta) \circ \Delta]) \circ \Delta](x) &= [Id_C \otimes [(Id_C \otimes \Delta) \circ \Delta]](x_1 \otimes x_2) = \\ &= x_1 \otimes ([Id_C \otimes \Delta]((x_2)_1 \otimes (x_2)_2)) = \\ &= x_1 \otimes (x_2)_1 \otimes ((x_2)_2)_1 \otimes ((x_2)_2)_2\end{aligned}$$

Por outro lado, utilizando a coassociativade, isto é $(x_1)_1 \otimes (x_1)_2 \otimes x_2 = x_1 \otimes (x_2)_1 \otimes (x_2)_2$, temos que

$$\begin{aligned}[(Id_C \otimes Id_C \otimes \Delta) \circ (\Delta \otimes Id_C) \circ \Delta](x) &= [Id_C \otimes Id_C \otimes \Delta]((x_1)_1 \otimes (x_1)_2 \otimes x_2) = \\ &= [Id_C \otimes Id_C \otimes \Delta](x_1 \otimes (x_2)_1 \otimes (x_2)_2) = \\ &= x_1 \otimes (x_2)_1 \otimes ((x_2)_2)_1 \otimes ((x_2)_2)_2\end{aligned}$$

Portanto, temos que vale a igualdade dada em (1.3).

Observe agora que vale também

$$(Id_C \otimes Id_C \otimes \Delta) \circ (\Delta \otimes Id_C) \circ \Delta = (\Delta \otimes \Delta) \circ \Delta \tag{1.4}$$

De fato, temos que

$$[(\Delta \otimes \Delta) \circ \Delta](x) = [\Delta \otimes \Delta](x_1 \otimes x_2) = \Delta(x_1) \otimes \Delta(x_2) = (x_1)_1 \otimes (x_1)_2 \otimes (x_2)_1 \otimes (x_2)_2$$

Por outro lado,

$$\begin{aligned}[(Id_C \otimes Id_C \otimes \Delta) \circ (\Delta \otimes Id_C) \circ \Delta](x) &= [Id_C \otimes Id_C \otimes \Delta]((x_1)_1 \otimes (x_1)_2 \otimes x_2) = \\ &= (x_1)_1 \otimes (x_1)_2 \otimes (x_2)_1 \otimes (x_2)_2\end{aligned}$$

Portanto, temos que vale a igualdade dada em (1.4).

Por fim, temos também a igualdade

$$(\Delta \otimes \Delta) \circ \Delta = (\Delta \otimes Id_C \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta \tag{1.5}$$

De fato, já sabemos que $[(\Delta \otimes \Delta) \circ \Delta](x) = (x_1)_1 \otimes (x_1)_2 \otimes (x_2)_1 \otimes (x_2)_2$. Por outro lado, temos que

$$\begin{aligned}[(\Delta \otimes Id_C \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta](x) &= [\Delta \otimes Id_C \otimes Id_C](x_1 \otimes (x_2)_1 \otimes (x_2)_2) = \\ &= (x_1)_1 \otimes (x_1)_2 \otimes (x_2)_1 \otimes (x_2)_2\end{aligned}$$

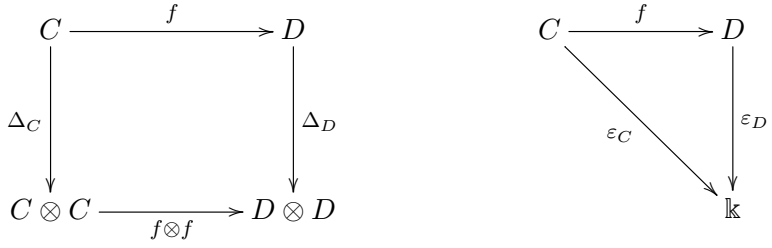
Portanto, temos que vale a igualdade dada em (1.5).

Logo, pelas igualdades dadas em (1.1),(1.2),(1.3),(1.4) e (1.5), obtemos o desejado, isto é, vale a igualdade $(Id_C \otimes \Delta \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta = (\Delta \otimes Id_C \otimes Id_C) \circ (Id_C \otimes \Delta) \circ \Delta$. □

Pelo que vimos durante a demonstração, em termos de elementos, o Lema 1.1.10 significa que para qualquer $x \in C$, vale a igualdade $(x_1)_1 \otimes (x_1)_2 \otimes (x_2)_1 \otimes (x_2)_2 = x_1 \otimes ((x_2)_1)_1 \otimes ((x_2)_1)_2 \otimes (x_2)_2$. Neste caso, generalizamos nossa notação e denotamos $x_1 \otimes x_2 \otimes x_3 \otimes x_4$ para significar tanto o elemento $(x_1)_1 \otimes (x_1)_2 \otimes (x_2)_1 \otimes (x_2)_2$ quanto o elemento $x_1 \otimes ((x_2)_1)_1 \otimes ((x_2)_1)_2 \otimes (x_2)_2$, já que são iguais.

Como apresentamos homomorfismo de álgebras através de diagramas, agora é natural pensarmos em homomorfismo entre coálgebras. Precisamente, temos:

Definição 1.1.11. *Sejam C e D duas coálgebras com comultiplicações Δ_C e Δ_D e counidades ε_C e ε_D, respectivamente. Uma aplicação $f : C \to D$ é um* homomorfismo de coálgebras *se os seguintes diagramas são comutativos:*



Ou seja, $f : C \longrightarrow D$ é um homomorfismo de coálgebras se valem

$$\Delta_D \circ f = (f \otimes f) \circ \Delta_C \qquad e \qquad \varepsilon_D \circ f = \varepsilon_C.$$

Em termos de elementos, e utilizando a notação de Sweedler, temos que para qualquer $c \in C$, valem

$$f(c_1) \otimes f(c_2) = (f(c))_1 \otimes (f(c))_2 \quad e \quad \varepsilon_D(f(c)) = \varepsilon_C(c).$$

Quando acontece de um $\Bbbk$-espaço vetorial ter tanto a estrutura de álgebra quanto a estrutura de coálgebra, podemos nos perguntar se estas estruturas são compatíveis. No caso positivo, obtemos as biálgebras. Precisamente, temos:

Definição 1.1.12. *Um $\Bbbk$-espaço vetorial B é dito uma* biálgebra *se existem aplicações $\Bbbk$-lineares $m : B \otimes B \longrightarrow B, u : \Bbbk \longrightarrow B, \Delta : B \longrightarrow B \otimes B$ e $\varepsilon : B \longrightarrow \Bbbk$ tais que as três condições abaixo são satisfeitas:*

(i) (B, m, u) *é uma álgebra;*

(ii) (B, Δ, ε) *é uma coálgebra;*

(iii) Δ *e* ε *são homomorfismos de álgebras.*

Observamos que quando (B, m, u) é uma álgebra e (B, Δ, ε) é uma coálgebra, então Δ e ε serem homomorfismos de álgebras é equivalente a m e u serem homomorfismos de coálgebras. Ou seja, quando B é uma biálgebra, temos que B tem estrutura de álgebra, estrutura de coálgebra, e essas duas estruturas são compatíveis, no sentido que Δ e ε são homomorfismos de álgebras e m e u são homomorfismo de coálgebras.

Esta compatibilidade é expressa pelas seguintes igualdades:

$$\Delta(ab) = \Delta(a)\Delta(b) \quad \text{e} \quad \Delta(1_B) = 1_B \otimes 1_B$$

$$\varepsilon(ab) = \varepsilon(a)\varepsilon(b) \quad \text{e} \quad \varepsilon(1_B) = 1_{\Bbbk}$$

para todo $a, b \in B$.

Exemplo 1.1.13. *Já temos pelo* Exemplo 1.1.4 *que $(\Bbbk G, m, u)$ é uma álgebra e pelo* Exemplo 1.1.9 *que $(\Bbbk G, \Delta, \varepsilon)$ é uma coálgebra. Para verificar que $\Bbbk G$ é uma biálgebra, resta apenas verificarmos que Δ e ε são homomorfismos de álgebras. Mas de fato, para quaisquer $g, h \in \Bbbk G$, temos que vale $\Delta(gh) = gh \otimes gh = (g \otimes g)(h \otimes h) = \Delta(g)\Delta(h)$ e $\Delta(e) = e \otimes e$, e portanto Δ é um homomorfismo de álgebras. Além disso, $\varepsilon(gh) = 1_{\Bbbk} = 1_{\Bbbk}1_{\Bbbk} = \varepsilon(g)\varepsilon(h)$ e $\varepsilon(e) = 1_{\Bbbk}$, e portanto ε é também um homomorfismo de álgebras.*

Sejam (C, Δ, ε) uma coálgebra e (A, m, u) uma álgebra. Obviamente temos que $Hom_{\Bbbk}(C, A)$ é um $\Bbbk$-espaço vetorial, já que tanto C quanto A são $\Bbbk$-espaços vetoriais. Notemos que em $Hom_{\Bbbk}(C, A)$ a soma é pontual, isto é $[f + g](x) = f(x) + g(x)$, e de forma natural a multiplicação por escalares é dada por $[\alpha f](x) = \alpha f(x) = f(\alpha x)$, para quaisquer que sejam $f, g \in Hom_{\Bbbk}(C, A)$, $\alpha \in \Bbbk$ e $x \in C$.

Em $Hom_{\Bbbk}(C, A)$ definimos duas aplicações $\Bbbk$-lineares, o *produto convolução*, que será denotado por $*$, dado por $f * g = m \circ (f \otimes g) \circ \Delta$, para $f, g \in Hom_{\Bbbk}(C, A)$, e a aplicação unidade, dada por $u_{Hom_{\Bbbk}(C,A)} : \Bbbk \longrightarrow Hom_{\Bbbk}(C, A)$, onde definimos $u_{Hom_{\Bbbk}(C,A)}(1_{\Bbbk}) = u \circ \varepsilon$, e estendemos linearmente.

Em termos de elementos, para quaisquer $f, g \in Hom_{\Bbbk}(C, A)$ e $c \in C$, o produto convolução se traduz como

$$\begin{aligned}[f * g](c) &= [[m \circ (f \otimes g)] \circ \Delta](c) = [m \circ (f \otimes g)](\Delta(c)) = [m \circ (f \otimes g)](c_1 \otimes c_2) = \\ &= m([f \otimes g](c_1 \otimes c_2)) = m(f(c_1) \otimes g(c_2)) = f(c_1)g(c_2)\end{aligned}$$

Afirmamos que com estas duas aplicações $Hom_{\Bbbk}(C, A)$ se torna uma álgebra. Para isso, precisamos verificar que valem as igualdades $f * (g * h) = (f * g) * h$ e $1_{Hom_{\Bbbk}(C,A)} * f = f * 1_{Hom_{\Bbbk}(C,A)} = f$, para quaisquer f, g e $h \in Hom_{\Bbbk}(C, A)$.

De fato, para qualquer $c \in C$, temos:

$$[f * (g * h)](c) = f(c_1)[(g * h)(c_2)] = f(c_1)[g((c_2)_1)h((c_2)_2)]$$

Por outro lado,

$$[(f * g) * h](c) = [(f * g)(c_1)]h(c_2) = [f((c_1)_1)g((c_1)_2)]h(c_2)$$

Desde que $c_1 \otimes (c_2)_1 \otimes (c_2)_2 = (c_1)_1 \otimes (c_1)_2 \otimes c_2$, para qualquer $c \in C$, temos que
$[f * (g * h)](c) = [(f * g) * h](c)$. Logo vale que $f * (g * h) = (f * g) * h$.

Por fim, lembre que usualmente denotamos $u_{Hom_{\Bbbk}(C,A)}(1_{\Bbbk}) := 1_{Hom_{\Bbbk}(C,A)}$. Desde que definimos $u_{Hom_{\Bbbk}(C,A)}(1_{\Bbbk}) = u \circ \varepsilon$, precisamos verificar que

$$f * (u \circ \varepsilon) = f = (u \circ \varepsilon) * f$$

De fato, para qualquer $c \in C$, temos que

$$\begin{aligned}[f * (u \circ \varepsilon)](c) &= f(c_1)[(u \circ \varepsilon)](c_2) = f(c_1)[u(\varepsilon(c_2)) = f(c_1)[\varepsilon(c_2)u(1_{\Bbbk})] = \\ &= f(c_1\varepsilon(c_2))1_A = f(c)\end{aligned}$$

Logo, $f * (u \circ \varepsilon) = f$. De forma análoga, obtemos que $(u \circ \varepsilon) * f = f$.

Com isso, concluímos que $Hom_{\Bbbk}(C, A)$ é de fato uma álgebra.

Lembremos agora que se B é uma biálgebra, então B tem tanto estrutura de álgebra quanto de coálgebra, portanto, pelo que vimos, $Hom_{\Bbbk}(B, B)$ é uma álgebra. Estamos agora aptos a definir o principal objeto de nosso estudo, as álgebras de Hopf.

Definição 1.1.14. *Seja $(H, m, u, \Delta, \varepsilon)$ uma biálgebra. Dizemos que H é uma* álgebra de Hopf *se existe um elemento $S \in Hom_{\Bbbk}(H, H)$ que é o inverso de Id_H com relação ao produto convolução $*$, isto é $S * Id_H = 1_{Hom_{\Bbbk}(C,A)} = u \circ \varepsilon$ e também $Id_H * S = u \circ \varepsilon$.*

A aplicação S é chamada antípoda *de H.*

Em termos de elementos, para qualquer $h \in H$, temos

$$[S * Id_H](h) = [m \circ (S \otimes Id_H) \circ \Delta](h) = \sum S(h_1)h_2$$

e analogamente $[Id_H * S](h) = \sum h_1 S(h_2)$. Desde que $[u \circ \varepsilon](h) = \varepsilon(h)1_H$, temos que numa álgebra de Hopf valem as igualdades

$$\sum S(h_1)h_2 = \sum h_1 S(h_2) = \varepsilon(h)1_H$$

Notemos que em uma álgebra de Hopf H, temos que a antípoda S é única, visto que é o elemento inverso de Id_H no produto convolução de $Hom_{\Bbbk}(H, H)$.

Exemplo 1.1.15. *Já tínhamos pelo* Exemplo 1.1.13 *que $\Bbbk G$ era uma biálgebra. Para que $\Bbbk G$ seja uma álgebra de Hopf, resta apenas definir a antípoda. Seja $S : \Bbbk G \longrightarrow \Bbbk G$ dada por $S(g) = g^{-1}$, onde g^{-1} denota o elemento inverso de g com relação a operação do grupo.*

Vamos verificar que S é de fato a antípoda de $\Bbbk G$. Notemos primeiramente que:

$$[u_{\Bbbk G} \circ \varepsilon_{\Bbbk G}](g) = u_{\Bbbk G}(\varepsilon_{\Bbbk G}(g)) = u_{\Bbbk G}(1_{\Bbbk}) = e$$

Por outro lado,

$$[S * Id_{\Bbbk G}](g) = S(g)Id_{\Bbbk G}(g) = S(g)g = g^{-1}g = e$$

Logo, $S * Id_{\Bbbk G} = u_{\Bbbk G} \circ \varepsilon_{\Bbbk G}$. Da mesma forma obtemos que $Id_{\Bbbk G} * S = u_{\Bbbk G} \circ \varepsilon_{\Bbbk G}$. Portanto S é de fato a antípoda de $\Bbbk G$.

Definição 1.1.16. *Seja H uma álgebra de Hopf. Um $\Bbbk$ subespaço vetorial B de H é dito uma* subálgebra de Hopf de H *se B é uma subálgebra de H, uma subcoálgebra de H e $S(B) \subseteq B$.*

Notemos que B ser uma subálgebra de H significa que $m(B \otimes B) \subseteq B$ e $1_H \in B$, e B ser uma subcoálgebra de H significa que $\Delta(B) \subseteq B \otimes B$. Assim, uma subálgebra de Hopf B de H tem a mesma unidade de H, e B é uma álgebra de Hopf com as estruturas induzidas de H.

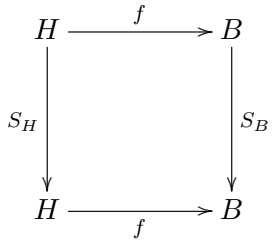
Exemplo 1.1.17. *É fácil verificar que se T é um subgrupo de G, então $\Bbbk T$ é subálgebra de Hopf de $\Bbbk G$.*

Definição 1.1.18. *Sejam H e B duas álgebras de Hopf. Dizemos que $f : H \longrightarrow B$ é um* homomorfismo de álgebras de Hopf *se f é um homomorfismo de álgebras e também é um homomorfismo de coálgebras.*

Seria natural exigir que, além de homomorfismo de álgebras e de coálgebras, um homomorfismo de álgebras de Hopf $f : H \longrightarrow B$ também exigisse que $S_B \circ f = f \circ S_H$. Veremos na proposição a seguir que não é necessário fazer esta exigência, uma vez que sempre teremos esta igualdade para uma tal f que seja homomorfismo de álgebras e de coálgebras.

Proposição 1.1.19. *Sejam H e B duas álgebras de Hopf e $f : H \longrightarrow B$ um homomorfismo de álgebras de Hopf. Então $S_B \circ f = f \circ S_H$. Em termos de diagrama, significa dizer que o diagrama*

abaixo é comutativo:



Demonstração. Considere a álgebra $Hom_{\Bbbk}(H,B)$, e lembre que a multiplicação é dada pelo produto convolução e a unidade é dada por $1_{Hom_{\Bbbk}(H,B)} = u_B \circ \varepsilon_H$. Temos que $S_B \circ f$ e $f \circ S_H$ são elementos de $Hom_{\Bbbk}(H,B)$. Vamos mostrar que f é um elemento inversível em $Hom_{\Bbbk}(H,B)$ com relação ao produto convolução. De fato, para qualquer $h \in H$, temos que

$$\begin{aligned}
[(S_B \circ f) * f](h) &= [S_B \circ f](h_1)f(h_2) = S_B(f(h_1))f(h_2) = S_B((f(h))_1)f(h)_2 = \\
&= \varepsilon_B(f(h))1_B = [\varepsilon_B \circ f](h)1_B = \varepsilon_H(h)1_B = \varepsilon_H(h)u_B(1_{\Bbbk}) = \\
&= u_B(\varepsilon_H(h)1_{\Bbbk}) = u_B(\varepsilon_H(h)) = [u_B \circ \varepsilon_H](h) = 1_{Hom_{\Bbbk}(H,B)}(h)
\end{aligned}$$

Logo, $S_B \circ f$ é um inverso à esquerda para f, no produto convolução. Analogamente, temos

$$\begin{aligned}
[f * (f \circ S_H)](h) &= f(h_1)[f \circ S_H](h_2) = f(h_1)f(S_H(h_2)) = f(h_1 S_H(h_2)) = \\
&= f(\varepsilon_H(h)1_H) = \varepsilon_H(h)f(1_H) = \varepsilon_H(h)1_B = \varepsilon_H(h)u_B(1_{\Bbbk}) = \\
&= u_B(\varepsilon_H(h)1_{\Bbbk}) = u_B(\varepsilon_H(h)) = [u_B \circ \varepsilon_H](h) = 1_{Hom_{\Bbbk}(H,B)}(h)
\end{aligned}$$

Logo, $f \circ S_H$ é um inverso à direita para f, no produto convolução.

Com isso, temos que f é inversível, e portanto os inversos à esquerda e à direita coincidem, isto é $f^{-1} = S_B \circ f = f \circ S_H$, como queríamos. □

Veremos a seguir algumas propriedades úteis e interessantes sobre a antípoda S de uma álgebra de Hopf H.

Proposição 1.1.20. *Seja $(H, m, u, \Delta, \varepsilon, S)$ uma álgebra de Hopf. Então, para quaisquer $g, h \in H$, temos:*

(*i*) $S(hg) = S(g)S(h)$;

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

(*iii*) $\Delta(S(h)) = S(h_2) \otimes S(h_1)$;

(*iv*) $\varepsilon(S(h)) = \varepsilon(h)$.

Os itens (*i*) e (*ii*) da proposição acima fazem com que digamos que S é um *anti-homomorfismo de álgebras*, e os itens (*iii*) e (*iv*) fazem com que digamos que S é também um *anti-homomorfismo de coálgebras.*

Demonstração. (i) Consideremos na álgebra $Hom_{\Bbbk}(H \otimes H, H)$, onde a multiplicação é dada pelo produto convolução e a unidade é dada por $u_{Hom_{\Bbbk}(H\otimes H,H)}(1_{\Bbbk}) = 1_{Hom_{\Bbbk}(H\otimes H,H)} = u_H \circ \varepsilon_{H\otimes H}$, as aplicações $F, G : H \otimes H \longrightarrow H$ dadas por $F(h \otimes g) = S(g)S(h)$ e $G(h \otimes g) = S(hg)$, para quaisquer $g, h \in H$. Vamos provar que F é um inverso à direita para m e G é um inverso à esquerda para m, donde segue que m é inversível e seu inverso é único, isto é $m^{-1} = F = G$, e com isso concluímos que $S(g)S(h) = S(hg), \forall g, h \in H$. Seja $h \otimes g \in H \otimes H$. Temos que

$$\begin{aligned}
[m * F](h \otimes g) &= m((h \otimes g)_1)F((h \otimes g)_2) = m(h_1 \otimes g_1)F(h_2 \otimes g_2) = \\
&= h_1 g_1 S(g_2)S(h_2) = h_1(g_1 S(g_2))S(h_2) = h_1 \varepsilon_H(g) 1_H S(h_2) = \\
&= \varepsilon_H(g)(h_1 S(h_2)) = \varepsilon_H(g)\varepsilon_H(h)1_H = \varepsilon_H(h)\varepsilon_H(g)1_H = \\
&= \varepsilon_{H\otimes H}(h \otimes g)1_H = [u_H \circ \varepsilon_{H\otimes H}](h \otimes g) = 1_{Hom_{\Bbbk}(H\otimes H,H)}(h \otimes g)
\end{aligned}$$

Logo, F é um inverso à direita para m, no produto convolução. Analogamente, temos

$$\begin{aligned}
[G * m](h \otimes g) &= G((h \otimes g)_1)m((h \otimes g)_2) = G(h_1 \otimes g_1)m(h_2 \otimes g_2) = S(h_1 g_1)h_2 g_2 = \\
&= S((hg)_1)(hg)_2 = \varepsilon_H(hg)1_H = \varepsilon_H(h)\varepsilon_H(g)1_H = \varepsilon_{H\otimes H}(h \otimes g)1_H = \\
&= \varepsilon_{H\otimes H}(h \otimes g)u_H(1_{\Bbbk}) = [u_H \circ \varepsilon_{H\otimes H}](h \otimes g) = 1_{Hom_{\Bbbk}(H\otimes H,H)}(h \otimes g)
\end{aligned}$$

Logo, G é um inverso à esquerda para m, no produto convolução. Portanto segue que $F = G$, e com isso $S(g)S(h) = S(hg), \forall g, h \in H$, como queríamos.

(ii) Sabemos que $S(h_1)h_2 = \varepsilon(h)1_H$, para qualquer $h \in H$ e também que $\Delta(1_H) = 1_H \otimes 1_H$ e $\varepsilon(1_H) = 1_{\Bbbk}$. Assim, em particular para $h = 1_H$, temos que $S(1_H)1_H = \varepsilon(1_H)1_H$, ou seja, $S(1_H) = 1_H$.

(iii) Consideremos na álgebra $Hom_{\Bbbk}(H, H \otimes H)$, onde a multiplicação é dada pelo produto convolução e a unidade é dada por $u_{Hom_{\Bbbk}(H,H\otimes H)}(1_{\Bbbk}) = 1_{Hom_{\Bbbk}(H,H\otimes H)} = u_{H\otimes H} \circ \varepsilon_H$, as aplicações $F, G : H \longrightarrow H \otimes H$ dadas por $F(h) = \Delta(S(h))$ e $G(h) = S(h_2) \otimes S(h_1)$, para qualquer $h \in H$. Vamos provar que F é um inverso à direita para Δ e G é um inverso à esquerda para Δ, donde segue que Δ é inversível e seu inverso é único, isto é $\Delta^{-1} = F = G$, e com isso $\Delta(S(h)) = S(h_2) \otimes S(h_1), \forall h \in H$. Seja $h \in H$. Temos que

$$\begin{aligned}
[\Delta * F](h) &= \Delta(h_1)F(h_2) = \Delta(h_1)\Delta(S(h_2)) = \Delta(h_1 S(h_2)) = \Delta(\varepsilon(h)1_H) = \varepsilon(h)\Delta(1_H) = \\
&= \varepsilon(h)(1_H \otimes 1_H) = \varepsilon(h)u_{H\otimes H}(1_{\Bbbk}) = u_{H\otimes H}(\varepsilon(h)1_{\Bbbk}) = u_{H\otimes H}(\varepsilon(h)) = [u_{H\otimes H} \circ \varepsilon](h)
\end{aligned}$$

Logo, F é um inverso à direita para Δ, no produto convolução. Utilizando a notação da coassociatividade generalizada e o Lema 1.1.10, obtemos analogamente que

$$\begin{aligned}
[G * \Delta](h) &= G(h_1)\Delta(h_2) = (S((h_1)_2) \otimes S((h_1)_1))((h_2)_1 \otimes (h_2)_2) = (S(h_2) \otimes S(h_1))(h_3 \otimes h_4) = \\
&= S(h_2)h_3 \otimes S(h_1)h_4 = S(((h_2)_1)_1)((h_2)_1)_2 \otimes S(h_1)(h_2)_2 = \varepsilon((h_2)_1)1_H \otimes S(h_1)(h_2)_2 = \\
&= 1_H \otimes S(\varepsilon((h_2)_1)h_1)(h_2)_2 = 1_H \otimes S(\varepsilon((h_1)_2)(h_1)_1)h_2 = \\
&= 1_H \otimes S(h_1)h_2 = 1_H \otimes \varepsilon(h)1_H = [u_{H\otimes H} \circ \varepsilon](h)
\end{aligned}$$

Logo, G é um inverso à esquerda para Δ, no produto convolução. Portanto segue que $F = G$, e com isso $\Delta(S(h)) = S(h_2) \otimes S(h_1), \forall h \in H$, como queríamos.

(iv) Sabemos que $h_1 S(h_2) = \varepsilon(h)1_H$ e também que $\varepsilon(hg) = \varepsilon(h)\varepsilon(g)$ e $\varepsilon(1_H) = 1_{\Bbbk}$, para quaisquer $g, h \in H$. Aplicando ε na igualdade $h_1 S(h_2) = \varepsilon(h)1_H$, obtemos que $\varepsilon(h_1 S(h_2)) = \varepsilon(\varepsilon(h)1_H)$, e com isso $\varepsilon(h_1)\varepsilon(S(h_2)) = \varepsilon(h)\varepsilon(1_H) = \varepsilon(h)$. Desde que $\varepsilon(h) \in \Bbbk, \forall h \in H$, e tanto ε quanto S são $\Bbbk$-lineares, temos que $\varepsilon(h_1)\varepsilon(S(h_2)) = \varepsilon(S(\varepsilon(h_1)h_2)) = \varepsilon(S(h))$. Ou seja, $\varepsilon(S(h)) = \varepsilon(h)$, como queríamos. □

Quando a antípoda S da álgebra de Hopf H é bijetora, isto é, existe S^{-1} tal que $S \circ S^{-1} = Id_H$ e também $Id_H = S^{-1} \circ S$, temos também que S^{-1} é um anti-homomorfismo de álgebras e de coálgebras. Ou seja, temos a seguinte proposição:

Proposição 1.1.21. *Seja $(H, m, u, \Delta, \varepsilon, S)$ uma álgebra de Hopf com antípoda S bijetora. Então, para quaisquer $g, h \in H$, temos:*

(i) $S^{-1}(hg) = S^{-1}(g)S^{-1}(h)$;

(ii) $S^{-1}(1_H) = 1_H$;

(iii) $\Delta(S^{-1}(h)) = S^{-1}(h_2) \otimes S^{-1}(h_1)$;

(iv) $\varepsilon(S^{-1}(h)) = \varepsilon(h)$.

Além disso, de $S * Id_H = u \circ \varepsilon = Id_H * S$, temos que vale também

(v) $S^{-1}(h_2)h_1 = h_2 S^{-1}(h_1) = \varepsilon(h)1_H$.

Demonstração. Considerando as propriedades demonstradas na Proposição 1.1.20 e que a antípoda S é bijetora, temos para quaisquer $h, g \in H$:

(i) Note que $hg = S(S^{-1}(h))S(S^{-1}(g)) = S(S^{-1}(g)S^{-1}(h))$. Assim, aplicando S^{-1} em ambos os lados, obtemos que $S^{-1}(hg) = S^{-1}(g)S^{-1}(h)$.

(ii) Como $S(1_H) = 1_H$, aplicando S^{-1} em ambos lados obtemos $S^{-1}(1_H) = 1_H$.

(iii) Lembre que denotamos $\Delta(h) = h_1 \otimes h_2, \forall h \in H$.

Mas, por outro lado, $\Delta(h) = \Delta(S(S^{-1}(h))) = S((S^{-1}(h))_2) \otimes S((S^{-1}(h))_1)$. Disto, concluímos que $h_1 \otimes h_2 = S((S^{-1}(h))_2) \otimes S((S^{-1}(h))_1)$. Assim, aplicando $S^{-1} \otimes S^{-1}$ nesta igualdade, obtemos que $S^{-1}(h_1) \otimes S^{-1}(h_2) = (S^{-1}(h))_2 \otimes (S^{-1}(h))_1$, e por fim, aplicando o *twist*, obtemos que

$$S^{-1}(h_2) \otimes S^{-1}(h_1) = (S^{-1}(h))_1 \otimes (S^{-1}(h))_2 = \Delta(S^{-1}(h)).$$

Logo, $\Delta(S^{-1}(h)) = S^{-1}(h_2) \otimes S^{-1}(h_1)$.

(iv) Como $h = S(S^{-1}(h))$, temos que $\varepsilon(h) = \varepsilon(S(S^{-1}(h))) = \varepsilon(S^{-1}(h))$, onde a última igualdade vem do item (iv) da Proposição 1.1.20.

(v) Temos $S^{-1}(h_2)h_1 = S^{-1}(h_2)S^{-1}(S(h_1)) = S^{-1}(S(h_1)h_2)$, onde a última igualdade vem do item (i). Como $S(h_1)h_2 = \varepsilon(h)1_H$, obtemos que

$$S^{-1}(h_2)h_1 = S^{-1}(S(h_1)h_2) = S^{-1}(\varepsilon(h)1_H) = \varepsilon(h)S^{-1}(1_H) = \varepsilon(h)1_H.$$

Analogamente obtemos que $h_2S^{-1}(h_1) = \varepsilon(h)1_H$. □

Utilizaremos estas propriedades para obter um exemplo importante em nosso estudo.

Exemplo 1.1.22. *Seja $(H, m, u, \Delta, \varepsilon, S)$ uma álgebra de Hopf com antípoda S bijetora. Então temos que $H^{cop} := (H, m, u, \Delta_{cop}, \varepsilon, S^{-1})$ é uma álgebra de Hopf com antípoda S^{-1}, onde $\Delta_{cop} = \tau \circ \Delta$, onde τ é o* twist.

No que segue, vamos considerar o dual linear $Hom_{\Bbbk}(V, \Bbbk)$ de um $\Bbbk$-espaço vetorial V, que denotaremos por V^*.

Para concluir esta seção, vejamos dois importantes resultados sobre álgebras e coálgebras. Estes resultados nos dão a dualidade entre estes conceitos, já que é a construção da estrutura de coálgebra em A^* a partir de uma álgebra A, quando esta tem dimensão finita, e também a construção da estrutura de álgebra em C^* a partir de uma coálgebra qualquer C.

Sabemos da álgebra linear que quando V e W são dois $\Bbbk$-espaços vetoriais, temos que aplicação $\Theta : V^* \otimes W^* \longrightarrow (V \otimes W)^*$ é injetiva, onde $\Theta(f \otimes g)$ é o funcional linear $\Theta(f \otimes g) : V \otimes W \longrightarrow \Bbbk$ dado por $[\Theta(f \otimes g)](v \otimes w) = f(v)g(w)$, para quaisquer $f \in V^*, g \in W^*, v \in V$ e $w \in W$. Assim se os espaços V e W têm dimensão finita, então Θ é um isomorfismo.

Dada uma aplicação $\phi : V \longrightarrow W$, denotamos por ϕ^* a aplicação $\phi^* : W^* \longrightarrow V^*$ dada por $\phi^*(f) = f \circ \phi$.

Proposição 1.1.23. *Seja (C, Δ, ε) uma coálgebra. Então C^* é uma álgebra.*

Demonstração. Definimos $m_{C^*} = \Delta^* \circ \Theta$ e $u_{C^*} = \varepsilon^* \circ \psi$, onde $\psi : \Bbbk \longrightarrow \Bbbk^*$ é o isomorfismo dado por $[\psi(\alpha)](x) = \alpha x$, para $\alpha, x \in \Bbbk$.

Vamos provar então que (C^*, m_{C^*}, u_{C^*}) é uma álgebra.

Para isso, precisamos verificar que $m_{C^*} \circ (m_{C^*} \otimes Id_{C^*}) = m_{C^*} \circ (Id_{C^*} \otimes m_{C^*})$ e que para qualquer $f \in C^*$, vale que $[m_{C^*} \circ (u_{C^*} \otimes Id_{C^*})](1 \otimes f) = f = [m_{C^*} \circ (Id_{C^*} \otimes u_{C^*})](f \otimes 1)$.

Primeiro vejamos que para quaisquer $f, g \in C^*$ e $x \in C$, temos que $[m_{C^*}(f \otimes g)](x) = f(x_1)g(x_2)$. De fato, temos

$$\begin{aligned}[m_{C^*}(f \otimes g)](x) &= [[\Delta^* \circ \Theta](f \otimes g)](x) = [\Delta^*(\Theta(f \otimes g))](x) = [\Theta(f \otimes g) \circ \Delta](x) = \\ &= [\Theta(f \otimes g)](\Delta(x)) = [\Theta(f \otimes g)](x_1 \otimes x_2) = f(x_1)g(x_2)\end{aligned}$$

Vejamos também que para qualquer $x \in C$, temos $[u_{C^*}(1_{\Bbbk})](x) = \varepsilon(x)$, ou seja, $u_{C^*}(1_{\Bbbk}) = 1_{C^*} = \varepsilon$. De fato, temos

$$[u_{C^*}(1_{\Bbbk})](x) = [[\varepsilon^* \circ \psi](1_{\Bbbk})](x) = [\varepsilon^*(\psi(1_{\Bbbk})](x) = [\psi(1_{\Bbbk}) \circ \varepsilon](x) = [\psi(1_{\Bbbk})](\varepsilon(x)) = 1_{\Bbbk}\varepsilon(x) = \varepsilon(x)$$

Agora, sejam $f, g, h \in C^*$ e $x \in C$. Temos que

$$\begin{aligned}[[m_{C^*} \circ (m_{C^*} \otimes Id_{C^*})](f \otimes g \otimes h)](x) &= [m_{C^*}(m_{C^*}(f \otimes g) \otimes Id_{C^*}(h))](x) = \\ = \quad [m_{C^*}(m_{C^*}(f \otimes g) \otimes h)](x) &= [m_{C^*}(f \otimes g)](x_1)h(x_2) = f((x_1)_1)g((x_1)_2)h(x_2)\end{aligned}$$

Por outro lado, obtemos analogamente que

$$[[m_{C^*} \circ (Id_{C^*} \otimes m_{C^*})](f \otimes g \otimes h)](x) = f(x_1)g((x_2)_1)h((x_2)_2)$$

Como $x_1 \otimes (x_2)_1 \otimes (x_2)_2 = (x_1)_1 \otimes (x_1)_2 \otimes x_2$, aplicando $f \otimes g \otimes h$ e utilizando o isomorfismo canônico de $\Bbbk \otimes \Bbbk \otimes \Bbbk$ em $\Bbbk$, temos que

$$f((x_1)_1)g((x_1)_2)h(x_2) = f(x_1)g((x_2)_1)h((x_2)_2)$$

e portanto vale que $m_{C^*} \circ (m_{C^*} \otimes Id_{C^*}) = m_{C^*} \circ (Id_{C^*} \otimes m_{C^*})$. Além disso, também temos que

$$\begin{aligned}[[m_{C^*} \circ (u_{C^*} \otimes Id_{C^*})](1 \otimes f)](x) &= [m_{C^*}([u_{C^*} \otimes Id_{C^*}](1 \otimes f))](x) = \\ = \quad [m_{C^*}(u_{C^*}(1) \otimes Id_{C^*}(f))](x) &= [m_{C^*}(\varepsilon \otimes f)](x) = \varepsilon(x_1)f(x_2) = f(\varepsilon(x_1)x_2) = f(x)\end{aligned}$$

Logo, $[m_{C^*} \circ (u_{C^*} \otimes Id_{C^*})](1 \otimes f) = f$.

Analogamente, obtemos também que $[m_{C^*} \circ (Id_{C^*} \otimes u_{C^*})](f \otimes 1) = f$.

Portanto (C^*, m_{C^*}, u_{C^*}) é de fato uma álgebra. □

Notemos que, pelo que foi realizado, a multiplicação em C^* é o produto convolução e a unidade 1_{C^*} é a aplicação ε.

Agora, vejamos a construção de uma coálgebra a partir de uma álgebra de dimensão finita.

Suponha que (A, m, u) é uma álgebra de dimensão finita. Desde que A tem dimensão finita, temos que $\Theta : A^* \otimes A^* \longrightarrow (A \otimes A)^*$ dada anteriormente é um isomorfismo, ou seja, podemos considerar $\Theta^{-1} : (A \otimes A)^* \longrightarrow A^* \otimes A^*$. Definimos então $\Delta_{A^*} = \Theta^{-1} \circ m^*$ e $\varepsilon_{A^*} = \varphi \circ u^*$, onde $\varphi : \Bbbk^* \longrightarrow \Bbbk$ é dada por $\varphi(f) = f(1_{\Bbbk})$, para qualquer $f \in \Bbbk^*$. Veremos logo a seguir que $(A^*, \Delta_{A^*}, \varepsilon_{A^*})$ é uma coálgebra.

Antes, contudo, vejamos uma importante caracterização desta comultiplicação Δ_{A^*}.

Notemos que $\Delta_{A^*}(f) = [\Theta^{-1} \circ m^*](f) = \Theta^{-1}(m^*(f)) = \Theta^{-1}(f \circ m) \in A^* \otimes A^*$.

Assim, se $\Delta_{A^*}(f) = \sum_{i=1}^n g_i \otimes h_i$, onde $g_i, h_i \in A^*$ para cada $i = 1, ..., n$, obtemos então que $\Theta^{-1}(f \circ m) = \sum_{i=1}^n g_i \otimes h_i$. Portanto, aplicando Θ em ambos lados dessa última igualdade, concluímos que $\Theta(\Theta^{-1}(f \circ m)) = \Theta(\sum_{i=1}^n g_i \otimes h_i)$, ou seja, $f \circ m = \Theta(\sum_{i=1}^n g_i \otimes h_i)$.

Com isso, o que obtemos então foi que para qualquer $a \otimes b \in A \otimes A$, temos que vale a igualdade $[f \circ m](a \otimes b) = [\Theta(\sum_{i=1}^{n} g_i \otimes h_i)](a \otimes b)$, e isto quer dizer que $f(ab) = \sum_{i=1}^{n} g_i(a)h_i(b)$.

Lembre que pela notação de Sweedler denotamos $\Delta_{A^*}(f) := f_1 \otimes f_2$, portanto a construção acima garante que se $\Delta_{A^*}(f) = f_1 \otimes f_2$, então $f(ab) = f_1(a)f_2(b)$.

Por outro lado, se existe uma família de pares de elementos $\{(g'_j, h'_j) | j \in J\} \subseteq A^* \times A^*$ tais que satisfazem $\sum_{\text{finita}} g'_j(a)h'_j(b) = f(ab)$, para quaisquer $a, b \in A$, então temos que vale a igualdade $[\Theta(\sum_{i=1}^{n} g_i \otimes h_i)](a \otimes b) = [\Theta(\sum_{\text{finita}} g'_j \otimes h'_j)](a \otimes b)$, e portanto $\Theta(\sum_{i=1}^{n} g_i \otimes h_i) = \Theta(\sum_{\text{finita}} g'_j \otimes h'_j)$. Segue então da injetividade de Θ que $\sum_{\text{finita}} g'_j \otimes h'_j = \sum_{i=1}^{n} g_i \otimes h_i = \Delta_{A^*}(f)$.

Utilizando a notação de Sweedler, o que obtemos foi que se $f_1(a)f_2(b) = f(ab)$, para quaisquer $a, b \in A$, então $\Delta_{A^*}(f) = f_1 \otimes f_2$.

Desta forma, provamos o seguinte resultado:

Proposição 1.1.24. *Seja A uma álgebra de dimensão finita e $f \in A^*$. Então $\Delta_{A^*}(f) = f_1 \otimes f_2$ se e somente se $f(ab) = f_1(a)f_2(b), \forall a, b \in A$.*

Estamos agora aptos a provar que A^*, com as aplicações Δ_{A^*} e ε_{A^*} como dadas acima, é uma coálgebra.

Proposição 1.1.25. *Seja (A, m, u) uma álgebra de dimensão finita. Então $(A^*, \Delta_{A^*}, \varepsilon_{A^*})$ é uma coálgebra.*

Demonstração. Desde que A tem dimensão finita, temos que Θ dada anteriormente é um isomorfismo. Consideremos então $\Delta_{A^*} = \Theta^{-1} \circ m^*$ e $\varepsilon_{A^*} = \varphi \circ u^*$, onde $\varphi : \Bbbk^* \longrightarrow \Bbbk$ é dada por $\varphi(f) = f(1_\Bbbk)$, para qualquer $f \in \Bbbk^*$.

Para provar que $(A^*, \Delta_{A^*}, \varepsilon_{A^*})$ é uma coálgebra, precisamos então verificar que vale a igualdade $(\Delta_{A^*} \otimes Id_{A^*}) \circ \Delta_{A^*} = (Id_{A^*} \otimes \Delta_{A^*}) \circ \Delta_{A^*}$ e que para qualquer $f \in A^*$, vale $[\varepsilon_{A^*} \otimes Id_{A^*}](\Delta_{A^*}(f)) = 1_\Bbbk \otimes f$ e também $[Id_{A^*} \otimes \varepsilon_{A^*}](\Delta_{A^*}(f)) = f \otimes 1_\Bbbk$.

Seja $f \in A^*$. Temos que

$$\begin{aligned}[(\Delta_{A^*} \otimes Id_{A^*}) \circ \Delta_{A^*}](f) &= [\Delta_{A^*} \otimes Id_{A^*}](\Delta_{A^*}(f)) = [\Delta_{A^*} \otimes Id_{A^*}](f_1 \otimes f_2) = \\ &= \Delta_{A^*}(f_1) \otimes Id_{A^*}(f_2) = (f_1)_1 \otimes (f_1)_2 \otimes f_2\end{aligned}$$

Por outro lado, de forma análoga, temos que

$$[(Id_{A^*} \otimes \Delta_{A^*}) \circ \Delta_{A^*}](f) = f_1 \otimes (f_2)_1 \otimes (f_2)_2$$

Agora, notemos que para qualquer $a \otimes b \otimes c \in A \otimes A \otimes A$, temos que

$$\begin{aligned}[(f_1)_1 \otimes (f_1)_2 \otimes f_2](a \otimes b \otimes c) &= (f_1)_1(a) \otimes (f_1)_2(b) \otimes f_2(c) = \\ &= f_1(ab)f_2(c) \otimes 1_\Bbbk \otimes 1_\Bbbk = f((ab)c) \otimes 1_\Bbbk \otimes 1_\Bbbk,\end{aligned}$$

onde usamos a proposição anterior para garantir que $(f_1)_1(a)(f_1)_2(b) = f_1(ab)$ e também que vale $f_1(ab)f_2(c) = f((ab)c)$.

Por outro lado, de forma análoga, obtemos que

$$[f_1 \otimes (f_2)_1 \otimes (f_2)_2](a \otimes b \otimes c) = f(a(bc)) \otimes 1_{\Bbbk} \otimes 1_{\Bbbk}.$$

Desde que $(ab)c = a(bc)$, concluímos que $(f_1)_1 \otimes (f_1)_2 \otimes f_2 = f_1 \otimes (f_2)_1 \otimes (f_2)_2$, ou seja, temos a igualdade $(\Delta_{A^*} \otimes Id_{A^*}) \circ \Delta_{A^*} = (Id_{A^*} \otimes \Delta_{A^*}) \circ \Delta_{A^*}$, como queríamos.

Para verificar que $[\varepsilon_{A^*} \otimes Id_{A^*}](\Delta_{A^*}(f)) = 1_{\Bbbk} \otimes f$, vejamos inicialmente que para qualquer $f \in A^*$, temos que $\varepsilon_{A^*}(f) = [\varphi \circ u^*](f) = \varphi(u^*(f)) = \varphi(f \circ u) = [f \circ u](1_{\Bbbk}) = f(u(1_{\Bbbk})) = f(1_A)$, ou seja, $\varepsilon_{A^*}(f) = f(1_A)$.

Desde que $f(1_A) \in \Bbbk$, obtemos disto e da Proposição 1.1.24 que para qualquer $a \in A$, vale que $f(a) = f(1_A a) = f_1(1_A)f_2(a)$, ou seja, $f_1(1_A)f_2 = f$. Da mesma forma, obtemos que $f_2(1_A)f_1 = f$.

Assim,

$$\begin{aligned}[\varepsilon_{A^*} \otimes Id_{A^*}](\Delta_{A^*}(f)) &= [\varepsilon_{A^*} \otimes Id_{A^*}](f_1 \otimes f_2) = \varepsilon_{A^*}(f_1) \otimes Id_{A^*}(f_2) = \\ &= f_1(1_A) \otimes f_2 = 1_{\Bbbk} \otimes f_1(1_A)f_2 = 1_{\Bbbk} \otimes f,\end{aligned}$$

ou seja, $[\varepsilon_{A^*} \otimes Id_{A^*}](\Delta_{A^*}(f)) = 1_{\Bbbk} \otimes f$ como queríamos.

De forma análoga, obtemos que $[Id_{A^*} \otimes \varepsilon_{A^*}](\Delta_{A^*}(f)) = f \otimes 1_{\Bbbk}$.

Logo, concluímos que $(A^*, \Delta_{A^*}, \varepsilon_{A^*})$ é uma coálgebra. □

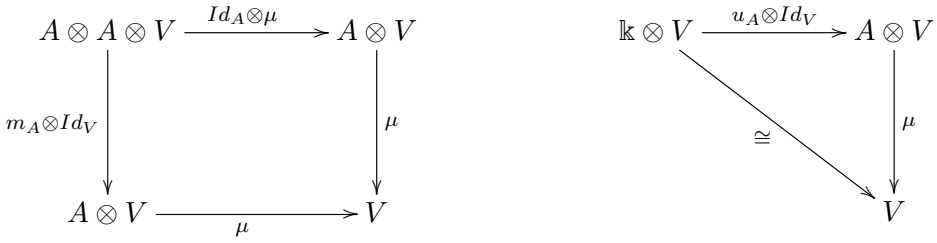
Podemos destacar destes últimos resultados que, quando $(H, m, u, \Delta, \varepsilon, S)$ é uma álgebra de Hopf de dimensão finita, então $(H^*, m_{H^*}, u_{H^*}, \Delta_{H^*}, \varepsilon_{H^*}, S^*)$ é uma álgebra de Hopf.

1.2 Módulos de Hopf

Nosso objetivo nesta seção será provar o Teorema Fundamental dos Módulos de Hopf. Para esse objetivo, introduziremos o conceito de comódulo, e assim como uma coálgebra tem o mesmo diagrama de definição que uma álgebra mas com as flechas invertidas, o comódulo se comporta da mesma forma mas com relação a definição de módulo. Portanto, começaremos essa seção dando uma definição de A-módulo à esquerda, utilizando diagramas e produtos tensoriais, mas ressaltamos que esta definição é equivalente a definição axiomática usualmente conhecida em textos clássicos. Observamos também que uma definição análoga pode ser feita para A-módulo à direita.

Definição 1.2.1. *Sejam V um $\Bbbk$-espaço vetorial e A uma álgebra sobre $\Bbbk$. Dizemos que V é um A-módulo à esquerda se existe uma aplicação $\Bbbk$-linear $\mu : A \otimes V \longrightarrow V$ tal que os diagramas abaixo*

comutam:



Notação 1.2.2. *Denotamos a imagem de um elemento $a \otimes v$ pela aplicação μ por $\mu(a \otimes v) := a \cdot v$ e dizemos que μ é uma ação e que A age em V.*

Com a notação fixada acima, temos que o primeiro diagrama diz que $\mu \circ (m_A \otimes Id_V) = \mu \circ (Id_A \otimes \mu)$, onde m_A é a multiplicação da álgebra A. Ou seja, para qualquer $a \otimes b \otimes v \in A \otimes A \otimes V$, temos

$$\begin{aligned} [\mu \circ (m_A \otimes Id_V)](a \otimes b \otimes v) &= [\mu \circ (Id_A \otimes \mu)](a \otimes b \otimes v) \\ \mu(m_A(a \otimes b) \otimes Id_V(v)) &= \mu(Id_A(a) \otimes \mu(b \otimes v) \\ \mu(ab \otimes v) &= \mu(a \otimes (b \cdot v)) \\ (ab) \cdot v &= a \cdot (b \cdot v) \end{aligned}$$

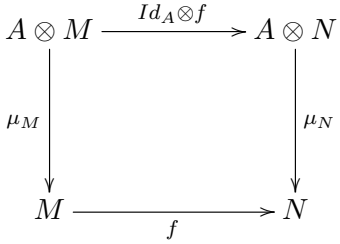
e o segundo diagrama diz que para qualquer $v \in V$, temos que $[\mu \circ (u_A \otimes Id_V)](1_\Bbbk \otimes v) = v$, onde u_A é a aplicação unidade da álgebra A.

Desde que $[\mu \circ (u_A \otimes Id_V)](1_\Bbbk \otimes v) = \mu(1_A \otimes v) = 1_A \cdot v$, temos a igualdade $1_A \cdot v = v$.

Como a aplicação μ é $\Bbbk$-linear, temos que esta definição é naturalmente equivalente a definição axiomática tradicionalmente utilizada para definir um A-módulo.

Exemplo 1.2.3. *Toda álgebra A é um A-módulo à esquerda via multiplicação m_A de A.*

Definição 1.2.4. *Sejam A uma $\Bbbk$-álgebra, M e N dois A-módulos à esquerda. Uma aplicação $f : M \longrightarrow N$ é um* homomorfismo de A-módulos à esquerda *se o seguinte diagrama é comutativo:*

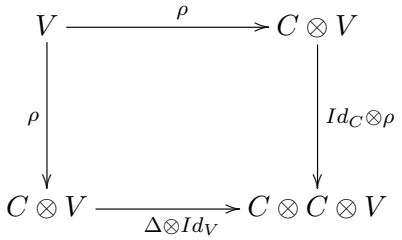


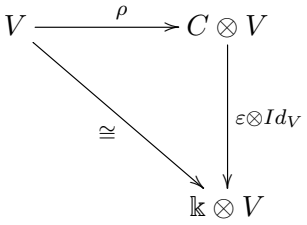
onde $\mu_M : A \otimes M \longrightarrow M$ é a ação de A em M e $\mu_N : A \otimes N \longrightarrow N$ é a ação de A em N. Ou seja, $f : M \longrightarrow N$ é um homomorfismo de A-módulos à esquerda se vale $\mu_N \circ (Id_A \otimes f) = f \circ \mu_M$.

Em termos de elementos, temos que para quaisquer $a \in A$ e $m \in M$, vale $f(a \cdot_M m) = a \cdot_N f(m)$.

Definição 1.2.5. *Sejam V um espaço vetorial sobre $\Bbbk$ e C uma coálgebra sobre $\Bbbk$. Dizemos que V é um C-comódulo à esquerda se existe uma aplicação $\Bbbk$-linear $\rho : V \longrightarrow C \otimes V$ tal que os seguintes*

diagramas comutam:





Assim, do primeiro diagrama temos a relação

$$(Id_C \otimes \rho) \circ \rho = (\Delta \otimes Id_V) \circ \rho$$

e do segundo diagrama temos que $[(\varepsilon \otimes Id_V) \circ \rho](v) = 1_{\Bbbk} \otimes v$, para todo $v \in V$.

A seguir estabeleceremos uma notação semelhante e inspirada na notação de Sweedler para denotar a imagem de um elemento $v \in V$ pela aplicação ρ.

Notação 1.2.6. *Denotamos a imagem de um elemento v pela aplicação ρ por $\rho(v) := v^{-1} \otimes v^0$ e dizemos que ρ é uma coação. Notemos que $v^{-1} \in C$ enquanto que $v^0 \in V$.*

Traduzindo os diagramas em termos de elementos, e utilizando a notação fixada acima, temos que para todo elemento v em um C-comódulo à esquerda V, vale pelo primeiro diagrama que

$$\begin{aligned}
[(Id_C \otimes \rho) \circ \rho](v) &= [(\Delta \otimes Id_V) \circ \rho](v) \\
[Id_C \otimes \rho](\rho(v)) &= [\Delta \otimes Id_V](\rho(v)) \\
[Id_C \otimes \rho](v^{-1} \otimes v^0) &= [\Delta \otimes Id_V](v^{-1} \otimes v^0) \\
Id_C(v^{-1}) \otimes \rho(v^0) &= \Delta(v^{-1}) \otimes Id_V(v^0) \\
v^{-1} \otimes (v^0)^{-1} \otimes (v^0)^0 &= (v^{-1})_1 \otimes (v^{-1})_2 \otimes v^0
\end{aligned}$$

Ou seja, vale a igualdade $v^{-1} \otimes (v^0)^{-1} \otimes (v^0)^0 = (v^{-1})_1 \otimes (v^{-1})_2 \otimes v^0$. Neste caso, generalizamos nossa notação e escrevemos $v^{-2} \otimes v^{-1} \otimes v^0$ para significar tanto $v^{-1} \otimes (v^0)^{-1} \otimes (v^0)^0$ quanto $(v^{-1})_1 \otimes (v^{-1})_2 \otimes v^0$.

Além disso, do segundo diagrama temos que para um elemento qualquer $v \in V$, vale que

$$[(\varepsilon \otimes Id_V) \circ \rho](v) = 1_{\Bbbk} \otimes v.$$

Mas

$$[(\varepsilon \otimes Id_V) \circ \rho](v) = [\varepsilon \otimes Id_V](\rho(v)) = [\varepsilon \otimes Id_V](v^{-1} \otimes v^0) = \varepsilon(v^{-1}) \otimes v^0 = 1_{\Bbbk} \otimes \varepsilon(v^{-1})v^0.$$

Assim, concluímos que para qualquer $v \in V$, vale que $v = \varepsilon(v^{-1})v^0$.

Exemplo 1.2.7. *Toda coálgebra C é um C-comódulo à esquerda via Δ.*

Definição 1.2.8. *Seja V um C-comódulo à esquerda via $\rho : V \longrightarrow C \otimes V$. Um $\Bbbk$-subespaço vetorial W de V é dito um* C-subcomódulo à esquerda *ou simplesmente* subcomódulo *se $\rho(W) \subseteq C \otimes W$.*

Observação 1.2.9. *Note que se W é um C-subcomódulo à esquerda de V, onde V é C-comódulo à esquerda via $\rho : V \longrightarrow C \otimes V$, então W é ele próprio um C-comódulo à esquerda via $\rho_W : W \longrightarrow C \otimes W$ dada por $\rho_W(w) = \rho(w)$ para todo $w \in W$.*

Nosso próximo teorema é conhecido como Teorema Fundamental dos Comódulos, e ele mostra que todo elemento não-nulo de um comódulo pertence a um subcomódulo de dimensão finita. Precisamente, temos:

Teorema 1.2.10. ***(Teorema Fundamental dos Comódulos)*** *Seja V um C-comódulo à esquerda. Qualquer elemento $v \in V$ pertence a um subcomódulo de dimensão finita.*

Demonstração. Seja V um C-comódulo à esquerda via $\rho : V \longrightarrow C \otimes V$ e considere $\{c_i\}_{i \in I}$ uma base de C. Fixando $v \in V$, podemos escrever $\rho(v) = \sum_i c_i \otimes v_i$, onde apenas uma quantidade finita dos v_i's é não-nulo. Considere agora W o $\Bbbk$-subespaço vetorial de V gerado por esses v_i's não-nulos. Note que W tem então dimensão finita. Como $\{c_i\}_{i \in I}$ é uma base de C, temos que $\{c_j \otimes c_k\}_{j,k \in I}$ é uma base para $C \otimes C$. Portanto, para cada i tal que v_i é não-nulo, temos que $\Delta(c_i) = \sum_{j,k} c_j \otimes \alpha^i_{j,k} c_k$, onde apenas uma quantidade finita dos $\alpha^i_{j,k}$'s são não-nulos.

Como V é um C-comódulo à esquerda via ρ, temos que

$$(Id_C \otimes \rho) \circ \rho = (\Delta \otimes Id_V) \circ \rho$$

Assim,

$$\begin{aligned}
[(Id_C \otimes \rho) \circ \rho](v) &= [(\Delta \otimes Id_V) \circ \rho](v) \\
[Id_C \otimes \rho](\rho(v)) &= [\Delta \otimes Id_V](\rho(v)) \\
[(Id_C \otimes \rho)]\left(\sum_i c_i \otimes v_i\right) &= [\Delta \otimes Id_V]\left(\sum_i c_i \otimes v_i\right) \\
\sum_i Id_C(c_i) \otimes \rho(v_i) &= \sum_i \Delta(c_i) \otimes Id_V(v_i) \\
\sum_i c_i \otimes \rho(v_i) &= \sum_{i,j,k} (c_j \otimes \alpha^i_{j,k} c_k) \otimes v_i
\end{aligned}$$

Portanto, aplicando $c_i^* \otimes Id_C \otimes Id_V$ na igualdade acima, para cada i tal que v_i é não-nulo, obtemos que

$$1_\Bbbk \otimes \rho(v_i) = \sum_{j,k} 1_\Bbbk \otimes \alpha^j_{i,k} c_k \otimes v_j = 1_\Bbbk \otimes \left(\sum_{j,k} \alpha^j_{i,k} c_k \otimes v_j\right)$$

Logo, $\rho(v_i) = \sum \alpha^j_{i,k} c_k \otimes v_j$, e com isso $\rho(v_i) \in C \otimes W$. Portanto concluímos que W é um subcomódulo de V, onde W tem dimensão finita.

Agora, só nos resta verificar que v é combinação linear destes v_i's, porque com isso teremos que $v \in W$, concluindo o desejado.

De fato, temos que $[(\varepsilon \otimes Id_V) \circ \rho](v) = 1_{\Bbbk} \otimes v$. Mas temos que

$$\begin{aligned}[(\varepsilon \otimes Id_V) \circ \rho](v) &= [\varepsilon \otimes Id_V](\rho(v)) = [\varepsilon \otimes Id_V](\sum_i c_i \otimes v_i) = \\ &= \sum_i \varepsilon(c_i) \otimes Id_V(v_i) = \sum_i 1_{\Bbbk} \otimes \varepsilon(c_i)v_i = 1_{\Bbbk} \otimes \sum_i \varepsilon(c_i)v_i\end{aligned}$$

Assim $v = \sum_i \varepsilon(c_i)v_i$ e portanto $v \in W$, como queríamos. □

Definição 1.2.11. *Sejam C uma $\Bbbk$-coálgebra, M e N dois C-comódulos à esquerda. Uma aplicação $f : M \longrightarrow N$ é um* homomorfismo de C-comódulos à esquerda *se o seguinte diagrama é comutativo:*

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ {\scriptstyle \rho_M}\downarrow & & \downarrow{\scriptstyle \rho_N} \\ C \otimes M & \xrightarrow[Id_C \otimes f]{} & C \otimes N \end{array}$$

onde $\rho_M : M \longrightarrow C \otimes M$ é a coação de C em M e $\rho_N : N \longrightarrow C \otimes N$ é a coação de C em N. Ou seja, $f : M \longrightarrow N$ é um homomorfismo de C-comódulos à esquerda se vale $\rho_N \circ f = (Id_C \otimes f) \circ \rho_M$.

Em termos de elementos, e utilizando a notação estabelecida, temos que para qualquer $m \in M$, vale $(f(m))^{-1} \otimes (f(m))^0 = m^{-1} \otimes f(m^0)$.

Definição 1.2.12. *Sejam V um $\Bbbk$-espaço vetorial e H uma álgebra de Hopf. Dizemos que V é um* H-módulo de Hopf à esquerda *se:*

(*i*) *V é um H-módulo à esquerda;*

(*ii*) *V é um H-comódulo à esquerda;*

(*iii*) $\rho(h \cdot v) = \sum h_1 v^{-1} \otimes h_2 \cdot v^0$.

Aqui estamos denotando naturalmente a ação de um elemento $h \in H$ em $v \in V$ por $h \cdot v$ e a coação por $\rho : V \longrightarrow H \otimes V$, onde denotamos $\rho(v) := v^{-1} \otimes v^0$. A condição (iii) acima é dita compatibilidade *entre as estruturas de H-módulo e H-comódulo de V.*

Exemplo 1.2.13. *Seja H uma álgebra de Hopf. Então H é um H-módulo de Hopf à esquerda via ação dada pela multiplicação m e coação dada pela comultiplicação Δ.*

O exemplo a seguir será importante para nosso estudo posterior, ele nos dá um exemplo simples de H-módulo de Hopf à esquerda.

Exemplo 1.2.14. *Sejam V um $\Bbbk$-espaço vetorial e H uma álgebra de Hopf.*

Definimos em $H \otimes V$ uma estrutura de H-módulo à esquerda fazendo $h \cdot \sum b \otimes v = \sum hb \otimes v$, para quaisquer $h, b \in H, v \in V$. Esta ação muitas vezes é dita trivial, pois os elementos de H agem somente na primeira posição tensorial de $H \otimes V$, via a multiplicação do próprio H.

Também em $H \otimes V$ definimos uma estrutura de H-comódulo à esquerda via $\rho = \Delta \otimes Id_V$, isto é, $\rho = \Delta \otimes Id_V : H \otimes V \longrightarrow H \otimes H \otimes V$. Notemos que neste caso ficamos com $\rho(h \otimes v) = \sum h_1 \otimes h_2 \otimes v$, para quaisquer $v \in V, h \in H$. Lembre que em nossa notação, ficamos com $\rho(h \otimes v) := (h \otimes v)^{-1} \otimes (h \otimes v)^0$.

Assim, neste caso, temos $(h \otimes v)^{-1} = h_1$ e $(h \otimes v)^0 = h_2 \otimes v$.

Afirmamos agora que $H \otimes V$ com estas estruturas de H-módulo à esquerda e H-comódulo à esquerda é um H-módulo de Hopf à esquerda. Para tal, resta verificarmos apenas a compatibilidade dada pelo item (iii) da Definição 1.2.12.

De fato, sejam $h, b \in H$ e $v \in V$. Então,

$$\begin{aligned} \rho(b \cdot (h \otimes v)) &= \rho(bh \otimes v) = (bh)_1 \otimes (bh)_2 \otimes v = b_1 h_1 \otimes b_2 h_2 \otimes v = \\ &= b_1 h_1 \otimes (b_2 \cdot (h_2 \otimes v)) := b_1 (h \otimes v)^{-1} \otimes b_2 \cdot (h \otimes v)^0. \end{aligned}$$

Veremos logo a frente que este exemplo caracteriza todos os módulos de Hopf, a menos de isomorfismo, isto é, todo H-módulo de Hopf à esquerda é isomorfo como módulo de Hopf a $H \otimes V$, onde $H \otimes V$ é módulo de Hopf como descrito no Exemplo 1.2.14 acima. Além disso, o $\Bbbk$-espaço vetorial V é um espaço vetorial específico do H-módulo de Hopf, a saber o subespaço dos coinvariantes. Este resultado é conhecido como Teorema Fundamental dos Módulos de Hopf. Antes de chegarmos a esse resultado, vejamos duas definições:

Definição 1.2.15. *Sejam V e W dois H-módulos de Hopf à esquerda. Dizemos que $f : V \longrightarrow W$ é um* homomorfismo de H-módulos de Hopf *se:*

(i) *f é um homomorfismo de H-módulos à esquerda;*

(ii) *f é um homomorfismo de H-comódulos à esquerda.*

Definição 1.2.16. *Sejam H uma álgebra de Hopf e M um H-comódulo à esquerda via a aplicação $\rho : M \longrightarrow H \otimes M$. O conjunto*

$$M^{coH} = \{m \in M \quad | \quad \rho(m) = 1_H \otimes m\}$$

é um $\Bbbk$-subespaço vetorial de M que é chamado de subespaço dos coinvariantes de M.

Teorema 1.2.17. ***(Teorema Fundamental dos Módulos de Hopf)*** *Sejam H uma álgebra de Hopf e M um H-módulo de Hopf à esquerda. Então a aplicação $\varphi : H \otimes M^{coH} \longrightarrow M$ dada por $\varphi(h \otimes m) = h \cdot m$ para quaisquer $h \in H, m \in M^{coH}$ é um isomorfismo de H-módulos de Hopf à esquerda.*

Em $H \otimes M^{coH}$ consideramos a estrutura de H-módulo de Hopf à esquerda como dada no Exemplo 1.2.14.

Demonstração. Para provar o teorema, primeiro notemos que o homomorfismo de H-módulos à esquerda φ está bem definido, pois ele é simplesmente a ação de H restrito a um subespaço vetorial de M. Exibiremos agora uma aplicação que será a inversa de φ, o que garantirá a bijeção desta aplicação. Por fim, verificaremos que φ é de fato um homomorfismo de H-módulos de Hopf à esquerda, isto é, φ é um homomorfismo de H-módulos à esquerda e de H-comódulos à esquerda. Assim, concluiremos que φ é um isomorfismo de H-módulos de Hopf à esquerda.

Para a construção da inversa de φ, vamos considerar inicialmente a aplicação $g : M \longrightarrow M$ dada por $g(m) = S(m^{-1}) \cdot m^0$, onde a estrutura de H-comódulo à esquerda de M é dada via $\rho : M \longrightarrow H \otimes M$ e denotada por $\rho(m) := m^{-1} \otimes m^0$, para qualquer $m \in M$.

Vejamos agora que $g(M) \subseteq M^{coH}$. De fato, seja $m \in M$. Temos $\rho(g(m)) = \rho(S(m^{-1}) \cdot m^0)$.

Como M é H-módulo de Hopf, a compatibilidade nos dá que

$$\rho(S(m^{-1}) \cdot m^0) = [S(m^{-1})]_1 (m^0)^{-1} \otimes [S(m^{-1})]_2 \cdot (m^0)^0$$

Como S é um anti-homomorfismo de coálgebras, temos

$$[S(m^{-1})]_1 (m^0)^{-1} \otimes [S(m^{-1})]_2 \cdot (m^0)^0 = S((m^{-1})_2)(m^0)^{-1} \otimes S((m^{-1})_1) \cdot (m^0)^0 \tag{1.6}$$

Do fato de M ser um H-comódulo à esquerda, temos que

$$(Id_H \otimes \rho) \circ \rho = (\Delta \otimes Id_M) \circ \rho$$

ou seja,

$$\begin{aligned}
[(Id_H \otimes \rho) \circ \rho](m) &= [(\Delta \otimes Id_M) \circ \rho](m) \\
[Id_H \otimes \rho](\rho(m)) &= [\Delta \otimes Id_M](\rho(m)) \\
[Id_H \otimes \rho](m^{-1} \otimes m^0) &= [\Delta \otimes Id_M](m^{-1} \otimes m^0) \\
Id_H(m^{-1}) \otimes \rho(m^0) &= \Delta(m^{-1}) \otimes Id_M(m^0) \\
m^{-1} \otimes (m^0)^{-1} \otimes (m^0)^0 &= (m^{-1})_1 \otimes (m^{-1})_2 \otimes m^0
\end{aligned}$$

E aplicando $\Delta \otimes Id_H \otimes Id_M$ nesta última igualdade, obtemos que

$$(m^{-1})_1 \otimes (m^{-1})_2 \otimes (m^0)^{-1} \otimes (m^0)^0 = [(m^{-1})_1]_1 \otimes [(m^{-1})_1]_2 \otimes (m^{-1})_2 \otimes m^0 \tag{1.7}$$

Agora, da estrutura de coálgebra de H, temos que $(Id_H \otimes \Delta) \circ \Delta = (\Delta \otimes Id_H) \circ \Delta$.

Assim, $[[(Id_H \otimes \Delta) \circ \Delta] \otimes Id_M] \circ \rho = [[(\Delta \otimes Id_H) \circ \Delta] \otimes Id_M] \circ \rho$. Logo, para qualquer $m \in M$, temos

$$\begin{aligned}
[[[(Id_H \otimes \Delta) \circ \Delta] \otimes Id_M] \circ \rho](m) &= [[[(\Delta \otimes Id_H) \circ \Delta] \otimes Id_M] \circ \rho](m) \\
[[(Id_H \otimes \Delta) \circ \Delta] \otimes Id_M](\rho(m)) &= [[(\Delta \otimes Id_H) \circ \Delta] \otimes Id_M](\rho(m)) \\
[[(Id_H \otimes \Delta) \circ \Delta] \otimes Id_M](m^{-1} \otimes m^0) &= [[(\Delta \otimes Id_H) \circ \Delta] \otimes Id_M](m^{-1} \otimes m^0) \\
[(Id_H \otimes \Delta) \circ \Delta](m^{-1}) \otimes Id_M(m^0) &= [(\Delta \otimes Id_H) \circ \Delta](m^{-1}) \otimes Id_M(m^0) \\
[Id_H \otimes \Delta](\Delta(m^{-1})) \otimes m^0 &= [\Delta \otimes Id_H](\Delta(m^{-1})) \otimes m^0 \\
[Id_H \otimes \Delta]((m^{-1})_1 \otimes (m^{-1})_2) \otimes m^0 &= (\Delta \otimes Id_H)((m^{-1})_1 \otimes (m^{-1})_2) \otimes m^0 \\
Id_H((m^{-1})_1) \otimes \Delta((m^{-1})_2) \otimes m^0 &= \Delta((m^{-1})_1) \otimes Id_H((m^{-1})_2) \otimes m^0 \\
(m^{-1})_1 \otimes \Delta((m^{-1})_2) \otimes m^0 &= \Delta((m^{-1})_1) \otimes (m^{-1})_2 \otimes m^0 \\
(m^{-1})_1 \otimes ((m^{-1})_2)_1 \otimes ((m^{-1})_2)_2 \otimes m^0 &= ((m^{-1})_1)_1 \otimes ((m^{-1})_1)_2 \otimes (m^{-1})_2 \otimes m^0
\end{aligned}$$

Assim, obtemos que

$$[(m^{-1})_1]_1 \otimes [(m^{-1})_1]_2 \otimes (m^{-1})_2 \otimes m^0 = (m^{-1})_1 \otimes [(m^{-1})_2]_1 \otimes [(m^{-1})_2]_2 \otimes m^0 \tag{1.8}$$

Disto, substituindo (1.8) em (1.7), obtemos que

$$(m^{-1})_1 \otimes (m^{-1})_2 \otimes (m^0)^{-1} \otimes (m^0)^0 = (m^{-1})_1 \otimes [(m^{-1})_2]_1 \otimes [(m^{-1})_2]_2 \otimes m^0 \tag{1.9}$$

Assim, substituindo a igualdade (1.9) em (1.6), obtemos que

$$S((m^{-1})_2)(m^0)^{-1} \otimes S((m^{-1})_1) \cdot (m^0)^0 = S(((m^{-1})_2)_1)((m^{-1})_2)_2 \otimes S((m^{-1})_1) \cdot m^0$$

Agora, segue das propriedades da antípoda e da counidade que

$$\begin{aligned}
S(((m^{-1})_2)_1)((m^{-1})_2)_2 \otimes S((m^{-1})_1) \cdot m^0 &= \varepsilon((m^{-1})_2)1_H \otimes S((m^{-1})_1) \cdot m^0 = \\
= 1_H \otimes S((m^{-1})_1 \varepsilon(m^{-1})_2) \cdot m^0 &= 1_H \otimes S(m^{-1}) \cdot m^0 = 1_H \otimes g(m)
\end{aligned}$$

Logo, $\rho(g(m)) = 1_H \otimes g(m)$, e portanto $g(m) \in M^{coH}$, para qualquer $m \in M$.

Estamos agora aptos a definir a inversa de φ. Seja $\psi : M \longrightarrow H \otimes M^{coH}$ a aplicação dada por $\psi(m) = \sum m^{-1} \otimes g(m^0)$ para qualquer $m \in M$. Já que para qualquer $m \in M$ vale que $g(m) \in M^{coH}$, temos que ψ está bem definida. Precisamos agora verificar que $\psi \circ \varphi = Id_{H \otimes M^{coH}}$ e $\varphi \circ \psi = Id_M$.

De fato, seja $h \otimes m \in H \otimes M^{coH}$. Então

$$[\psi \circ \varphi](h \otimes m) = \psi(\varphi(h \otimes m)) = \psi(h \cdot m) = (h \cdot m)^{-1} \otimes g((h \cdot m)^0)$$

Como M é um H-módulo de Hopf, a compatibilidade nos dá que

$$(h \cdot m)^{-1} \otimes g((h \cdot m)^0) = h_1 m^{-1} \otimes g(h_2 \cdot m^0)$$

Agora, lembre que denotamos $\rho(m) := m^{-1} \otimes m^0$, mas como $m \in M^{coH}$, temos que $\rho(m) = 1_H \otimes m$, ou seja, neste caso $m^{-1} = 1_H$ e $m^0 = m$. Disto, e da definição de g, temos as igualdades

$$h_1 m^{-1} \otimes g(h_2 \cdot m^0) = h_1 \otimes g(h_2 \cdot m) = h_1 \otimes [S((h_2 \cdot m)^{-1}) \cdot ((h_2 \cdot m)^0)]$$

Novamente pela compatibilidade de M, temos que

$$h_1 \otimes [S((h_2 \cdot m)^{-1}) \cdot ((h_2 \cdot m)^0)] = h_1 \otimes [S((h_2)_1 m^{-1}) \cdot ((h_2)_2 \cdot m^0)]$$

donde segue novamente por $m \in M^{coH}$ que $h_1 \otimes [S((h_2)_1 m^{-1}) \cdot ((h_2)_2 \cdot m^0)] = h_1 \otimes [S((h_2)_1) \cdot ((h_2)_2 \cdot m)]$. Agora, utilizando o fato de M ser um H-módulo à esquerda, e também as propriedades da antípoda e da counidade, temos

$$h_1 \otimes [S((h_2)_1) \cdot ((h_2)_2 \cdot m)] = h_1 \otimes [(S((h_2)_1)(h_2)_2) \cdot m] = h_1 \otimes [\varepsilon(h_2) 1_H \cdot m] = h_1 \varepsilon(h_2) \otimes [1_H \cdot m] = h \otimes m.$$

Logo, $\psi \circ \varphi = Id_{H \otimes M^{coH}}$.

Seja agora $m \in M$. Temos que

$$[\varphi \circ \psi](m) = \varphi(\psi(m)) = \varphi(m^{-1} \otimes g(m^0)) = \varphi(m^{-1} \otimes [S((m^0)^{-1}) \cdot (m^0)^0])$$

Como M é H-comódulo à esquerda, temos

$$m^{-1} \otimes (m^0)^{-1} \otimes (m^0)^0 = (m^{-1})_1 \otimes (m^{-1})_2 \otimes m^0$$

donde obtemos que

$$\begin{aligned} &\varphi(m^{-1} \otimes [S((m^0)^{-1}) \cdot (m^0)^0]) = \varphi((m^{-1})_1 \otimes [S((m^{-1})_2) \cdot m^0] = (m^{-1})_1 \cdot [S((m^{-1})_2) \cdot m^0] = \\ &= \quad [(m^{-1})_1 S((m^{-1})_2)] \cdot m^0 = \varepsilon(m^{-1}) 1_H \cdot m^0 = 1_H \cdot (\varepsilon(m^{-1}) m^0) = 1_H \cdot m = m \end{aligned}$$

Logo, $\varphi \circ \psi = Id_M$.

Assim, φ é uma bijeção, e só nos resta mostrar que é um homomorfismo de H-módulos de Hopf à esquerda.

Temos que φ é um homomorfismo de H-módulos à esquerda, pois para quaisquer $b \otimes m \in H \otimes M^{coH}$ e $h \in H$, vale que

$$\varphi(h \cdot (b \otimes m)) = \varphi(hb \otimes m) = (hb) \cdot m = h \cdot (b \cdot m) = h \cdot (\varphi(b \otimes m))$$

Por fim, para provarmos que φ é um homomorfismo de H-comódulos à esquerda, precisamos mostrar que $\rho \circ \varphi = (Id_H \otimes \varphi) \circ (\Delta \otimes Id_{M^{coH}})$. Mas de fato, para qualquer $h \otimes m \in H \otimes M^{coH}$, temos que

$$\begin{aligned} &[(Id_H \otimes \varphi) \circ (\Delta \otimes Id_{M^{coH}})](h \otimes m) = [Id_H \otimes \varphi([\Delta \otimes Id_{M^{coH}}](h \otimes m)) = \\ &= [Id_H \otimes \varphi](\Delta(h) \otimes Id_{M^{coH}}(m)) = [Id_H \otimes \varphi](h_1 \otimes h_2 \otimes m) = \\ &= Id_H(h_1) \otimes \varphi(h_2 \otimes m) = h_1 \otimes (h_2 \cdot m) \end{aligned}$$

Por outro lado, temos $[\rho\circ\varphi](h\otimes m) = \rho(\varphi(h\otimes m)) = \rho(h\cdot m) = (h\cdot m)^{-1}\otimes(h\cdot m)^0$. Pela compatibilidade e pelo fato de $m \in M^{coH}$, temos

$$(h\cdot m)^{-1}\otimes(h\cdot m)^0 = h_1 m^{-1}\otimes(h_2\cdot m^0) = h_1 1_H\otimes(h_2\cdot m) = h_1\otimes(h_2\cdot m)$$

Logo, $\rho\circ\varphi = (Id_H\otimes\varphi)\circ(\Delta\otimes Id_{M^{coH}})$, e concluímos o desejado. □

1.3 O Teorema de Larson-Sweedler

O objetivo desta seção é demonstrar o Teorema de Larson-Sweedler, um resultado importantíssimo sobre álgebras de Hopf de dimensão finita, que mostra que o espaço das integrais tem dimensão 1 e que a antípoda é bijetora.

Definição 1.3.1. *Seja H uma álgebra de Hopf. O conjunto*

$$\int_H^l = \{t\in H \quad | \quad ht = \varepsilon(h)t, \quad \forall h\in H\}$$

é chamado espaço das integrais à esquerda de H. *Analogamente, o conjunto*

$$\int_H^r = \{t\in H \quad | \quad th = \varepsilon(h)t, \quad \forall h\in H\}$$

é chamado espaço das integrais à direita de H.

Observação 1.3.2. *Os conjuntos $\int_H^l$ e $\int_H^r$ são de fato subespaços vetoriais de H, e mais, eles são também ideais bilaterais de H. De fato, sejam $t, b\in\int_H^l, k, h\in H$ e $\alpha\in\Bbbk$. Temos que:*

- $0\in\int_H^l$, *pois* $h0 = 0 = \varepsilon(h)0$;
- $t-b\in\int_H^l$, *pois* $h(t-b) = ht - hb = \varepsilon(h)t - \varepsilon(h)b = \varepsilon(h)(t-b)$;
- $\alpha t\in\int_H^l$, *pois* $h(\alpha t) = (\alpha h)t = \varepsilon(\alpha h)t = (\alpha\varepsilon(h))t = \varepsilon(h)(\alpha t)$.

Os três itens acima provam que $\int_H^l$ é um subespaço vetorial de H. Vejamos agora que $\int_H^l$ é um ideal bilateral de H, e para isto resta verificar que $th\in\int_H^l$ e que $ht\in\int_H^l$, onde $t\in\int_H^l$ e $h\in H$. Temos:

- $th\in\int_H^l$, *pois* $k(th) = (kt)h = (\varepsilon(k)t)h = \varepsilon(k)th$;
- $ht\in\int_H^l$, *pois* $k(ht) = (kh)t = \varepsilon(kh)t = \varepsilon(k)\varepsilon(h)t = \varepsilon(k)(\varepsilon(h)t) = \varepsilon(k)(ht)$.

As contas são análogas para $\int_H^r$.

Lema 1.3.3. *Sejam V um $\Bbbk$-espaço vetorial e $a, b \in V$ tais que $f(a) = f(b)$, para toda $f \in V^*$. Então $a = b$.*

Demonstração. Sejam V um $\Bbbk$-espaço vetorial e $a, b \in V$ tais que $f(a) = f(b)$ para toda $f \in V^*$. Considere $\{v_i\}_{i\in I}$ uma base de V. Então o conjunto $\{v_i^*\}_{i\in I}$ é *l. i.* em V^*.

Podemos supor sem perda de generalidade que $a = \sum_{i=1}^{n} \alpha_i v_i$ e $b = \sum_{i=1}^{n} \beta_i v_i$, onde $\alpha_i, \beta_i \in \Bbbk$, para cada $i = 1, 2, ..., n$.

Assim, para $i = 1, 2, ..., n$, temos $v_i^*(a) = v_i^*(b)$, por hipótese. Assim,

$$\begin{aligned} v_i^*\Big(\sum_{i=1}^{n} \alpha_i v_i\Big) &= v_i^*\Big(\sum_{i=1}^{n} \beta_i v_i\Big) \\ \sum_{i=1}^{n} v_i^*(\alpha_i v_i) &= \sum_{i=1}^{n} v_i^*(\beta_i v_i) \\ \sum_{i=1}^{n} \alpha_i v_i^*(v_i) &= \sum_{i=1}^{n} \beta_i v_i^*(v_i) \\ \alpha_i &= \beta_i \end{aligned}$$

Logo $a = \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} \beta_i v_i = b$. □

Vejamos agora uma proposição que caracteriza elementos integrais na álgebra de Hopf H^*.

Proposição 1.3.4. *Seja H uma álgebra de Hopf de dimensão finita. Então*

$$r \in \int_{H^*}^{l} \iff r(h)1_H = h_1 r(h_2) \tag{1.10}$$

e

$$\sigma \in \int_{H^*}^{r} \iff \sigma(h)1_H = \sigma(h_1)h_2 \tag{1.11}$$

para todo $h \in H$, onde $\Delta(h) = h_1 \otimes h_2$.

Demonstração. Sejam $r \in \int_{H*}^{l}$, $\sigma \in \int_{H*}^{r}$ e $f \in H^*$. Lembremos que o produto em H^* é o produto convolução e que $\varepsilon_{H^*}(f) = f(1_H)$.

Prova de (1.10):

$$\begin{aligned} r \in \int_{H*}^{l} &\iff f * r = \varepsilon_{H^*}(f)r = f(1_H)r, \forall f \in H^* \iff \\ &\iff (f * r)(h) = f(1_H)r(h), \forall f \in H^*, \forall h \in H \iff \\ &\iff f(h_1)r(h_2) = f(1_H)r(h), \forall f \in H^*, \forall h \in H \iff \\ &\iff f(h_1 r(h_2)) = f(1_H r(h)), \forall f \in H^*, \forall h \in H \iff \\ &\iff h_1 r(h_2) = 1_H r(h) = r(h)1_H, \forall h \in H, \end{aligned}$$

onde a última equivalência é garantida pelo Lema 1.3.3.

Analogamente, provamos (1.11):

$$\begin{aligned}
\sigma \in \int_{H*}^{r} &\iff \sigma * f = \varepsilon_{H^*}(f)\sigma = f(1_H)\sigma, \forall f \in H^* \iff \\
&\iff (\sigma * f)(h) = f(1_H)\sigma(h), \forall f \in H^*, \forall h \in H \iff \\
&\iff \sigma(h_1)f(h_2) = f(1_H)\sigma(h), \forall f \in H^*, \forall h \in H \iff \\
&\iff f(\sigma(h_1)h_2) = f(1_H\sigma(h)), \forall f \in H^*, \forall h \in H \iff \\
&\iff \sigma(h_1)h_2 = 1_H\sigma(h) = \sigma(h)1_H, \forall h \in H.
\end{aligned}$$

□

Começaremos agora a construção de uma estrutura de H-módulo de Hopf à esquerda em H^*, onde H é uma álgebra de Hopf de dimensão finita. Tal estrutura será utilizada de forma muito importante na demonstração do Teorema de Larson-Sweedler.

Proposição 1.3.5. *Seja H uma álgebra de Hopf de dimensão finita. Então:*

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

$$\begin{aligned}
\leftharpoonup : H^* \otimes H &\longrightarrow H^* \\
f \otimes h &\mapsto \ \leftharpoonup (f \otimes h) := f \leftharpoonup h
\end{aligned}$$

onde

$$\begin{aligned}
f \leftharpoonup h : H &\longrightarrow \Bbbk \\
k &\mapsto (f \leftharpoonup h)(k) = f(hk)
\end{aligned}$$

Com a ação $\leftharpoonup$ dada no item (i) acima e a antípoda S de H, construímos uma ação de H em H^* à esquerda, conforme abaixo:

(ii) H^* é um H-módulo à esquerda via $\rightharpoonup$:

$$\begin{aligned}
\rightharpoonup : H \otimes H^* &\longrightarrow H^* \\
h \otimes f &\mapsto \ \rightharpoonup (h \otimes f) := h \rightharpoonup f
\end{aligned}$$

onde $h \rightharpoonup f = f \leftharpoonup S(h)$.

Demonstração. Prova de (i):

Para que $\leftharpoonup$ seja uma ação à direita temos que verificar que valem as igualdades $f \leftharpoonup 1_H = f$ e $f \leftharpoonup (hk) = (f \leftharpoonup h) \leftharpoonup k)$. Sejam $h, k, a \in H$ e $f \in H^*$. Temos:

- $(f \leftharpoonup 1_H)(h) = f(1_H h) = f(h)$. Logo, $f \leftharpoonup 1_H = f$.

- Notemos que $[(f \leftharpoonup h) \leftharpoonup k)](a) = (f \leftharpoonup h)(ka) = f(h(ka))$. Por outro lado, temos que $[f \leftharpoonup (hk)](a) = f((hk)a)$. Como $h(ka) = (hk)a$, temos que $f \leftharpoonup (hk) = (f \leftharpoonup h) \leftharpoonup k)$.

Prova de (ii):

Para que $\rightharpoonup$ seja uma ação à esquerda, temos que verificar que valem as igualdades $1_H \rightharpoonup f = f$ e $(hk) \rightharpoonup f = h \rightharpoonup (k \rightharpoonup f)$. Sejam $h, k \in H$ e $f \in H^*$. Já temos que $\leftharpoonup$ é uma ação à direita, então temos:

$$(1_H \rightharpoonup f) = f \leftharpoonup S(1_H) = f \leftharpoonup 1_H = f$$

e portanto $1_H \rightharpoonup f = f$. E também temos:

$$\begin{aligned}(hk) \rightharpoonup f &= f \leftharpoonup S(hk) = f \leftharpoonup (S(k)S(h)) = (f \leftharpoonup S(k)) \leftharpoonup S(h)) = \\ &= (k \rightharpoonup f) \leftharpoonup S(h) = h \rightharpoonup (k \rightharpoonup f)\end{aligned}$$

e portanto $(hk) \rightharpoonup f = h \rightharpoonup (k \rightharpoonup f)$. □

Lema 1.3.6. *Seja H uma álgebra de Hopf de dimensão finita. Então $(H^*)^*$ é isomorfo a H como álgebras de Hopf.*

Demonstração. Sejam H uma álgebra de Hopf de dimensão finita, $\{h_1, ..., h_n\}$ uma base para H sobre $\Bbbk$ e $\{h_1^*, ..., h_n^*\}$ sua base dual.

Definimos $J : H \longrightarrow (H^*)^*$ por $J(h_i) = \widehat{h_i}$, para $i = 1, 2, .., n$, onde $\widehat{h_i} : H^* \longrightarrow \Bbbk$ é dada por $\widehat{h_i}(h_j^*) = \delta_{ij}$, onde δ_{ij} é o *delta de Kronecker*, ou seja, $\widehat{h_i}(h_j^*) = 1_\Bbbk$ se $i = j$ e $\widehat{h_i}(h_j^*) = 0$ caso contrário.

Note que $\widehat{h_i}(f) = f(h_i)$ para qualquer $f \in H^*$, $i = 1, ..., n$. De fato, temos que $f = \sum_{j=1}^n \alpha_j h_j^*$, onde $\alpha_j \in \Bbbk$. Assim,

$$\widehat{h_i}(f) = \widehat{h_i}\Big(\sum_{j=1}^n \alpha_j h_j^*\Big) = \sum_{j=1}^n \widehat{h_i}(\alpha_j h_j^*) = \sum_{j=1}^n \alpha_j \widehat{h_i}(h_j^*) = \alpha_i$$

Por outro lado,

$$f(h_i) = \Big(\sum_{j=1}^n \alpha_j h_j^*\Big)(h_i) = \sum_{j=1}^n (\alpha_j h_j^*)(h_i) = \sum_{j=1}^n \alpha_j (h_j^*(h_i)) = \alpha_i$$

Ou seja, $\widehat{h_i}(f) = \alpha_i = f(h_i)$, onde $f = \sum_{j=1}^n \alpha_j h_j^*$.

Para $h \in H$, denotamos $J(h)$ por $\widehat{h}$. Escrevendo $h = \sum_{i=1}^n \sigma_i h_i$, onde $\sigma_i \in \Bbbk$, temos $J(h) = \sum_{i=1}^n \sigma_i \widehat{h_i} := \widehat{h}$. Temos então que $\widehat{h}(f) = f(h), \forall f \in H^*$. De fato,

$$\widehat{h}(f) = \Big(\sum_{i=1}^n \sigma_i \widehat{h_i}\Big)(f) = \sum_{i=1}^n \sigma_i [\widehat{h_i}(f)] = \sum_{i=1}^n \sigma_i f(h_i) = \sum_{i=1}^n f(\sigma_i h_i) = f\Big(\sum_{i=1}^n \sigma_i h_i\Big) = f(h)$$

Vemos então que J está bem definida. De fato temos $J(h) = \widehat{h} \in (H^*)^*$, para qualquer $h \in H$, e se $h = k$ então $\widehat{h}(f) = f(h) = f(k) = \widehat{k}(f)$, para qualquer $f \in H^*$, ou seja, $J(h) = J(k)$.

Vejamos agora que a aplicação J realiza o isomorfismo entre álgebras de Hopf, isto é, J é homomorfismo de álgebras, é homomorfismo de coálgebras e é bijetora.

Para que J seja homomorfismo de álgebras, temos que verificar dois itens:

- $m_{(H^*)^*} \circ (J \otimes J) = J \circ m_H$. De fato, seja $a \otimes b \in H \otimes H$, temos

  $$[m_{(H^*)^*} \circ J \otimes J](a \otimes b) = m_{(H^*)^*}(J(a) \otimes J(b)) = m_{(H^*)^*}(\widehat{a} \otimes \widehat{b}) = \widehat{a} * \widehat{b}.$$

  Por outro lado, $[J \circ m_H](a \otimes b) = J(ab) = \widehat{ab}$.

  Mas notemos que $\widehat{ab}(f) = f(ab)$ e $(\widehat{a} * \widehat{b})(f) = \widehat{a}(f_1)\widehat{b}(f_2) = f_1(a)f_2(b) = f(ab), \forall f \in H^*$, onde $\Delta_{H^*}(f) = f_1 \otimes f_2$, e a última igualdade vem da Proposição 1.1.24.

  Portanto, $\widehat{ab} = \widehat{a} * \widehat{b}$, e então $m_{(H^*)^*} \circ (J \otimes J) = J \circ m_H$.

- $\widehat{1}_H * f = f, \forall f \in (H^*)^*$. De fato, para $g \in H^*$ temos

  $$[\widehat{1}_H * f](g) = \widehat{1}_H(g_1)f(g_2) = g_1(1_H)f(g_2) = \varepsilon_{H^*}(g_1)f(g_2) = f(\varepsilon_{H^*}(g_1)g_2) = f(g).$$

  Logo, $\widehat{1}_H * f = f$.

Portanto, J é homomorfismo de álgebras.

Para que J seja homomorfismo de coálgebras, temos que verificar dois itens:

- $\Delta_{(H^*)^*} \circ J = (J \otimes J) \circ \Delta_H$. De fato, seja $h \in H$, temos

  $$[\Delta_{(H^*)^*} \circ J](h) = \Delta_{(H^*)^*}(J(h)) = \Delta_{(H^*)^*}(\widehat{h}) = \widehat{h}_1 \otimes \widehat{h}_2.$$

  Por outro lado, $[(J \otimes J) \circ \Delta_H](h) = (J \otimes J)(\Delta_H(h)) = (J \otimes J)(h_1 \otimes h_2) = J(h_1) \otimes J(h_2) = \widehat{h_1} \otimes \widehat{h_2}$.

  Mas notemos que para cada $f \otimes g \in H^* \otimes H^*$, temos

  $$(\widehat{h_1} \otimes \widehat{h_2})(f \otimes g) = \widehat{h_1}(f) \otimes \widehat{h_2}(g) = f(h_1) \otimes g(h_2) = f(h_1)g(h_2) \otimes 1_{\Bbbk} = (f * g)(h) \otimes 1_{\Bbbk} = \widehat{h}(f * g) \otimes 1_{\Bbbk}$$

  Por outro lado,

  $$(\widehat{h}_1 \otimes \widehat{h}_2)(f \otimes g) = \widehat{h}_1(f) \otimes \widehat{h}_2(g) = \widehat{h}_1(f)\widehat{h}_2(g) \otimes 1_{\Bbbk} = \widehat{h}(f * g) \otimes 1_{\Bbbk}$$

  onde $\Delta_{(H^*)^*}(\widehat{h}) = \widehat{h}_1 \otimes \widehat{h}_2$, e a última igualdade também vem da Proposição 1.1.24, já que $(H^*)^*$ é o dual de H^*.

  Logo, $\Delta_{(H^*)^*} \circ J = (J \otimes J) \circ \Delta_H$.

- $\varepsilon_H = \varepsilon_{(H^*)^*} \circ J$. De fato, para $h \in H$ temos

  $$[\varepsilon_{(H^*)^*} \circ J](h) = \varepsilon_{(H^*)^*}(J(h)) = \varepsilon_{(H^*)^*}(\widehat{h}) = \widehat{h}(1_{H^*}) = \widehat{h}(\varepsilon_H) = \varepsilon_H(h)$$

  Logo, $\varepsilon_H = \varepsilon_{(H^*)^*} \circ J$.

Portanto, J é homomorfismo de coálgebras.

Resta apenas verificar que J é uma bijeção.

Provaremos que J é injetora, e como H tem dimensão finita, temos que H^* e $(H^*)^*$ ambos também têm, sendo a mesma de H, e segue então que J é bijetora.

Sejam $a, b \in H$ tais que $J(a) = J(b)$. Temos que $a = \sum_{i=1}^{n} \alpha_i h_i$ e $b = \sum_{i=1}^{n} \beta_i h_i$. Portanto, temos

$$\begin{aligned} J(a) &= J(b) \\ J\Big(\sum_{i=1}^{n} \alpha_i h_i\Big) &= J\Big(\sum_{i=1}^{n} \beta_i h_i\Big) \\ \sum_{i=1}^{n} \alpha_i J(h_i) &= \sum_{i=1}^{n} \beta_i J(h_i) \\ \sum_{i=1}^{n} \alpha_i \widehat{h_i} &= \sum_{i=1}^{n} \beta_i \widehat{h_i} \end{aligned}$$

Assim, para cada $j = 1, ..., n$, temos

$$\begin{aligned} J(a)(h_j^*) &= J(b)(h_j^*) \\ \Big[\sum_{i=1}^{n} \alpha_i \widehat{h_i}\Big](h_j^*) &= \Big[\sum_{i=1}^{n} \beta_i \widehat{h_i}\Big](h_j^*) \\ \sum_{i=1}^{n} \alpha_i h_j^*(h_i) &= \sum_{i=1}^{n} \beta_i h_j^*(h_i) \\ \alpha_j &= \beta_j \end{aligned}$$

Ou seja, $a = \sum_{i=1}^{n} \alpha_i h_i = \sum_{i=1}^{n} \beta_i h_i = b$. Logo, J é injetiva.

Portanto, J é uma bijeção.

Concluímos então que J é um isomorfismo de álgebras de Hopf entre H e $(H^*)^*$. □

Proposição 1.3.7. *Sejam A uma álgebra de dimensão finita e V um $\Bbbk$-espaço vetorial de dimensão finita. Se V é um A-módulo à direita, então V é um A^*-comódulo à esquerda.*

Demonstração. Sejam A uma álgebra de dimensão finita e V um $\Bbbk$-espaço vetorial de dimensão finita. Considere V um A-módulo à direita via a ação $\cdot : V \otimes A \longrightarrow V$. Pela Proposição 1.1.25, temos que A^* é uma coálgebra. Queremos construir uma coação à esquerda de A^* em V, isto é, uma aplicação $\rho : V \longrightarrow A^* \otimes V$.

Considere $\{v_1, v_2, ..., v_n\}$ uma base de V sobre $\Bbbk$. Vejamos que fixando um elemento $v \in V$, para qualquer $a \in A$, obtemos que $v \cdot a \in V$. Assim, temos que $v \cdot a = \sum_{i=1}^{n} \alpha_i v_i$, onde $\alpha_i \in \Bbbk$.

Para este v fixado, definimos então, para cada $i = 1, ..., n$, as aplicações $\alpha_i^v : A \longrightarrow \Bbbk$, dadas por $\alpha_i^v(a) = \alpha_i$, onde $v \cdot a = \sum_{i=1}^{n} \alpha_i v_i$. Ou seja, α_i^v aplicado em um elemento a tem como resultado a i-ésima coordenada da ação de a em v. Notemos que α_i^v está bem definida, já que $\{v_1, v_2, ..., v_n\}$ é

base de V. Precisamente, seja $a = b$. Temos que $\alpha_i^v(a) = \alpha_i$, onde $v \cdot a = \sum_{i=1}^n \alpha_i v_i$, e $\alpha_i^v(b) = \beta_i$, onde $v \cdot b = \sum_{i=1}^n \beta_i v_i$. Desde que $a = b$, temos que $v \cdot a = v \cdot b$, isto é, $\sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n \beta_i v_i$. Já que $\{v_i\}_{i=1}^n$ é base de V, temos que $\alpha_i = \beta_i$. Portanto $\alpha_i^v(a) = \alpha_i^v(b)$. Logo α_i^v está bem definida.

Além disso, α_i^v é $\Bbbk$-linear. De fato, sejam $a, b \in A$ e $\beta \in \Bbbk$. Temos que $\alpha_i^v(a+b) = \alpha_i$, onde $v \cdot (a+b) = \sum_{i=1}^n \alpha_i v_i$, $\alpha_i^v(a) = \alpha_i'$, onde $v \cdot a = \sum_{i=1}^n \alpha_i' v_i$, e $\alpha_i^v(b) = \alpha_i''$, onde $v \cdot b = \sum_{i=1}^n \alpha_i'' v_i$.

Como $\sum_{i=1}^n \alpha_i v_i = v \cdot (a+b) = (v \cdot a) + (v \cdot b) = \sum_{i=1}^n \alpha_i' v_i + \sum_{i=1}^n \alpha_i'' v_i = \sum_{i=1}^n (\alpha' + \alpha_i'') v_i$, obtemos que $\alpha_i = \alpha_i' + \alpha_i''$, ou seja, $\alpha_i^v(a+b) = \alpha_i^v(a) + \alpha_i^v(b)$.

Além disso, $\alpha_i^v(\beta a) = \alpha_i$, onde $v \cdot (\beta a) = \sum_{i=1}^n \alpha_i v_i$, e $\alpha_i^v(a) = \alpha_i'$, onde $v \cdot a = \sum_{i=1}^n \alpha_i' v_i$. Como $\sum_{i=1}^n \alpha_i v_i = v \cdot (\beta a) = \beta(v \cdot a) = \beta(\sum_{i=1}^n \alpha_i' v_i) = \sum_{i=1}^n (\beta \alpha') v_i$, obtemos que $\alpha_i = \beta \alpha_i'$, ou seja, $\alpha_i^v(\beta a) = \beta(\alpha_i^v(a))$.

Com isso, concluímos que $\alpha_i^v \in A^*$. E mais, temos que vale $v \cdot a = \sum_{i=1}^n \alpha_i^v(a) v_i$.

Definimos então nossa coação $\rho : V \longrightarrow A^* \otimes V$ por $\rho(v) = \sum_{i=1}^n \alpha_i^v \otimes v_i$.

Resta verificarmos que de fato ρ é uma coação, isto é, precisamos verificar que valem as igualdades $(Id_{A^*} \otimes \rho) \circ \rho = (\Delta_{A^*} \otimes Id_V) \circ \rho$ e $[(\varepsilon_{A^*} \otimes Id_V) \circ \rho](v) = 1 \otimes v, \forall v \in V$.

Vamos verificar que as igualdades são satisfeitas na base de V.

Notemos inicialmente que, $\alpha_i^{v_j}(1_A) = \alpha_i$ tal que $v_j \cdot 1_A = \sum_{i=1}^n \alpha_i v_i$, donde concluímos que $\alpha_i^{v_j}(1_A) = \delta_{ij}$.

Lembrando que $\varepsilon_{A^*}(f) = f(1_A)$ para qualquer $f \in A^*$, obtemos facilmente a segunda igualdade, já que

$$[(\varepsilon_{A^*} \otimes Id_V) \circ \rho](v_j) = [\varepsilon_{A^*} \otimes Id_V](\rho(v_j)) = [\varepsilon_{A^*} \otimes Id_V] \left(\sum_{i=1}^n \alpha_i^{v_j} \otimes v_i \right) =$$
$$= \sum_{i=1}^n \varepsilon_{A^*}(\alpha_i^{v_j}) \otimes Id_V(v_i) = \sum_{i=1}^n \alpha_i^{v_j}(1_A) \otimes v_j = \sum_{i=1}^n \delta_{ij} \otimes v_j = 1 \otimes v_j$$

Portanto, nos resta agora verificar que $(Id_{A^*} \otimes \rho) \circ \rho = (\Delta_{A^*} \otimes Id_V) \circ \rho$.

Notemos que

$$\begin{aligned} [(Id_{A^*} \otimes \rho) \circ \rho](v_j) &= [Id_{A^*} \otimes \rho] \left(\sum_{i=1}^n \alpha_i^{v_j} \otimes v_i \right) = \sum_{i=1}^n \alpha_i^{v_j} \otimes \rho(v_i) = \\ &= \sum_{i=1}^n \left(\alpha_i^{v_j} \otimes \left(\sum_{k=1}^n \alpha_k^{v_i} \otimes v_k \right) \right) = \sum_{k=1}^n \left(\sum_{i=1}^n \alpha_i^{v_j} \otimes \alpha_k^{v_i} \right) \otimes v_k \end{aligned}$$

Por outro lado,

$$\begin{aligned} [(\Delta_{A^*} \otimes Id_V) \circ \rho](v_j) &= [\Delta_{A^*} \otimes Id_V](\rho(v_j)) = [\Delta_{A^*} \otimes Id_V] \left(\sum_{i=1}^n \alpha_i^{v_j} \otimes v_i \right) = \\ &= \sum_{i=1}^n \Delta_{A^*}(\alpha_i^{v_j}) \otimes Id_V(v_i) = \sum_{k=1}^n \Delta_{A^*}(\alpha_k^{v_j}) \otimes v_k \end{aligned}$$

Assim, é suficiente provarmos que para cada $k \in \{1, ..., n\}$, temos que vale $\Delta_{A^*}(\alpha_k^{v_j}) = \sum_{i=1}^n (\alpha_i^{v_j} \otimes \alpha_k^{v_i})$.

Notemos que, para quaisquer $a, b \in A$, temos que

$$\begin{aligned}(v_j \cdot a) \cdot b &= \left(\sum_{i=1}^n \alpha_i^{v_j}(a) v_i\right) \cdot b = \sum_{i=1}^n [(\alpha_i^{v_j}(a))(v_i \cdot b)] = \sum_{i=1}^n \left[\alpha_i^{v_j}(a) \left(\sum_{k=1}^n \alpha_k^{v_i}(b) v_k\right)\right] = \\ &= \sum_{i=1}^n \left(\sum_{k=1}^n \alpha_i^{v_j}(a)\alpha_k^{v_i}(b) v_k\right) = \sum_{k=1}^n \left(\sum_{i=1}^n \alpha_i^{v_j}(a)\alpha_k^{v_i}(b)\right) v_k\end{aligned}$$

Por outro lado, $v_j \cdot (ab) = \sum_{i=1}^n \alpha_i^{v_j}(ab) v_i = \sum_{k=1}^n \alpha_k^{v_j}(ab) v_k$.

Como $(v_j \cdot a) \cdot b = v_j \cdot (ab)$, temos que para todo $k = 1, ..., n$, vale que $\sum_{i=1}^n [\alpha_i^{v_j}(a)\alpha_k^{v_i}(b)] = \alpha_k^{v_j}(ab)$.

Por fim, notemos que

$$[\Delta_A^*(\alpha_k^{v_j})](a \otimes b) = [(\alpha_k^{v_j})_1](a) \otimes [(\alpha_k^{v_j})_2](b) = ([(\alpha_k^{v_j})_1](a))([(\alpha_k^{v_j})_2](b)) \otimes 1_{\Bbbk} = [\alpha_k^{v_j}](ab) \otimes 1_{\Bbbk}$$

E, por outro lado,

$$\begin{aligned}\left[\sum_{i=1}^n \alpha_i^{v_j} \otimes \alpha_k^{v_i}\right](a \otimes b) &= \sum_{i=1}^n [\alpha_i^{v_j} \otimes \alpha_k^{v_i}](a \otimes b) = \sum_{i=1}^n [\alpha_i^{v_j}(a) \otimes \alpha_k^{v_i}(b)] = \\ &= \sum_{i=1}^n [(\alpha_i^{v_j}(a))(\alpha_k^{v_i}(b)) \otimes 1_{\Bbbk}] = \left(\sum_{i=1}^n \alpha_i^{v_j}(a)\alpha_k^{v_i}(b)\right) \otimes 1_{\Bbbk}\end{aligned}$$

Assim, concluímos que $\sum_{i=1}^n (\alpha_i^{v_j} \otimes \alpha_k^{v_i}) = \Delta_A^*(\alpha_k^{v_j})$, como queríamos.

Logo, ρ é de fato uma coação. □

A proposição acima reflete uma propriedade importante, principalmente quando tratamos de uma álgebra de Hopf de dimensão finita H. Veremos a seguir a construção da coação à esquerda de H em H^* com mais detalhes.

Seja H uma álgebra de Hopf de dimensão finita. Então temos que H^* é um H^*-módulo à direita via a multiplicação usual de H^*, isto é, o produto convolução.

Então, pela Proposição 1.3.7, temos que H^* é um $(H^*)^*$-comódulo à esquerda, e pelo Lema 1.3.6, temos que $H \cong (H^*)^*$ como álgebras de Hopf. Logo H^* é um H-comódulo à esquerda.

Seja $\{\phi_1, ..., \phi_n\}$ uma base de H^*. Sabemos que o produto em H^* é dado pelo produto convolução. Assim, fixando $f \in H^*$, temos que $f * g \in H^*$, para cada $g \in H^*$, e portanto $f * g = \sum_{i=1}^n \alpha_i \phi_i$, com $\alpha_i \in \Bbbk$. Notemos que da mesma forma como foi realizado na prova da Proposição 1.3.7, temos aplicações $\Bbbk$-lineares $\alpha_i^f : H^* \longrightarrow \Bbbk$ que satisfazem $\alpha_i^f(g) = \alpha_i$, onde $f * g = \sum_{i=1}^n \alpha_i \phi_i$. Ou seja, $\alpha_i^f \in (H^*)^*$ e satisfazem $f * g = \sum_{i=1}^n \alpha_i^f(g)\phi_i$.

Agora, como vimos no Lema 1.3.6, H é isomorfo a $(H^*)^*$ via J. Assim, existem $h_1^f, ..., h_n^f \in H$ tais que $J(h_i^f) = \alpha_i^f$, para cada $i = 1, ..., n$, ou seja, $\widehat{h_i^f} = \alpha_i^f$.

Lembre que a coação dada pela Proposição 1.3.7 é

$$\begin{aligned} \rho : H^* &\longrightarrow (H^*)^* \otimes H^* \\ f &\mapsto \sum_{i=1}^{n} \alpha_i^f \otimes \phi_i \end{aligned}$$

Donde temos que $\rho_J = (J^{-1} \otimes Id_{H^*}) \circ \rho$ é coação, onde

$$\begin{aligned} \rho_J : H^* &\longrightarrow H \otimes H^* \\ f &\mapsto \sum_{i=1}^{n} h_i^f \otimes \phi_i \end{aligned}$$

Por fim, note que

$$f * g = \sum_{i=1}^{n} \alpha_i^f(g)\phi_i = \sum_{i=1}^{n} \widehat{h_i^f}(g)\phi_i = \sum_{i=1}^{n} g(h_i^f)\phi_i$$

Portanto, temos que vale a igualdade $f * g = \sum_{i=1}^{n} g(h_i^f)\phi_i$.

Lembre que usualmente denotamos a imagem de uma coação por $\rho_J(f) := f^{-1} \otimes f^0$. Neste caso, denotamos a igualdade $f * g = \sum_{i=1}^{n} g(h_i^f)\phi_i$ por $g(f^{-1})f^0$.

Assim, quando consideramos H^* como um H-comódulo à esquerda via ρ_J, a seguinte igualdade é satisfeita $f * g = g(f^{-1})f^0, \forall g \in H^*$, onde $\rho_J(f) = f^{-1} \otimes f^0$.

Deste ponto em diante, quando considerarmos uma álgebra de Hopf H e nos referirmos a H^* como um H-comódulo à esquerda, denotaremos a coação ρ_J simplesmente por ρ.

Lema 1.3.8. *Seja H uma álgebra de Hopf de dimensão finita. Então H^* é um H-módulo de Hopf à esquerda via $\rightharpoonup$, como dada na Proposição 1.3.5 e ρ como construída acima.*

Demonstração. Lembrando que H^* é um H-módulo à esquerda via $\rightharpoonup$:

$$\begin{aligned} \rightharpoonup : H \otimes H^* &\longrightarrow H^* \\ h \otimes f &\mapsto h \rightharpoonup f = f \leftharpoonup S(h) : H \longrightarrow \Bbbk \\ & \qquad\qquad k \mapsto f(S(h)k) \end{aligned}$$

e H^* é um H-comódulo à esquerda via ρ:

$$\begin{aligned} \rho : H^* &\longrightarrow H \otimes H^* \\ f &\mapsto \sum_{i=1}^{n} r_i^f \otimes \phi_i := f^{-1} \otimes f^0 \end{aligned}$$

onde $\{\phi_1, ..., \phi_n\}$ é base de H^* e $r_1^f, ..., r_n^f$ satisfazem $f * g = \sum_{i=1}^{n} g(r_i^f)\phi_i := g(f^{-1})f^0, \forall g \in H^*$.

Para que H^* seja um H-módulo de Hopf à esquerda, resta somente mostrar a compatibilidade, isto é, $\rho(h \rightharpoonup f) = h_1 f^{-1} \otimes h_2 \rightharpoonup f^0$, onde $\Delta(h) = h_1 \otimes h_2$.

Pela construção dada anteriormente, temos que

$$\rho(h \rightharpoonup f) = h_1 f^{-1} \otimes h_2 \rightharpoonup f^0 \iff (h \rightharpoonup f) * g = g(h_1 f^{-1})(h_2 \rightharpoonup f^0), \forall g \in H^*$$

Notemos que $g(h_1 f^{-1}) \in \Bbbk$ e $h_2 \rightharpoonup f^0 \in H^*$.

Assim, para quaisquer $x \in H$ e $g \in H^*$, temos que

$$\begin{aligned} [g(h_1 f^{-1})(h_2 \rightharpoonup f^0)](x) &= [g(h_1 f^{-1})(f^0 \leftharpoonup S(h_2)](x) = \\ &= g(h_1 f^{-1}) f^0(S(h_2)x) = [g \leftharpoonup h_1](f^{-1}) f^0(S(h_2)x) \end{aligned}$$

Nota que pelo que vimos, para todo $h \in H$, vale que

$$[g \leftharpoonup h](f^{-1}) f^0 = f * (g \leftharpoonup h)$$

Donde seguimos com

$$\begin{aligned} [g \leftharpoonup h_1](f^{-1}) f^0(S(h_2)x) &= [f * (g \leftharpoonup h_1)](S(h_2)x) = \\ &= f([S(h_2)x]_1)[g \leftharpoonup h_1]([S(h_2)x]_2) = \\ &= f([S(h_2)]_1 x_1)[g \leftharpoonup h_1]([S(h_2)]_2 x_2) = \\ &= f(S((h_2)_2)x_1)[g \leftharpoonup h_1](S((h_2)_1)x_2) = \\ &= f(S(h_2)x_1)[g \leftharpoonup (h_1)_1](S((h_1)_2)x_2) = \\ &= f(S(h_2)x_1) g((h_1)_1 S((h_1)_2)x_2) = \\ &= f(S(h_2)x_1) g(\varepsilon(h_1) 1_H x_2) = \\ &= f(S(\varepsilon(h_1)h_2)x_1) g(1_H x_2) = f(S(h)x_1) g(x_2) \end{aligned}$$

Por outro lado, temos que

$$[(h \rightharpoonup f) * g](x) = [h \rightharpoonup f](x_1) g(x_2) = [f \leftharpoonup S(h)](x_1) g(x_2) = f(S(h)x_1) g(x_2)$$

Logo, $(h \rightharpoonup f) * g = g(h_1 f^{-1})(h_2 \rightharpoonup f^0)$, donde concluímos que vale a compatibilidade. □

Estamos agora aptos a provar o resultado principal desta seção.

Teorema 1.3.9. ***(Teorema de Larson-Sweedler)*** *Seja H uma álgebra de Hopf de dimensão finita. Então:*

(*i*) $\dim_{\Bbbk}(\int_H^r) = 1$;

(*ii*) *S é bijetora;*

(*iii*) $S(\int_H^l) = \int_H^r$;

(*iv*) $\dim_{\Bbbk}(\int_H^l) = 1$.

Demonstração. Prova de (i):

Seja H uma álgebra de Hopf de dimensão n. Considere H^* com estrutura de H-módulo de Hopf à esquerda via $\rightharpoonup$ e ρ como no Lema 1.3.8.

Pelo Teorema Fundamental dos Módulos de Hopf à esquerda 1.2.17, temos $H^* \cong H \otimes (H^*)^{coH}$ como H-módulos de Hopf à esquerda.

Lembremos que $(H^*)^{coH} = \{f \in H^* \quad | \quad \rho(f) = 1_H \otimes f\}$, e também que se denotarmos $\rho(f) := f^{-1} \otimes f^0$, a igualdade $f * g = g(f^{-1})f^0$ é satisfeita para toda $g \in H^*$.

Como $\dim_{\Bbbk}(H) = n = \dim_{\Bbbk}(H^*)$, temos

$$n = \dim_{\Bbbk}(H^*) = \dim_{\Bbbk}(H \otimes (H^*)^{coH}) = \dim_{\Bbbk}(H)\dim_{\Bbbk}((H^*)^{coH}) = n\dim_{\Bbbk}((H^*)^{coH}),$$

donde concluímos que $\dim_{\Bbbk}((H^*)^{coH}) = 1$.

Agora, note que

$$\begin{aligned}
f \in (H^*)^{coH} &\iff \rho(f) := f^{-1} \otimes f^0 = 1_H \otimes f \iff \\
&\iff f * g = g(f^{-1})f^0 = g(1_H)f, \forall g \in H^* \iff \\
&\iff f(h_1)g(h_2) = g(1_H)f(h), \forall g \in H^*, h \in H \iff \\
&\iff g(f(h_1)h_2) = g(f(h)1_H), \forall g \in H^*, h \in H \iff \\
&\iff f(h_1)h_2 = f(h)1_H, \forall h \in H \iff \\
&\iff f \in \int_{H^*}^r
\end{aligned}$$

onde a última equivalência vem da Proposição 1.3.4.

Assim, como espaços vetoriais temos que $(H^*)^{coH} = \int_{H^*}^r$.

Portanto $\dim_{\Bbbk}(\int_{H^*}^r) = \dim_{\Bbbk}((H^*)^{coH}) = 1$.

Agora, considerando inicialmente a álgebra de Hopf $B = H^*$, pelo mesmo argumento concluímos que $\dim_{\Bbbk}(\int_{B^*}^r) = 1$, isto é, $\dim_{\Bbbk}(\int_{(H^*)^*}^r) = 1$. Como $(H^*)^* \cong H$ como álgebra de Hopf pelo Lema 1.3.6, temos que $\dim_{\Bbbk}(\int_H^r) = 1$.

Prova de (ii):

Note inicialmente que pelo item (i), temos que $(H^*)^{coH} = \int_{H^*}^r$ como $\Bbbk$-espaços vetoriais, donde temos que $H \otimes (H^*)^{coH} = H \otimes \int_{H^*}^r$ como módulos de Hopf à esquerda, onde a estrutura de módulo de Hopf à esquerda em ambos é dada como no Exemplo 1.2.14.

Pelo Teorema Fundamental dos Módulos de Hopf à esquerda 1.2.17, temos que $H \otimes (H^*)^{coH} \cong H^*$ como H-módulos de Hopf à esquerda, ou seja, $H \otimes \int_{H^*}^r \cong H^*$ como H-módulos de Hopf à esquerda, via $\varphi : H \otimes \int_{H^*}^r \longrightarrow H^*$ dada por $\varphi(h \otimes \lambda) = h \rightharpoonup \lambda$, para quaisquer $\lambda \in \int_{H^*}^r \subseteq H^*$ e $h \in H$.

Como $\dim_{\Bbbk}(\int_{H^*}^r) = 1$, temos que existe $\sigma \in \int_{H^*}^r, \sigma \neq 0$. Fixemos tal elemento não-nulo σ.

Vamos agora mostrar que $S : H \longrightarrow H$ é injetiva, donde seguirá que S é bijeção, pois H tem dimensão finita. De fato, seja $h \in \ker(S)$, isto é, $S(h) = 0$. Vamos mostrar que $h = 0$.

Note que para qualquer $k \in H$, temos que

$$[\varphi(h \otimes \sigma)](k) = [h \rightharpoonup \sigma](k) = [\sigma \leftharpoonup S(h)](k) = \sigma(S(h)k) = \sigma(0k) = \sigma(0) = 0$$

Assim, $k \in \ker(h \rightharpoonup \sigma)$. Como $k \in H$ é qualquer, temos que $\ker(h \rightharpoonup \sigma) = H$.

Desta maneira, $(h \rightharpoonup \sigma)(k) = 0, \forall k \in H$, e segue que $h \rightharpoonup \sigma = \bar{0}$, onde $\bar{0}$ é o homomorfismo nulo.

Temos então que $\varphi(h \otimes \sigma) = (h \rightharpoonup \sigma) = \bar{0}$. Como φ é um isomorfismo, temos que $h \otimes \sigma = 0$. Como $\sigma \neq 0$ e o produto tensorial está sobre o corpo $\Bbbk$, concluímos que $h = 0$.

Portanto, S é injetiva, e o resultado segue.

Prova de (iii):

Já temos pelo item (ii) que S é bijeção, donde existe S^{-1} tal que $S \circ S^{-1} = S^{-1} \circ S = Id_H$.

Seja $h \in \int_H^l$. Para qualquer $k \in H$, utilizando as propriedades dadas em 1.1.21, temos:

$$\begin{aligned} S(h)k &= S(h)Id_H(k) = S(h)S(S^{-1}(k)) = S(S^{-1}(k)h) = \\ &= S(\varepsilon(S^{-1}(k))h) = S(\varepsilon(k)h) = \varepsilon(k)S(h) \end{aligned}$$

Assim, $S(h) \in \int_H^r$, e temos que

$$S\left(\int_H^l\right) \subseteq \int_H^r \tag{1.12}$$

Por outro lado, seja $h \in \int_H^r$. Analogamente, para qualquer $k \in H$, temos

$$\begin{aligned} kS^{-1}(h) &= Id_H(k)S^{-1}(h) = S^{-1}(S(k))S^{-1}(h) = S^{-1}(hS(k)) = \\ &= S^{-1}(\varepsilon(S(k))h) = S^{-1}(\varepsilon(k)h) = \varepsilon(k)S^{-1}(h) \end{aligned}$$

Assim, $S^{-1}(h) \in \int_H^l$, e com isso $h = S(S^{-1}(h)) \in S(\int_H^l)$. Portanto,

$$\int_H^r \subseteq S\left(\int_H^l\right) \tag{1.13}$$

Das contenções 1.12 e 1.13 temos a igualdade $\int_H^r = S(\int_H^l)$.

Prova de (iv):

Este item segue diretamente dos itens anteriores. De fato, pelo item (i), temos que $\dim_{\Bbbk}(\int_H^r) = 1$, e pelo item (iii) temos que $S(\int_H^l) = \int_H^r$. Agora, pelo item (ii) temos que S é bijetora, donde concluímos que $\dim_{\Bbbk}(\int_H^l) = \dim_{\Bbbk}(S(\int_H^l)) = \dim_{\Bbbk}(\int_H^r) = 1$. □

Vamos provar agora o último resultado desta seção, que mostra que $H \cong H^*$ como H-módulos à esquerda, quando H é uma álgebra de Hopf de dimensão finita.

Consideremos então H uma álgebra de Hopf de dimensão finita.

Tome H como um H-módulo à esquerda via multiplicação de H, e H^* como um H-módulo à esquerda via ação $\rightharpoonup$ dada no item (ii) da Proposição 1.3.5. Lembremos que $\rightharpoonup$: $H \otimes H^* \longrightarrow H^*$ é dada por $\rightharpoonup (h \otimes f) := h \rightharpoonup f = f \leftharpoonup S(h)$, onde $f \leftharpoonup S(h) : H \longrightarrow \Bbbk$ é dada por $[f \leftharpoonup S(h)](k) = f(S(h)k)$, para qualquer $k \in H$.

Como H é uma álgebra de Hopf de dimensão finita, temos que H^* também é uma álgebra de Hopf, e também de dimensão finita, portanto, segue do item (i) do Teorema de Larson-Sweedler 1.3.9, que o $\Bbbk$-espaço vetorial $\int_{H^*}^r$ tem dimensão 1, ou seja, existem elementos não-nulos em $\int_{H^*}^r$.

Temos então o seguinte resultado:

Teorema 1.3.10. *Seja H uma álgebra de Hopf de dimensão finita. Para cada $\lambda \in \int_{H^*}^r$, $\lambda \neq 0$, temos que a aplicação $\varphi_\lambda : H \longrightarrow H^*$ dada por $\varphi_\lambda(h) = h \rightharpoonup \lambda = \lambda \leftharpoonup S(h)$, para todo $h \in H$, é um isomorfismo de H-módulos à esquerda.*

Demonstração. Seja $\lambda \in \int_{H^*}^r$, $\lambda \neq 0$. Pela Proposição 1.3.5, temos que $\rightharpoonup$ é uma ação de H em H^* pela esquerda, donde segue que φ_λ é um homomorfismo de H-módulos à esquerda. De fato, para todo $h, k \in H$, temos:

- $\underline{\varphi_\lambda(h+k) = \varphi_\lambda(h) + \varphi_\lambda(k) :}$

  $\varphi_\lambda(h+k) = (h+k) \rightharpoonup \lambda = (h \rightharpoonup \lambda) + (k \rightharpoonup \lambda) = \varphi_\lambda(h) + \varphi_\lambda(k)$

- $\underline{\varphi_\lambda(h \cdot k) = h \rightharpoonup \varphi_\lambda(k) :}$

  $\varphi_\lambda(h \cdot k) = \varphi_\lambda(hk) = (hk) \rightharpoonup \lambda = h \rightharpoonup (k \rightharpoonup \lambda) = h \rightharpoonup \varphi_\lambda(k)$

Agora, resta provarmos que φ_λ é uma bijeção.

Pelo item (ii) do Teorema de Larson-Sweedler 1.3.9, temos que S é bijetora e, além disso, durante a prova deste item vimos que $H \otimes \int_{H^*}^r \cong H^*$ como H-módulos de Hopf à esquerda, via $\varphi : H \otimes \int_{H^*}^r \longrightarrow H^*$ dada por $\varphi(h \otimes \lambda) = h \rightharpoonup \lambda = \lambda \leftharpoonup S(h)$, para quaisquer $\lambda \in \int_{H^*}^r \subseteq H^*, h \in H$, e onde a ação $\leftharpoonup$ de H em H^* pela direita é dada conforme o item (i) da Proposição 1.3.5.

Assim, temos:

- $\underline{\varphi_\lambda \text{ é injetora:}}$

  Sejam $h, k \in H$ tais que $\varphi_\lambda(h) = \varphi_\lambda(k)$. Temos então as seguintes equivalências:

$$\begin{aligned} \varphi_\lambda(h) &= \varphi_\lambda(k) \\ h \rightharpoonup \lambda &= k \rightharpoonup \lambda \\ \varphi(h \otimes \lambda) &= \varphi(k \otimes \lambda) \end{aligned}$$

Desde que φ é um isomorfismo, temos que $h \otimes \lambda = k \otimes \lambda$, e portanto temos $h \otimes \lambda - k \otimes \lambda = 0$, ou seja, $(h-k) \otimes \lambda = 0$. Como o produto tensorial está sobre o corpo $\Bbbk$, e $\lambda \neq 0$, temos que $h - k = 0$, e segue que $h = k$.

Logo, φ_λ é injetora.

- φ_λ é sobrejetora:

  Como H tem dimensão finita, segue que H^* também tem dimensão finita e é a mesma de H, e temos que $\varphi_\lambda : H \longrightarrow H^*$ injetora, onde H e H^* tem a mesma dimensão. Segue portanto que φ_λ é também sobrejetora.

Portanto, concluímos que para cada $\lambda \in \int_{H^*}^r$, $\lambda \neq 0$, a aplicação φ_λ é um isomorfismo de H-módulos à esquerda. □

1.4 Injetividade

Nesta seção mostramos que toda álgebra de Hopf de dimensão finita é um H-módulo injetivo. Para alcançar este objetivo, retomamos o estudo da teoria de módulos, nos orientando principalmente pelas referências [7] e [17], onde veremos um pouco sobre módulos injetivos, para que ao final concluamos o desejado desta seção.

Primeiramente, queremos definir um A-módulo à esquerda injetivo. Para isso, veremos um teorema que garante equivalência entre três propriedades para um A-módulo à esquerda. De posse deste teorema, definiremos então como sendo um A-módulo à esquerda injetivo um módulo que satisfaz essas propriedades. Observamos que a definição de um A-módulo à direita injetivo é feito de forma análoga.

Antes de enunciarmos o teorema que caracteriza módulos injetivos, vejamos alguns resultados preliminares que irão facilitar a prova do referido teorema:

Definição 1.4.1. *Dizemos que uma sequência exata curta de A-módulos à esquerda*

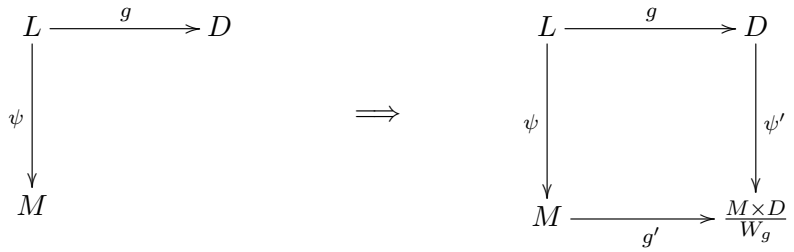
$$0 \longrightarrow M \xrightarrow{i} N \xrightarrow{j} L \longrightarrow 0$$

cinde *se existe um homomorfismo A-linear $p : N \longrightarrow M$ tal que $p \circ i = Id_M$.*

Lema 1.4.2. *Sejam $\psi : L \longrightarrow M$ e $g : L \longrightarrow D$ dois homomorfismos de A-módulos à esquerda. Então existem homomorfismos $\psi' : D \longrightarrow \frac{M \times D}{W_g}$ e $g' : M \longrightarrow \frac{M \times D}{W_g}$ que satisfazem $g' \circ \psi = \psi' \circ g$, onde $W_g = \{(\psi(x), -g(x)) \,|x \in L\}$ é submódulo de $M \times D$.*

Além disso, se ψ é injetor, então ψ' também é.

Em outras palavras, o lema acima diz que sempre podemos estender o primeiro diagrama abaixo ao segundo, que comuta.



E mais, se $0 \longrightarrow L \xrightarrow{\psi} M$ é exata, então também é $0 \longrightarrow D \xrightarrow{\psi'} \frac{M\times D}{W_g}$.

Demonstração. Sejam $\psi : L \longrightarrow M$ e $g : L \longrightarrow D$ dois homomorfismos de A-módulos à esquerda. Definimos $\psi' : D \longrightarrow \frac{M\times D}{W_g}$ por $\psi'(d) = (0, d) + W_g$ e $g' : M \longrightarrow \frac{M\times D}{W_g}$ por $g'(m) = (m, 0) + W_g$. Temos que ψ' e g' são homomorfismos de A-módulos à esquerda.

Vamos apenas verificar que $g' \circ \psi = \psi' \circ g$.

Seja $l \in L$. Então temos que $(g' \circ \psi)(l) = g'(\psi(l)) = (\psi(l), 0) + W_g$.

Por outro lado, temos que $(\psi' \circ g)(l) = \psi'(g(l)) = (0, g(l)) + W_g$.

Desde que $(\psi(l), 0) - (0, g(l)) = (\psi(l), -g(l)) \in W_g$, temos que $(\psi(l), 0) + W_g = (0, g(l)) + W_g$.

Logo, $[g' \circ \psi](l) = [\psi' \circ g](l)$. Como $l \in L$ foi qualquer, temos que $g' \circ \psi = \psi' \circ g$.

Além disso, temos que se ψ for injetora, então ψ' também é. De fato, sejam $d_1, d_2 \in D$ tais que $\psi'(d_1) = \psi'(d_2)$. Então $\psi'(d_1 - d_2) = 0 + W_g$, ou seja, $(0, d_1 - d_2) \in W_g$. Assim, existe $l \in L$ tal que $(0, d_1 - d_2) = (\psi(l), -g(l))$. Desta maneira, $\psi(l) = 0$ e $d_1 - d_2 = -g(l)$. Como ψ é injetora, temos que $l = 0$. Portanto $g(l) = g(0) = 0$.

Logo, temos $d_1 = d_2$, e concluímos que ψ' é injetora. □

Lema 1.4.3. *Seja*

$$L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

uma sequência exata de A-módulos à esquerda. Então para qualquer A-módulo à esquerda X, a sequência

$$0 \longrightarrow Hom_A(N, X) \xrightarrow{\varphi^*} Hom_A(M, X) \xrightarrow{\psi^*} Hom_A(L, X)$$

é uma sequência exata de grupos abelianos, onde

$$\psi^*(g) = g \circ \psi \qquad e \qquad \varphi^*(f) = f \circ \varphi$$

para quaisquer $g \in Hom_A(M, X)$ e $f \in Hom_A(N, X)$.

Demonstração. Suponhamos que

$$L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

seja uma sequência exata de A-módulos à esquerda. Queremos provar que para qualquer A-módulo à esquerda X, a sequência

$$0 \longrightarrow Hom_A(N, X) \xrightarrow{\varphi^*} Hom_A(M, X) \xrightarrow{\psi^*} Hom_A(L, X) \tag{1.14}$$

é uma sequência exata de grupos abelianos, onde

$$\psi^*(g) = g \circ \psi \qquad \text{e} \qquad \varphi^*(f) = f \circ \varphi$$

para quaisquer $g \in Hom_A(M, X)$ e $f \in Hom_A(N, X)$.

Para isso, precisamos verificar apenas dois itens:

(i) φ^* é injetora:

Seja $f \in \ker(\varphi^*)$. Então $\varphi^*(f) = 0$, isto é, $f \circ \varphi = 0$. Queremos mostrar que $f : N \longrightarrow X$ é o homomorfismo nulo. Como φ é sobrejetora, para todo $n \in N$, existe $m_n \in M$ tal que $n = \varphi(m_n)$. Assim, para qualquer $n \in N$, temos que $f(n) = f(\varphi(m_n)) = [f \circ \varphi](m_n) = 0(m_n) = 0$. Logo, f é o homomorfismo nulo, e portanto φ^* é injetora.

(ii) $im(\varphi^*) = \ker(\psi^*)$:

Seja $g \in im(\varphi^*)$. Então existe $f \in Hom_A(N, X)$ tal que $\varphi^*(f) = g$. Queremos mostrar que $g \in \ker(\psi^*)$, ou seja, que $\psi^*(g) = 0$. Como a sequência da hipótese é exata, temos que $\varphi \circ \psi = 0$. Assim, temos que $\psi^*(g) = g \circ \psi = \varphi^*(f) \circ \psi = (f \circ \varphi) \circ \psi = f \circ (\varphi \circ \psi) = f \circ 0 = 0$.

Logo, $im(\varphi^*) \subseteq \ker(\psi^*)$.

Reciprocamente, seja $g \in \ker(\psi^*)$. Então $\psi^*(g) = 0$, donde segue que $g \circ \psi = 0$. Vamos construir uma $f \in Hom_A(N, X)$ tal que $\varphi^*(f) = g$. Desde que, por hipótese, $\varphi : M \longrightarrow N$ é sobrejetora, temos que para cada $n \in N$, existe um $m_n \in M$ tal que $\varphi(m_n) = n$. Definimos então a aplicação $f : N \longrightarrow X$ por $f(n) = g(m_n)$, onde $m_n \in M$ é tal que $\varphi(m_n) = n$. Como para cada $n \in N$ existe $m_n \in M$ tal que $\varphi(m_n) = n$ e $g : M \longrightarrow X$, temos que a aplicação f faz sentido. Resta verificar que está bem definida, e então que satisfaz $\varphi^*(f) = g$. Para verificar que f está bem definida, precisamos verificar que se m_1 e m_2 são tais que $\varphi(m_1) = \varphi(m_2) = n$, então $g(m_1) = g(m_2)$.

Suponhamos então que $\varphi(m_1) = \varphi(m_2)$. Então $m_1 - m_2 \in \ker(\varphi)$. Como a sequência da hipótese é exata, temos que $\ker(\varphi) = im(\psi)$. Assim, existe $l \in L$ tal que $\psi(l) = m_1 - m_2$. Desta maneira, $g(\psi(l)) = g(m_1 - m_2)$, e portanto $[g \circ \psi](l) = g(m_1) - g(m_2)$. Como $g \circ \psi = 0$, temos que $0 = g(m_1) - g(m_2)$, ou seja, $g(m_1) = g(m_2)$, como queríamos.

Além disso, como $f(n) = g(m_n)$, temos que f é A-linear. Logo, $f \in Hom_A(N, X)$. Por fim, notamos que para qualquer $m \in M$, temos que $\varphi(m) \in N$, e vale $f(\varphi(m)) = g(m)$. Portanto $f \circ \varphi = g$.

Logo, $\ker(\psi^*) \subseteq im(\varphi^*)$.

Com isso, concluímos que $\ker(\psi^*) = im(\varphi^*)$.

Pelos itens (i) e (ii) acima, concluímos que a sequência de grupos abelianos dada em (1.14) é exata. $\square$

Vejamos agora o teorema que caracteriza os módulos injetivos, e na sequência sua definição.

Teorema 1.4.4. *Sejam A um anel com 1_A e D um A-módulo à esquerda qualquer fixado. Sejam M, L e N A-módulos à esquerda e $\varphi : M \longrightarrow N$, $\psi : L \longrightarrow M$ homomorfismos de A-módulos à esquerda. São equivalentes:*

(i) *Para toda sequência exata curta de A-módulos à esquerda*

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

a sequência

$$0 \longrightarrow Hom_A(N, D) \xrightarrow{\varphi^*} Hom_A(M, D) \xrightarrow{\psi^*} Hom_A(L, D) \longrightarrow 0$$

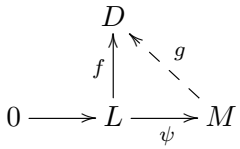
é uma sequência exata curta de grupos abelianos, onde

$$\psi^*(f) = f \circ \psi \qquad e \qquad \varphi^*(g) = g \circ \varphi$$

para quaisquer $f \in Hom_A(M, D)$ e $g \in Hom_A(N, D)$.

(ii) *Para qualquer homomorfismo de A-módulos à esquerda injetor $\psi : L \longrightarrow M$, temos que o homomorfismo de grupos abelianos $\psi^* : Hom_A(M, D) \longrightarrow Hom_A(L, D)$ é sobrejetor, onde $\psi^*(f) = f \circ \psi, \forall f \in Hom_A(M, D)$. Isto é, para toda $h \in Hom_A(L, D)$, existe $g \in Hom_A(M, D)$ tal que $\psi^*(g) = h$.*

Em outras palavras, o seguinte diagrama comuta:



(iii) *Para quaisquer A-módulos à esquerda M e N, temos que se*

$$0 \longrightarrow D \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

é uma sequência exata curta de A-módulos à esquerda, então ela cinde.

Demonstração. $[(i) \Longrightarrow (ii)]$ Seja $\psi : L \longrightarrow M$ um homomorfismo de A-módulos à esquerda injetor. Então temos que

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\pi} M/im(\psi) \longrightarrow 0$$

é uma sequência exata curta de A-módulos à esquerda. Portanto, pelo item (i), temos que

$$0 \longrightarrow Hom_A(M/im(\psi), D) \xrightarrow{\pi^*} Hom_A(M, D) \xrightarrow{\psi^*} Hom_A(L, D) \longrightarrow 0$$

é uma sequência exata curta de grupos abelianos, donde segue que $\psi^* : Hom_A(M, D) \longrightarrow Hom_A(L, D)$ é sobrejetor.

$[(ii) \Longrightarrow (iii)]$ Suponhamos que

$$0 \longrightarrow D \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

é uma sequência exata curta de A-módulos à esquerda. Temos então que $f : D \longrightarrow M$ é injetora. Assim, pelo item (ii), temos que a aplicação $f^* : Hom_A(M, D) \longrightarrow Hom_A(D, D)$ é sobrejetora. Como $Id_D \in Hom_A(D, D)$, temos que existe $p : M \longrightarrow D$ tal que $f^*(p) = Id_D$, ou seja, $p \circ f = Id_D$. Logo, temos que a sequência dada cinde.

$[(iii) \Longrightarrow (i)]$ Suponhamos que

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0 \tag{1.15}$$

seja uma sequência exata curta de A-módulos à esquerda.

Queremos provar que

$$0 \longrightarrow Hom_A(N, D) \xrightarrow{\varphi^*} Hom_A(M, D) \xrightarrow{\psi^*} Hom_A(L, D) \longrightarrow 0 \tag{1.16}$$

é uma sequência exata curta de grupos abelianos, onde

$$\psi^*(f) = f \circ \psi \qquad \text{e} \qquad \varphi^*(g) = g \circ \varphi$$

para quaisquer $f \in Hom_A(M, D)$ e $g \in Hom_A(N, D)$.

Observamos inicialmente que, pelo Lema 1.4.3, para provar que a sequência (1.16) é uma sequência exata curta de grupos abelianos, resta verificarmos que ψ^* é sobrejetora. Seja $g \in Hom_A(L, D)$. Queremos mostrar que existe $f \in Hom_A(M, D)$ tal que $\psi^*(f) = g$, isto é, $f \circ \psi = g$. Desde que ψ é injetora, pelo Lema 1.4.2, existem aplicações A-lineares $\psi' : D \longrightarrow \frac{M \times D}{W_g}$ e $g' : M \longrightarrow \frac{M \times D}{W_g}$, com ψ' injetora, tais que o seguinte diagrama comuta

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ L & \xrightarrow{g} & D \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi'} \\ M & \xrightarrow{g'} & \frac{M \times D}{W_g} \end{array}$$

onde $W_g = \{(\psi(x), -g(x)) \,|\, x \in L\}$ é submódulo de $M \times D$. Assim, $g' \circ \psi = \psi' \circ g$.

Notemos então que

$$0 \longrightarrow D \xrightarrow{\psi'} \frac{M \times D}{W_g} \xrightarrow{\pi} \frac{\frac{M\times D}{W_g}}{\psi'(D)} \longrightarrow 0$$

é uma sequência exata curta de A-módulos à esquerda. Portanto, pela hipótese (iii), temos que ela cinde, isto é, existe um homomorfismo A-linear $h : \frac{M\times D}{W_g} \longrightarrow D$ que satisfaz $h \circ \psi' = Id_D$.

Definimos então $f : M \longrightarrow D$ por $f = h \circ g'$. Resta verificarmos que $\psi^*(f) = g$. Mas de fato,

$$\psi^*(f) = f \circ \psi = (h \circ g') \circ \psi = h \circ (g' \circ \psi) = h \circ (\psi' \circ g) = (h \circ \psi') \circ g = Id_D \circ g = g$$

Portanto, a sequência (1.16) é uma sequência exata curta de grupos abelianos. □

Definição 1.4.5. *Dizemos que D é um A-módulo à esquerda injetivo se D satisfaz uma, e portanto todas, das condições equivalentes do* Teorema 1.4.4 *acima.*

Exemplo 1.4.6. *Qualquer $\Bbbk$-espaço vetorial V é injetivo.*

De fato, suponhamos que V é um $\Bbbk$-espaço vetorial e que

$$0 \longrightarrow V \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

é uma sequência exata curta de $\Bbbk$-espaços vetoriais.

Consideramos então $\{v_i\}_{i\in I}$ uma base de V sobre $\Bbbk$. Como f é injetora, $\{f(v_i)\}_{i\in I}$ é um conjunto l.i. *em M, e então podemos estender este conjunto a uma base de M, digamos que $\{f(v_i)\}_{i\in I} \bigcup \{w_j\}_{j\in J}$ seja esta base. Assim, definimos a aplicação $\Bbbk$-linear $h : M \longrightarrow V$ na base por $h(f(v_i)) = v_i$ e $h(w_j) = 0$, e estendemos linearmente.*

Temos que h é uma aplicação $\Bbbk$-linear e vale que $h \circ f = Id_V$. Logo, a sequência exata dada cinde.

Segue portanto da condição (iii) do Teorema 1.4.4 *que V é injetivo como $\Bbbk$-espaço vetorial.*

Observação 1.4.7. *Vimos pelo exemplo anterior que todo $\Bbbk$-espaço vetorial V é injetivo. Segue então que pela condição (i) do* Teorema 1.4.4*, que para qualquer $\Bbbk$-espaço vetorial V, se a sequência*

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

é uma sequência exata curta de $\Bbbk$-módulos à esquerda, isto é, de $\Bbbk$-espaços vetoriais, então

$$0 \longrightarrow Hom_{\Bbbk}(N, V) \xrightarrow{\varphi^*} Hom_{\Bbbk}(M, V) \xrightarrow{\psi^*} Hom_{\Bbbk}(L, V) \longrightarrow 0$$

é uma sequência exata curta de grupos abelianos, onde $\psi^*(f) = f \circ \psi, \forall f \in Hom_{\Bbbk}(M, D)$ e $\varphi^*(g) = g \circ \varphi, \forall g \in Hom_{\Bbbk}(N, D)$.

O Teorema 1.4.4 reflete uma propriedade muito interessante dos módulos injetivos, que enunciaremos como o seguinte corolário:

Corolário 1.4.8. *Se D é submódulo de um A-módulo M, então D ser injetivo significa que D é um somando direto de M.*

Demonstração. Suponha que D é um A-submódulo de M e que D é injetivo como A-módulo. Note que a inclusão $\iota : D \longrightarrow M$ é um homomorfismo de A-módulos à esquerda injetor. Então temos que a sequência

$$0 \longrightarrow D \xrightarrow{\iota} M \xrightarrow{\pi} M/D \longrightarrow 0$$

é uma sequência exata curta de A-módulos à esquerda. Como D é injetivo, pelo item (iii) do Teorema 1.4.4, esta sequência cinde. Seja $p : M \longrightarrow D$ o homomorfismo tal que $p \circ \iota = Id_D$.

Afirmamos agora que $M = D \oplus \ker(p)$. De fato, temos que $D, \ker(p) \subseteq M$, logo $D + \ker(p) \subseteq M$. Vamos verificar agora que $M \subseteq D + \ker(p)$. Considere $x \in M$. Assim, temos que $p(x) \in D$. Desde que $p(x) \in D$, temos que $[\iota \circ p](x) = \iota(p(x)) = p(x) \in D$. Disto, obtemos que valem as igualdades $p(x) = Id_D(p(x)) = [Id_D \circ p](x) = [p \circ \iota \circ p](x) = p([\iota \circ p](x))$. Com isso, temos que, $x - [\iota \circ p](x) \in \ker(p)$. Assim, $x = [x - [\iota \circ p](x)] + [\iota \circ p](x)$, onde $[\iota \circ p](x) \in D$ e $x - [\iota \circ p](x) \in \ker(p)$. Logo, $x \in \ker(p) + D$. Por último, seja $z \in D \cap \ker(p)$. Assim, $z \in D$ e $z \in \ker(p)$. Do fato de $z \in D$, temos que $z = \iota(z)$, e do fato de $z \in \ker(p)$, temos que $p(z) = 0$. Consequentemente, $0 = p(z) = p(\iota(z)) = (p \circ \iota)(z) = Id_D(z) = z$, ou seja, $z = 0$. Logo, $D \cap \ker(p) = \{0\}$.

Com isso concluímos que D é um somando direto de M, como queríamos. □

Observação 1.4.9. *Seja A uma $\Bbbk$-álgebra. Para qualquer $\Bbbk$-espaço vetorial V, temos que $Hom_{\Bbbk}(A, V)$ é um A-módulo à esquerda, via*

$$(a \cdot f)(x) = f(xa), \quad \forall f \in Hom_{\Bbbk}(A, V), \quad \forall a, x \in A.$$

No que segue, denotaremos por $\tilde{V}$ o A-módulo à esquerda $Hom_{\Bbbk}(A, V)$, onde a estrutura de A-módulo é dada na observação acima.

Lema 1.4.10. *Sejam A uma álgebra sobre $\Bbbk$ e V um $\Bbbk$-espaço vetorial. Então para qualquer A-módulo à esquerda M, temos que*

$$Hom_A(M, \tilde{V}) \cong Hom_{\Bbbk}(A \otimes_A M, V)$$

como $\Bbbk$-espaços vetoriais.

Demonstração. Inicialmente, vemos que pela Observação 1.4.9, $\tilde{V} := Hom_{\Bbbk}(A, V)$ é um A-módulo à esquerda, donde segue que $Hom_A(M, \tilde{V})$ é um $\Bbbk$-espaço vetorial.

Para cada $f \in Hom_{\Bbbk}(A \otimes_A M, V)$, temos que $f : A \otimes_A M \longrightarrow V$ é $\Bbbk$-linear. Assim, para cada $m \in M$, definimos $f_m : A \longrightarrow V$ por $f_m(a) = f(a \otimes m)$. Notemos que $f_m(a) = f(a \otimes m) \in V$ e portanto f_m está bem definida. Claramente, f_m é uma aplicação $\Bbbk$-linear. De fato, para quaisquer $a, b \in A$ e

$\alpha \in \Bbbk$, temos que $f_m(a+b) = f((a+b)\otimes m) = f(a\otimes m + b\otimes m) = f(a\otimes m) + f(b\otimes m) = f_m(a) + f_m(b)$ e $f_m(\alpha a) = f(\alpha a \otimes m) = f(\alpha(a\otimes m)) = \alpha f(a\otimes m) = \alpha f_m(a)$. Assim, $f_m \in Hom_{\Bbbk}(A, V)$.

Com isso, definimos $\psi_f : M \longrightarrow Hom_{\Bbbk}(A,V) = \tilde{V}$ por $\psi_f(m) = f_m$. Afirmamos que ψ_f é A-linear. De fato, para quaisquer $m, n \in M$ e $a, x \in A$, temos que

$$\begin{aligned}[\psi_f(m+n)](x) &= f_{m+n}(x) = f(x\otimes(m+n)) = f(x\otimes m + x\otimes n) = f(x\otimes m) + f(x\otimes n) = \\ &= f_m(x) + f_n(x) = (f_m + f_n)(x) = (\psi_f(m) + \psi_f(n))(x)\end{aligned}$$

Logo, $\psi_f(m+n) = \psi_f(m) + \psi_f(n)$. E também temos que $\psi_f(a\cdot m) = a\cdot\psi_f(m)$. De fato, temos que $[\psi_f(a\cdot m)](x) = f_{a\cdot m}(x) = f(x\otimes a\cdot m)$. Por outro lado, $[a\cdot\psi_f(m)](x) = [\psi_f(m)](xa) = f(xa\otimes m)$. Desde que $xa\otimes m = x\otimes a\cdot m$, concluímos que $\psi_f(a\cdot m) = a\cdot\psi_f(m)$. Assim, $\psi_f \in Hom_A(M,\tilde{V})$.

Portanto, temos que está bem definida a aplicação $\psi : Hom_{\Bbbk}(A\otimes_A M, V) \longrightarrow Hom_A(M,\tilde{V})$ dada por $\psi(f) = \psi_f$. Além disso, temos que esta aplicação é $\Bbbk$-linear. De fato, para quaisquer $f, g \in Hom_{\Bbbk}(A\otimes_A M, V)$ e $\alpha \in \Bbbk$, temos que $\psi(f+g) = \psi_{f+g}$. Assim, para qualquer $m \in M$, temos que $\psi_{f+g}(m) = (f+g)_m$, e segue que para qualquer $a \in A$, temos que

$$[(f+g)_m](a) = [f+g](a\otimes m) = f(a\otimes m) + g(a\otimes m) = f_m(a) + g_m(a) = [f_m + g_m](a)$$

Portanto $(f+g)_m = f_m + g_m$, e consequentemente $[\psi_{f+g}](m) = [\psi_f + \psi_g](m)$. Logo $\psi_{f+g} = \psi_f + \psi_g$, ou seja, $\psi(f+g) = \psi(f) + \psi(g)$. Além disso, afirmamos que também vale $\psi(\alpha f) = \alpha\psi_f$. De fato, temos que $\psi(\alpha f) = \psi_{\alpha f}$, e como para qualquer $m \in M$, vale que $\psi_{\alpha f}(m) = (\alpha f)_m$, segue que para qualquer $a \in A$, temos que $[(\alpha f)_m](a) = [\alpha f](a\otimes m) = f(\alpha a\otimes m) = f(a\otimes \alpha m) = f_{\alpha m}(a)$. Portanto $(\alpha f)_m = f_{\alpha m}$, e assim, vale que $[\psi_{\alpha f}](m) = [\psi_f](\alpha m) = [\alpha\psi_f](m)$, e com isso temos que $\psi_{\alpha f} = \alpha\psi_f$, ou seja, $\psi(\alpha f) = \alpha\psi(f)$.

Agora, para mostrar que ψ é um isomorfismo, apresentamos sua inversa.

Se $g : M \longrightarrow Hom_{\Bbbk}(A,V) = \tilde{V}$ é A-linear, definimos então $g' : A\otimes_A M \longrightarrow V$ por $g'(a\otimes m) = g_m(a)$, onde denotamos por g_m a imagem de m pela aplicação g, isto é, $g_m := g(m)$.

Temos que g' está bem definida e é $\Bbbk$-linear.

Assim, podemos definir $\phi : Hom_A(M,\tilde{V}) \longrightarrow Hom_{\Bbbk}(A\otimes_A M, V)$ dada por $\phi(g) = g'$.

Por fim, notemos que ϕ é a inversa de ψ, isto é: $\psi\circ\phi = Id_{Hom_A(M,\tilde{V})}$ e $\phi\circ\psi = Id_{Hom_{\Bbbk}(A\otimes_A M,V)}$.

De fato, seja $f \in Hom_A(M,\tilde{V})$. Então, para qualquer $m \in M$ e $a \in A$, temos que

$$\begin{aligned}[[[\psi\circ\phi](f)](m)](a) &= [[\psi(\phi(f))](m)](a) = [[\psi(f')](m)](a) = [\psi_{f'}(m)](a) = \\ &= [f'_m](a) = f(a\otimes m) = f_m(a) = [f(m)](a),\end{aligned}$$

ou seja, $[\psi\circ\phi](f) = f$. Logo, $\psi\circ\phi = Id_{Hom_A(M,\tilde{V})}$.

Por outro lado, seja $g \in Hom_{\Bbbk}(A \otimes_A M, V)$. Então, para qualquer $a \otimes m \in A \otimes_A M$, temos que

$$\begin{aligned}[[\phi \circ \psi](g)](a \otimes m) &= [\phi(\psi(g))](a \otimes m) = [\phi(\psi_g)](a \otimes m) = [(\psi_g)'](a \otimes m) = \\ &= [(\psi_g)_m](a) = [(\psi_g)(m)](a) = g_m(a) = g(a \otimes m),\end{aligned}$$

ou seja, $[\phi \circ \psi](g) = g$. Logo, $\phi \circ \psi = Id_{Hom_{\Bbbk}(A \otimes_A M, V)}$.

Portanto ψ é um isomorfismo $\Bbbk$-linear. □

Teorema 1.4.11. *Sejam A uma $\Bbbk$-álgebra e V um $\Bbbk$-espaço vetorial. Então $\tilde{V} = Hom_{\Bbbk}(A, V)$ é um A-módulo à esquerda injetivo.*

Demonstração. Vamos provar que o A-módulo à esquerda $\tilde{V} = Hom_{\Bbbk}(A, V)$ satisfaz a condição (i) do Teorema 1.4.4. Seja então

$$0 \longrightarrow L \xrightarrow{\psi} T \xrightarrow{\varphi} N \longrightarrow 0 \tag{1.17}$$

uma sequência exata curta de A-módulos à esquerda.

Queremos mostrar que

$$0 \longrightarrow Hom_A(N, \tilde{V}) \xrightarrow{\varphi^*} Hom_A(T, \tilde{V}) \xrightarrow{\psi^*} Hom_A(L, \tilde{V}) \longrightarrow 0$$

é uma sequência exata curta de grupos abelianos, onde $\psi^*(f) = f \circ \psi, \forall f \in Hom_A(T, \tilde{M})$ e $\varphi^*(g) = g \circ \varphi, \forall g \in Hom_A(N, \tilde{M})$.

Desde que $A \otimes_A X \cong X$ como A-módulo à esquerda, para qualquer A-módulo à esquerda X, obtemos da sequência exata curta (1.17), que a sequência

$$0 \longrightarrow A \otimes_A L \xrightarrow{Id_A \otimes \psi} A \otimes_A T \xrightarrow{Id_A \otimes \varphi} A \otimes_A N \longrightarrow 0 \tag{1.18}$$

é uma sequência exata curta de A-módulos à esquerda. Em particular, a sequência (1.18) é uma sequência exata curta de $\Bbbk$-espaços vetoriais.

Assim, pela Observação 1.4.7, temos que

$$0 \longrightarrow Hom_{\Bbbk}(A \otimes_A N, V) \xrightarrow{(Id_A \otimes \varphi)^*} Hom_{\Bbbk}(A \otimes_A T, V) \xrightarrow{(Id_A \otimes \psi)^*} Hom_{\Bbbk}(A \otimes_A L, V) \longrightarrow 0$$

é uma sequência exata curta de grupos abelianos.

Agora, pelo Lema 1.4.10, temos que $Hom_{\Bbbk}(A \otimes_A X, V) \cong Hom_A(X, \tilde{V})$ como $\Bbbk$-espaços vetoriais, e em particular como grupos abelianos, para todo A-módulo à esquerda X. Assim, substituindo $Hom_{\Bbbk}(A \otimes_A X, V)$ pelo $\Bbbk$-espaço vetorial isomorfo $Hom_A(X, \tilde{V})$, para $X = L, T$ e N, concluímos que a sequência

$$0 \longrightarrow Hom_A(N, \tilde{V}) \xrightarrow{\varphi^*} Hom_A(T, \tilde{V}) \xrightarrow{\psi^*} Hom_A(L, \tilde{V}) \longrightarrow 0$$

é uma sequência exata curta de grupos abelianos.

Logo, a sequência (1.18) é uma sequência exata curta de grupos abelianos, como queríamos, e portanto, $\tilde{V}$ é um A-módulo à esquerda injetivo. □

Corolário 1.4.12. *Seja A uma $\Bbbk$-álgebra. Então $A^* = Hom_{\Bbbk}(A, \Bbbk)$ é um A-módulo à esquerda injetivo.*

Demonstração. Imediatamente do teorema anterior, tomando $V = \Bbbk$. □

Para concluir esta seção, e também este capítulo, vejamos o principal resultado desta seção, que juntamente com o Teorema de Krull-Schmidt, será importante para a demonstração das proposições do próximo, e principal, capítulo desta dissertação.

Teorema 1.4.13. *Seja H uma álgebra de Hopf de dimensão finita. Então H é um H-módulo à esquerda injetivo.*

Demonstração. Pelo corolário anterior, temos que H^* é um H-módulo à esquerda injetivo. Agora, pelo Teorema 1.3.10, temos que $H^* \cong H$ como H-módulos à esquerda. Portanto que H é injetivo como H-módulo à esquerda. □

Capítulo 2

O Teorema de Nichols-Zöeller

Neste capítulo provaremos o principal resultado desta dissertação, o Teorema de Nichols-Zöeller. Este é um teorema muito interessante e estende o bem conhecido Teorema de Lagrange para grupos finitos para o caso de álgebras de Hopf de dimensão finita.

2.1 Preliminares

Começamos esta seção enunciando o clássico Teorema de Krull-Schmidt:

Teorema de Krull-Schmidt *Todo módulo $M \neq \{0\}$ de comprimento finito tem uma decomposição em soma direta de submódulos*

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r \qquad (D)$$

onde cada M_i é um submódulo indecomponível de M, para $i = 1, 2, ..., r$. Além disso, essa decomposição é única a menos de isomorfismo, isto é, se tivermos também

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_s \qquad (D')$$

onde cada N_j é um submódulo indecomponível de M, para $j = 1, 2, ..., s$, então $r = s$ e, reindexando os índices se necessário, nós temos $M_i \cong N_i$, para cada $i = 1, 2, ..., r$.

Uma decomposição para o módulo M como dada em (D) é dita uma *decomposição de Krull-Schmidt*.

A prova do teorema é feita com todos os detalhes no apêndice. Vejamos no restante desta seção alguns resultados preliminares que nos serão úteis para a prova do Teorema de Nichols-Zöeller.

Definição 2.1.1. *Dizemos que o A-módulo M é A-*fiel*, ou simplesmente* fiel*, se $ann_A(M) = \{0\}$.*

Se M e W são dois B-módulos à esquerda, onde B é uma álgebra de Hopf, então $M \otimes W$ é um

B-módulo à esquerda via a ação

$$b \cdot (m \otimes w) = b_1 m \otimes b_2 w$$

para quaisquer $m \in M$, $w \in W$ e $b \in B$, com $\Delta(b) = b_1 \otimes b_2$.

De fato, para quaisquer $b, h \in B$ e $m \otimes w, m' \otimes w' \in M \otimes W$ temos:

- $1_B \cdot m \otimes w = (1_B)_1 m \otimes (1_B)_2 w = 1_B m \otimes 1_B w = m \otimes w$;
- $b \cdot (h \cdot m \otimes w) = b \cdot (h_1 m \otimes h_2 w) = b_1(h_1 m) \otimes b_2(h_2 w) = (b_1 h_1)m \otimes (b_2 h_2)w = (bh)_1 m \otimes (bh)_2 w = (bh) \cdot m \otimes w$.

Quando M e W forem dois B-módulos à esquerda, onde B é uma álgebra de Hopf, sempre consideraremos $M \otimes W$ com estrutura de B-módulo à esquerda via Δ, como na observação acima. Um caso particularmente interessante é quando algum dos B-módulos, M ou W, for o próprio B, como veremos mais adiante.

Lema 2.1.2. *Sejam B uma álgebra de Hopf e W um B-módulo à esquerda. Considere $B \otimes W$ um B-comódulo à esquerda via $\rho = \Delta \otimes Id_W$. Então $(B \otimes W)^{coB} = 1 \otimes W$.*

Demonstração. Seja B uma álgebra de Hopf e W um B-módulo à esquerda. Em particular, W é um $\Bbbk$-espaço vetorial. Temos então que $B \otimes W$ é um B-comódulo à esquerda via ρ, onde $\rho = \Delta \otimes Id_W$, como no Exemplo 1.2.14.

Com essa estrutura, temos:

$$\begin{aligned} (B \otimes W)^{coB} &= \{b \otimes w \in B \otimes W \mid \rho(b \otimes w) = 1 \otimes b \otimes w\} = \\ &= \{b \otimes w \in B \otimes W \mid b_1 \otimes b_2 \otimes w = 1 \otimes b \otimes w\} \end{aligned}$$

Vamos mostrar então que neste caso $(B \otimes W)^{coB} = 1 \otimes W$. De fato, vejamos:

$\underline{1 \otimes W \subseteq (B \otimes W)^{coB}:}$

Seja $\sum_{i=1}^n 1 \otimes w_i \in 1 \otimes W$. Note que $\sum_{i=1}^n 1 \otimes w_i = 1 \otimes (\sum_{i=1}^n w_i) = 1 \otimes w$, para $w = (\sum_{i=1}^n w_i)$. Logo, um elemento qualquer de $1 \otimes W$ é da forma $1 \otimes w$, com $w \in W$.

Assim,

$$\rho(1 \otimes w) = [\Delta \otimes Id_W](1 \otimes w) = \Delta(1) \otimes Id_W(w) = 1 \otimes 1 \otimes w$$

Logo, $1 \otimes w \in (B \otimes W)^{coB}$ e vale $1 \otimes W \subseteq (B \otimes W)^{coB}$.

$\underline{(B \otimes W)^{coB} \subseteq 1 \otimes W:}$

Notemos que um elemento qualquer de $B \otimes W$ é da forma $\sum_{i=1}^n b_i \otimes w_i$. Além disso, podemos supor sem perda de generalidade que $\{w_i\}_{i=1}^n$ é um conjunto *l. i.* sobre $\Bbbk$. Com isso, temos que $\{w_i^*\}_{i=1}^n$

é um conjunto *l. i.* sobre $\Bbbk$ em W^*, e que satisfaz $w_i^*(w_j) = \delta_{i,j}$, onde $\delta_{i,j} = 1$, se $i = j$ e 0 caso contrário.

Seja $b \otimes w \in (B \otimes W)^{coB}$. Então,

$$\begin{aligned}
\rho(b \otimes w) &= 1 \otimes b \otimes w \\
\rho\left(\sum_{i=1}^{n} b_i \otimes w_i\right) &= 1 \otimes \left(\sum_{i=1}^{n} b_i \otimes w_i\right) \\
[\Delta \otimes Id_W]\left(\sum_{i=1}^{n} b_i \otimes w_i\right) &= \left(\sum_{i=1}^{n} 1 \otimes b_i \otimes w_i\right) \\
\left(\sum_{i=1}^{n} \Delta(b_i) \otimes w_i\right) &= \left(\sum_{i=1}^{n} 1 \otimes b_i \otimes w_i\right) \\
\left(\sum_{i=1}^{n} (b_i)_1 \otimes (b_i)_2 \otimes w_i\right) &= \left(\sum_{i=1}^{n} 1 \otimes b_i \otimes w_i\right)
\end{aligned}$$

Assim, fixando $j \in \{1, ..., n\}$, e aplicando $Id_B \otimes Id_B \otimes w_j^*$, temos que

$$[Id_B \otimes Id_B \otimes w_j^*]\left(\sum_{i=1}^{n} (b_i)_1 \otimes (b_i)_2 \otimes w_i\right) = [Id_B \otimes Id_B \otimes w_j^*]\left(\sum_{i=1}^{n} 1 \otimes b_i \otimes w_i\right)$$

e portanto temos

$$\begin{aligned}
\sum_{i=1}^{n} (b_i)_1 \otimes (b_i)_2 \otimes w_j^*(w_i) &= \sum_{i=1}^{n} 1 \otimes b_i \otimes w_j^*(w_i) \\
(b_i)_1 \otimes (b_i)_2 \otimes 1_{\Bbbk} &= 1 \otimes b_i \otimes 1_{\Bbbk}
\end{aligned}$$

donde segue pelo isomorfismo canônico que $(b_j)_1 \otimes (b_j)_2 = 1 \otimes b_j$.

Agora, aplicando $Id_B \otimes \varepsilon$ na última igualdade obtida, obtemos que $(b_j)_1 \otimes \varepsilon((b_j)_2) = 1 \otimes \varepsilon(b_j)$, e segue novamente pelo isomorfismo canônico que $(b_j)_1\varepsilon((b_j)_2) = 1\varepsilon(b_j)$. Desde que $(b_j)_1\varepsilon((b_j)_2) = b_j$, concluímos que, para cada $j = 1, ..., n$, temos $b_j = 1\varepsilon(b_j)$.

Assim, $b \otimes w = \sum_{i=1}^{n} b_i \otimes w_i = \sum_{i=1}^{n} 1\varepsilon(b_i) \otimes w_i = \sum_{i=1}^{n} 1 \otimes \varepsilon(b_i)w_i \in 1 \otimes W$.

Logo, concluímos que $1 \otimes W = (B \otimes W)^{coB}$, como queríamos. □

Teorema 2.1.3. *Sejam B uma álgebra de Hopf de dimensão finita e W um B-módulo à esquerda. Então $B \otimes W \cong W \otimes B \cong B^{\dim_{\Bbbk}(W)}$ como B-módulos à esquerda.*

Demonstração. Iremos provar o teorema em 3 passos. Primeiramente vamos mostrar que $B \otimes W$ é um B-módulo de Hopf à esquerda. Em seguida, provaremos que $B \otimes W \cong B^{\dim_{\Bbbk}(W)}$, e, por fim provaremos que $B^{\dim_{\Bbbk}(W)} \cong W \otimes B$.

Passo 1: $B \otimes W$ é um B-módulo de Hopf à esquerda.

Notemos que $B \otimes W$ é um B-módulo à esquerda com a ação dada por

$$h \cdot (b \otimes w) = h_1 b \otimes h_2 w, \qquad \forall w \in W \text{ e } h, b \in B, \text{ com } \Delta(h) = h_1 \otimes h_2,$$

e é também B-comódulo à esquerda com coação $\rho : B \otimes W \longrightarrow B \otimes (B \otimes W)$ dada por

$$\rho(b \otimes w) = b_1 \otimes (b_2 \otimes w) := (b \otimes w)^{-1} \otimes (b \otimes w)^0.$$

Para concluirmos então que $B \otimes W$ é um B-módulo de Hopf à esquerda, resta verificar a compatibilidade entre as duas estruturas, isto é:

$$\rho(h \cdot (b \otimes w)) = h_1(b \otimes w)^{-1} \otimes h_2 \cdot (b \otimes w)^0,$$

ou seja,

$$\rho(h \cdot (b \otimes w)) = h_1 b_1 \otimes h_2 \cdot (b_2 \otimes w).$$

Notemos que:

$$\begin{aligned} \rho(h \cdot (b \otimes w)) &= \rho(h_1 b \otimes h_2 w) = (h_1 b)_1 \otimes (h_1 b)_2 \otimes h_2 w = (h_1)_1 b_1 \otimes (h_1)_2 b_2 \otimes h_2 w = \\ &= h_1 b_1 \otimes h_2 b_2 \otimes h_3 w = h_1 b_1 \otimes (h_2)_1 b_2 \otimes (h_2)_2 w = h_1 b_1 \otimes h_2 \cdot (b_2 \otimes w) \end{aligned}$$

Portanto vale a compatibilidade, e assim $B \otimes W$ é um B-módulo de Hopf à esquerda.

Passo 2: $B \otimes W \cong B^{\dim_{\Bbbk}(W)}$ como B-módulos à esquerda.

Como $B \otimes W$ é um B-módulo de Hopf à esquerda, temos pelo Teorema Fundamental dos Módulos de Hopf à esquerda 1.2.17 que $B \otimes W \cong B \otimes (B \otimes W)^{coB}$ como B-módulos de Hopf, e então, em particular, este é um isomorfismo de B-módulos, onde $B \otimes (B \otimes W)^{coB}$ é um B-módulo à esquerda com ação trivial, isto é, B age na primeira componente tensorial de $B \otimes (B \otimes W)^{coB}$, como no exemplo 1.2.14.

Vimos no Lema 2.1.2 que $(B \otimes W)^{coB} = 1 \otimes W$.

Como a ação de B em $B \otimes (B \otimes W)^{coB}$ é dada somente na primeira componente tensorial, temos que $B \otimes (B \otimes W)^{coB} = B \otimes 1 \otimes W$ como B-módulos, e portanto $B \otimes 1 \otimes W \cong B \otimes W$ como B-módulos, onde a ação de B neste último também é a ação trivial.

Quando a ação em $B \otimes W$ é trivial, isto é, B age somente no primeiro componente tensorial, temos $B \otimes W \cong B^{\dim_{\Bbbk}(W)}$ como B-módulos. Assim, concluímos que

$$B \otimes W \cong B \otimes (B \otimes W)^{coB} = B \otimes 1 \otimes W \cong B \otimes W \cong B^{\dim_{\Bbbk}(W)}$$

onde todos os isomorfismos são de B-módulos.

Note que na linha de isomorfismos acima, o primeiro módulo é um B-módulo com ação dada pelo Δ, o último módulo é um B-módulo via ditributividade do produto de B em cada componente de $B^{\dim_{\Bbbk}(W)}$, enquanto que os demais são B-módulos de forma trivial, isto é, B age somente na primeira componente tensorial de cada módulo, que é o próprio B, via produto usual. Assim, $B \otimes W \cong B^{\dim_{\Bbbk}(W)}$ e isto conclui a segunda parte.

Passo 3: $B^{\dim_{\Bbbk}(W)} \cong W \otimes B$ como B-módulos à esquerda.

Como B é uma álgebra de Hopf de dimensão finita, temos pelo item (ii) do Teorema de Larson-Sweedler 1.3.9 que a antípoda S é bijetora. Assim, podemos considerar a álgebra de Hopf B^{cop}, que é uma álgebra de Hopf com a mesma multiplicação, unidade e counidade de B, mas com antípoda dada por S^{-1} e a comultiplicação $\Delta_{cop} : B \longrightarrow B \otimes B$ dada por $\Delta_{cop}(b) = b_2 \otimes b_1$, onde $\Delta(b) = b_1 \otimes b_2$, conforme o Exemplo 1.1.22.

Como $B = B^{cop}$ como $\Bbbk$-álgebra, temos que W é um B^{cop}-módulo à esquerda e podemos considerar $B^{cop} \otimes W$ como B^{cop}-módulo à esquerda via Δ_{cop}. Explicitamente, a estrutura de B^{cop}-módulo à esquerda de $B^{cop} \otimes W$ é dada por $h \cdot (b \otimes w) = h_2 b \otimes h_1 w$, onde $\Delta(h) = h_1 \otimes h_2$ e disto segue que $\Delta_{cop}(h) = h_2 \otimes h_1$.

Segue então, pelo **passo 2** acima, que $B^{cop} \otimes W \cong (B^{cop})^{\dim_{\Bbbk}(W)}$ como B^{cop}-módulos.

Novamente, pelo fato de $B = B^{cop}$ como $\Bbbk$-álgebra, concluímos que $B = B^{cop}$ como B-módulo à esquerda, e portanto $B^{\dim_{\Bbbk}(W)} = (B^{cop})^{\dim_{\Bbbk}(W)}$ como B-módulo à esquerda. Além disso, temos que $B^{cop} \otimes W$ é também um B-módulo à esquerda via ação $b \cdot (h \otimes w) = b_2 h \otimes b_1 w$, onde $\Delta(b) = b_1 \otimes b_2$. De fato,

$$1 \cdot (h \otimes w) = 1_2 h \otimes 1_1 w = 1h \otimes 1w = h \otimes w$$

e

$$(bb') \cdot (h \otimes w) = (bb')_2 h \otimes (bb')_1 w = (b_2 b'_2) h \otimes (b_1 b'_1) w = b \cdot (b'_2 h \otimes b'_1 w) = b \cdot (b' \cdot (h \otimes w)).$$

Com isso, vemos que a ação de B em $B^{cop} \otimes W$ é a mesma de B^{cop} em $B^{cop} \otimes W$, ou seja, $B^{cop} \otimes W$ como B^{cop}-módulo é igual à $B^{cop} \otimes W$ como B-módulo.

Vejamos agora que $B^{cop} \otimes W \cong W \otimes B$ como B-módulos à esquerda, onde o isomorfismo é dado pela aplicação *twist* $\tau : B^{cop} \otimes W \longrightarrow W \otimes B$, dada por $\tau(b \otimes w) = w \otimes b$. De fato, para ver que τ é um isomorfismo de B-módulos, denotemos a ação de B em $B^{cop} \otimes W$ por $h \cdot_{B^{cop} \otimes W} (b \otimes w) = h_2 b \otimes h_1 w$, e denotemos a ação de B em $W \otimes B$ por $h \cdot_{W \otimes B} (w \otimes b) = h_1 w \otimes h_2 b$, onde $\Delta(h) = h_1 \otimes h_2$. Assim, temos que

$$\tau(h \cdot_{B^{cop} \otimes W} (b \otimes w)) = \tau(h_2 b \otimes h_1 w) = h_1 w \otimes h_2 b = h \cdot_{W \otimes B} (w \otimes b) = h \cdot_{W \otimes B} \tau(b \otimes w).$$

Também temos que $\tau(b \otimes w + b' \otimes w') = w \otimes b + w' \otimes b' = \tau(b \otimes w) + \tau(b' \otimes w')$. Além disso, $\tau' : W \otimes B \longrightarrow B^{cop} \otimes W$ dado por $\tau'(w \otimes b) = b \otimes w$ é tal que $\tau \circ \tau' = Id_{W \otimes B}$ e $\tau' \circ \tau = Id_{B^{cop} \otimes W}$.

Com isso, temos que $W \otimes B \cong B^{cop} \otimes W$ como B-módulos à esquerda. Para concluir, note que temos $W \otimes B \cong B^{cop} \otimes W$ como B-módulos à esquerda, mas $B^{cop} \otimes W$ como B-módulo é igual à $B^{cop} \otimes W$ como B^{cop}-módulo. Por sua vez, $B^{cop} \otimes W \cong (B^{cop})^{\dim_{\Bbbk}(W)}$ como B^{cop}-módulos, e portanto $B^{cop} \otimes W \cong (B^{cop})^{\dim_{\Bbbk}(W)}$ como B-módulos. Como $(B^{cop})^{\dim_{\Bbbk}(W)} = B^{\dim_{\Bbbk}(W)}$ como B-módulo, temos então que $W \otimes B \cong B^{cop} \otimes W \cong (B^{cop})^{\dim_{\Bbbk}(W)} = B^{\dim_{\Bbbk}(W)}$ como B-módulos, donde concluímos que $W \otimes B \cong B^{\dim_{\Bbbk}(W)}$ como queríamos. □

Antes de prosseguir, é interessante deixar registrado um resultado simples, mas que nos possibilita a utilização do Teorema de Krull-Schmidt em alguns casos.

Proposição 2.1.4. *Sejam A uma $\Bbbk$-álgebra de dimensão finita e M um A-módulo à esquerda finitamente gerado. Então:*

(*i*) *M tem dimensão finita como $\Bbbk$-espaço vetorial;*

(*ii*) *M tem comprimento finito como A-módulo à esquerda.*

Demonstração. Prova de (i): Suponha que $\{v_1, ..., v_n\}$ é uma base de A sobre $\Bbbk$ e que $m_1, ..., m_r$ geram M sobre A. Denotando $w_{ij} := v_i m_j$, $i = 1, ..., n$ e $j = 1, ..., r$, afirmamos que o conjunto finito $\{w_{ij}\}_{i,j}$ gera M sobre $\Bbbk$, e portanto podemos extrair dele uma base para M como $\Bbbk$-espaço vetorial. Para ver que de fato $\{w_{ij}\}_{i,j}$ gera M sobre $\Bbbk$, notemos que para qualquer $x \in M$, existem $a_1, ..., a_r \in A$ tais que $x = \sum_{i=1}^{r} a_i m_i$. Mas, para cada a_i, existem $\alpha_1^i, ..., \alpha_n^i \in \Bbbk$ tais que $a_i = \sum_{j=1}^{n} \alpha_j^i v_j$.

Assim, $x = \sum_{i=1}^{r} a_i m_i = \sum_{i=1}^{r} \left(\sum_{j=1}^{n} \alpha_j^i v_j \right) m_i = \sum_{i,j} \alpha_j^i v_j m_i = \sum_{i,j} \alpha_j^i w_{ij}$.

Logo, $\{w_{ij}\}_{i,j}$ gera M sobre $\Bbbk$, como queríamos.

Prova de (ii): Pelo item (i), já sabemos que M tem dimensão finita como $\Bbbk$-espaço vetorial. Queremos agora ver que M tem comprimento finito como A-módulo, e para isso vejamos que M não admite nenhuma cadeia estrita e infinita de A-submódulos, nem ascendente, nem descendente. Desta forma, M satisfaz ACC e DCC, e portanto tem comprimento finito.

Temos que todo A-submódulo de M é, em particular, um $\Bbbk$-subespaço vetorial de M. Assim, qualquer cadeia de A-submódulos de M é, em particular, uma cadeia de $\Bbbk$-subespaços vetoriais de M. Desde que M tem dimensão finita, todo A-submódulo de M também tem dimensão finita como $\Bbbk$-espaço vetorial. Como cada inclusão estrita, ou contenção estrita, de $\Bbbk$-espaços vetoriais precisa aumentar, ou diminuir, pelo menos uma dimensão do $\Bbbk$-espaço vetorial, temos que não pode existir uma cadeia estrita e infinita, ascendente ou descendente, de $\Bbbk$-subespaços vetoriais de M. Logo não há também uma cadeia estrita e infinita de A-submódulos de M, e com isso M tem comprimento finito como A-módulo. □

Como consequência imediata da proposição anterior, temos o seguinte corolário:

Corolário 2.1.5. *Se A é uma $\Bbbk$-álgebra de dimensão finita e M é um A-módulo à esquerda finitamente gerado, então temos que o Teorema de Krull-Schmidt se aplica ao A-módulo M.*

Em particular, para qualquer $\Bbbk$-álgebra de dimensão finita A, temos que o Teorema de Krull-Schmidt se aplica à representação regular de A, isto é, o teorema se aplica ao A-módulo A.

No próximo resultado veremos uma caracterização para um módulo ser fiel. Antes, precisamos da seguinte definição:

Definição 2.1.6. *Sejam M e N dois A-módulos. Dizemos que $f : M \longrightarrow N$ é uma* imersão *se f é um homomorfismo de A-módulos injetor. Neste caso, dizemos que M está imerso em N.*

Se $f : M \longrightarrow N$ é uma imersão, podemos ver M como um submódulo de N, já que $f(M)$ é um submódulo de N e $M \cong f(M)$ como A-módulo.

Lema 2.1.7. *Seja A uma $\Bbbk$-álgebra de dimensão finita e M um A-módulo à esquerda finitamente gerado. Então M é A-fiel se, e somente se, A é imerso em M^n como um A-módulo à esquerda para algum inteiro positivo n.*

Demonstração. [$\Longrightarrow$] Seja M A-fiel. Então temos que $ann_A(M) = \{0\}$.

Como M é finitamente gerado como um A-módulo e A é uma $\Bbbk$-álgebra de dimensão finita, pelo que vimos anteriormente temos que $\dim_{\Bbbk}(M) < \infty$. Consideremos então $\{m_1, m_2, ..., m_n\}$ uma base de M sobre $\Bbbk$.

Defina $f : A \longrightarrow M^n$ por $f(a) = (am_1, am_2, ..., am_n)$.

Afirmamos que f é um homomorfismo de A-módulos à esquerda injetor. De fato, temos que f é um homomorfismo de A-módulos à esquerda, vamos apenas provar que é injetor.

Seja $a \in \ker(f)$. Então $f(a) = 0$, isto é, $(am_1, am_2, ..., am_n) = (0, \ldots, 0)$, ou seja, $am_i = 0$, para $i = 1, 2, \cdots n$. Assim, para qualquer $m \in M$, temos que $m = \alpha_1 m_1 + \cdots + \alpha_n m_n$, e portanto

$$a \cdot m = a \cdot (\alpha_1 m_1 + \cdots + \alpha_n m_n) = \alpha_1 am_1 + \cdots + \alpha_n am_n = 0 + \cdots + 0 = 0,$$

isto é, $a \in ann_A(M) = \{0\}$. Logo $a = 0$ e com isso f é um homomorfismo injetor.

Portantoo A é imerso em M^n.

[$\Longleftarrow$] Se A é imerso em M^n como A-módulo à esquerda, então temos que existe um homomorfismo de A módulos injetor $f : A \longrightarrow M^n$, donde temos que $f(A)$ é um submódulo de M^n isomorfo à A como A-módulo. Assim,

$$ann_A(M) = ann_A(M^n) \subseteq ann_A(f(A)) = ann_A(A) = \{0\}$$

Logo $ann_A(M) = \{0\}$ e, portanto, M é A-fiel. □

Lembremos que quando um A-módulo N tem comprimento finito, então pelo Teorema de Krull-Schmidt ele possui uma decomposição da forma $N = N_1 \oplus \cdots \oplus N_s$, onde cada $N_i \subseteq N$ é um submódulo indecomponível de N, para $i \in \{1, 2, ..., s\}$, e essa decomposição é única a menos de isomorfismo.

Além disso, podemos reordenar essa soma e agrupar os submódulos que são isomorfos entre si, obtendo $N \cong N_{j_1}^{s_1} \oplus N_{j_2}^{s_2} \oplus \cdots \oplus N_{j_t}^{s_t}$ onde $t \leq s$, $s_1 + s_2 + \cdots + s_t = s$ e $N_{j_i} \ncong N_{j_l}$ para $i \neq l$, onde $i, l \in \{1, 2, ..., t\}$.

Cada N_{j_i} como acima, $i = 1, 2, \cdots, t$, é dito ser um *tipo de A-módulo à esquerda indecomponível principal de N*. Assim, temos a seguinte proposição:

Proposição 2.1.8. *Sejam A uma álgebra sobre $\Bbbk$ de dimensão finita tal que A como A-módulo à esquerda é injetivo e $P_1, ..., P_t$ os tipos de A-módulos à esquerda indecomponíveis principais de A. Se M é um A-módulo à esquerda finitamente gerado, então M é A-fiel se, e somente se, cada P_i é isomorfo a um somando direto do A-módulo M.*

Para esta prova vamos utilizar fortemente o Teorema de Krull-Schmidt, para garantir tanto a existência quanto a unicidade da decomposição de Krull-Schmidt. Destacamos ainda que quando um módulo tem comprimento finito, todo submódulo também tem comprimento finito, e portanto o Teorema de Krull-Schmidt também se aplica. Este resultado é o Corolário A.1.33 do apêndice.

Demonstração. Seja M um A-módulo à esquerda finitamente gerado. Então pelo item (ii) da Proposição 2.1.4, M tem comprimento finito. Assim, pelo Teorema de Krull-Schmidt, temos que $M = M_1 \oplus M_2 \oplus \cdots \oplus M_s$, onde cada M_i é um submódulo indecomponível de M, para cada $i \in \{1, 2, ..., s\}$.

[$\Longrightarrow$] Suponha que M é A-fiel. Então pelo Lema 2.1.7, temos que A é imerso em M^n, para algum inteiro positivo n. Isto quer dizer que A pode ser visto como um submódulo de M^n, e pela hipótese de A ser injetivo como A-módulo à esquerda, significa que ele é então um somando direto de M^n, conforme o Corolário 1.4.8. Assim, existe um submódulo X de M^n tal que $M^n \cong A \oplus X$.

Da hipótese que $P_1, ..., P_t$ são os tipos de A-módulos à esquerda indecomponíveis principais de A, temos que $A \cong \bigoplus_{i=1}^{t} P_i^{s_i}$, onde $s_i \geq 1$ e P_i é indecomponível para $i = 1, 2, ..., t$.

Como M é finitamente gerado, temos que M^n também é finitamente gerado, e segue pelo item (ii) da Proposição 2.1.4 que M^n tem comprimento finito. Desta maneira, $X \subseteq M^n$ é submódulo de M^n, e com isso temos que X tem comprimento finito, donde segue que o Teorema de Krull-Schmidt também se aplica a X. Logo, temos que $X = \bigoplus_{i=1}^{r} X_i$, onde cada X_i é um submódulo indecomponível de X, para $i = 1, 2, ..., r$.

Assim,

$$M^n \cong A \oplus X \cong \left(\bigoplus_{i=1}^{t} P_i^{s_i}\right) \bigoplus \left(\bigoplus_{i=1}^{r} X_i\right) \cong \left(\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{s_i} P_i\right)\right) \bigoplus \left(\bigoplus_{i=1}^{r} X_i\right)$$

e, portanto, temos a decomposição de Krull-Schmidt dada por

$$M^n \cong \left(\bigoplus_{i=1}^{t} \left(\bigoplus_{j=1}^{s_i} P_i\right)\right) \bigoplus \left(\bigoplus_{i=1}^{r} X_i\right), \tag{2.1}$$

ou seja, M^n é isomorfo a uma soma direta de indecomponíveis onde os somandos são sempre isomorfos a P_i ou X_j.

Por outro lado, como $M^n \cong \bigoplus_{k=1}^{n} M$, temos a seguinte decomposição de Krull-Schmidt também

$$M^n \cong \bigoplus_{k=1}^{n} M = \bigoplus_{k=1}^{n} (M_1 \oplus M_2 \oplus \cdots \oplus M_s), \tag{2.2}$$

isto é, M^n é isomorfo a uma soma direta de indecomponíveis, onde cada indecomponível é isomorfo a algum M_i.

Agora, pela unicidade da decomposição de Krull-Schmidt, temos que a decomposição de M^n é única a menos de isomorfismo, donde concluímos pelas decomposições (2.2) e (2.1) que para cada $j \in \{1, 2, ..., t\}$ existe $i \in \{1, 2, ..., s\}$ tal que $M_i \cong P_j$.

Portanto, M contém um somando direto isomorfo a cada P_j, para todo $j = 1, 2, ..., t$.

[$\Longleftarrow$] Suponha que cada P_i é isomorfo a um somando direto do A-módulo M. Então, para cada $i \in \{1, 2, ..., t\}$, existe X_i submódulo de M tal que $M \cong P_i \oplus X_i$. Assim,

$$M^t \cong \bigoplus_{i=1}^{t} M \cong \bigoplus_{i=1}^{t} (P_i \oplus X_i)$$

Como $A \cong \bigoplus_{i=1}^{t} P_i^{s_i}$, seja $n = max\{s_1, s_2, ..., s_t\}$. Então

Assim,

$$\begin{aligned}
M^{tn} &\cong (M^t)^n \cong \left(\bigoplus_{i=1}^{t} (P_i \oplus X_i)\right)^n = \left[\left(\bigoplus_{i=1}^{t} P_i\right) \oplus \left(\bigoplus_{i=1}^{t} X_i\right)\right]^n \cong \\
&\cong \left(\bigoplus_{i=1}^{t} P_i\right)^n \oplus \left(\bigoplus_{i=1}^{t} X_i\right)^n \cong \left(\bigoplus_{i=1}^{t} P_i^n\right) \oplus \left(\bigoplus_{i=1}^{t} X_i\right)^n \cong \\
&\cong \left(\bigoplus_{i=1}^{t} (P_i^{s_i} \oplus P_i^{n-s_i})\right) \oplus \left(\bigoplus_{i=1}^{t} X_i\right)^n = \\
&= \left(\bigoplus_{i=1}^{t} P_i^{s_i}\right) \oplus \left(\bigoplus_{i=1}^{t} P_i^{n-s_i}\right) \oplus \left(\bigoplus_{i=1}^{t} X_i\right)^n \cong \\
&\cong A \oplus \left(\bigoplus_{i=1}^{t} P_i^{n-s_i}\right) \oplus \left(\bigoplus_{i=1}^{t} X_i\right)^n
\end{aligned}$$

Donde concluímos então que A está imerso em M^{tn}. Assim, pelo Lema 2.1.7 temos que M é A-fiel. □

Notemos que na prova anterior, durante a parte [$\Longleftarrow$], poderíamos ter assumido que $P_i \cong M_i$, para cada $i = 1, ..., t$, logo de início, por causa do Teorema de Krull-Schmidt. De fato, tínhamos que $M = \bigoplus_{i=1}^{n} M_i$, onde cada M_i é um submódulo indecomponível. Por outro lado, para cada i, $M = P_i \oplus X_i$. Em particular, para $i = 1$, temos $M = P_1 \oplus X_1$. Desta maneira, X_1 admite uma decomposição de Krull-Schmidt. Suponhamos que seja $X_1 = N_1 \oplus N_2 \oplus \cdots \oplus N_r$ esta decomposição. Então, $M = M_1 \oplus \cdots M_n = P_1 \oplus N_1 \oplus \cdots N_r$, e sabemos pelo Teorema de Krull-Schmidt que $n = r + 1$, e que existe j tal que $P_1 \cong M_j$. Sem perda de generalidade, suponhamos que $j = 1$. Repetindo o

argumento para $i = 2$, obtemos que existe $j \neq 1$ tal que $P_2 \cong M_j$, e sem perda de generalidade, podemos dizer que $j = 2$. De fato, $j \geq 2$, pois se fosse $j = 1$, teríamos $P_1 \cong M_1 \cong P_2$, o que seria um absurdo já que $P_1 \ncong P_2$. Procedendo indutivamente, temos que $t \leq n$ e $P_i \cong M_i$, para cada $i = 1, 2, ..., t$.

Para a próxima proposição, utilizaremos esse fato. Além disso, também usaremos o fato que se um módulo tem comprimento finito, então cada submódulo é finitamente gerado. A prova deste fato é dada pelo lema a seguir, lembrando que ter comprimento finito é equivalente a ser noetheriano e artiniano. Para estas definições e maiores informações, recomendamos a leitura da primeira seção do apêndice.

Lema 2.1.9. *Se M é um A-módulo noetheriano, então cada submódulo de M é finitamente gerado.*

Demonstração. Sejam N um submódulo de M e $\mathcal{F}$ o conjunto de todos submódulos finitamente gerados de N. Então temos que $\mathcal{F}$ não é vazia, pois $\{0\} \in \mathcal{F}$. Como M é noetheriano, então N também é noetheriano, e segue que $\mathcal{F}$ tem um elemento maximal. Digamos que N_0 é um elemento maximal de $\mathcal{F}$. Se $N_0 \neq N$, então existe $x \in N \setminus N_0$, e consideramos então o A-módulo $N_1 = N_0 + Ax$. Como N_0 é finitamente gerado, N_1 também é finitamente gerado, assim $N_1 \in \mathcal{F}$ e $N_0 \subsetneq N_1$, o que contradiz a maximalidade de N_0.

Logo, $N_0 = N$ e portanto N é finitamente gerado. □

Proposição 2.1.10. *Seja A uma álgebra sobre $\Bbbk$ de dimensão finita tal que A como A-módulo à esquerda é injetivo. Se W é um A-módulo à esquerda finitamente gerado, então existe um inteiro positivo r tal que $W^r = F \oplus E$, onde F é um A-módulo à esquerda livre e E é um A-módulo à esquerda que não é A-fiel.*

Demonstração. Se W não é A-fiel, tomamos $r = 1$, $F = \{0\}$ e $E = W$.

Assumimos agora que W é A-fiel. Seja $A \cong P_1^{n_1} \oplus \cdots \oplus P_t^{n_t}$, onde $P_1, P_2, ..., P_t$ são os tipos de A-módulos à esquerda indecomponíveis principais de A. Como W é finitamente gerado e A é uma $\Bbbk$-álgebra de dimensão finita, temos que W tem comprimento finito e portanto ele tem uma decomposição em soma direta de módulos indecomponíveis. Seja $W = M_1 \oplus \cdots \oplus M_n$ essa decomposição. Como estamos assumindo W A-fiel, pela Proposição 2.1.8 vista anteriormente, temos que cada P_i é isomorfo a um somando direto de W. Pelo que vimos anteriormente, temos $t \leq n$ e podemos considerar $P_i \cong M_i$, para $i = 1, ..., t$. Analisamos então os submódulos M_i restantes, se existirem, isto é, olhamos M_i para $i > t$, e então, reorganizando os submódulos isomorfos entre si, obtemos que $W \cong P_1^{s_1} \oplus \cdots \oplus P_t^{s_t} \oplus Q$, com $s_i > 0$ para cada $i \in \{1, 2, ..., t\}$, e algum A-módulo Q, que é a soma direta dos demais submódulos indecomponíveis da decomposição de W, tal que nenhum somando direto de Q é isomorfo à P_i, $i \in \{1, 2, ..., t\}$.

Consideramos agora $r = mmc\{n_1, n_2, ..., n_t\}$. Assim, temos que existem r_i tais que $r = n_i r_i$, para cada $i = 1, 2, ..., t$.

Portanto,

$$\begin{aligned} W^r &\cong (P_1^{s_1} \oplus \cdots \oplus P_t^{s_t} \oplus Q)^r \cong P_1^{rs_1} \oplus \cdots \oplus P_t^{rs_t} \oplus Q^r \cong \\ &\cong P_1^{n_1 r_1 s_1} \oplus \cdots \oplus P_t^{n_t r_t s_t} \oplus Q^r \cong (P_1^{n_1})^{r_1 s_1} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t} \oplus Q^r \end{aligned}$$

Isto é, $W^r \cong (P_1^{n_1})^{r_1 s_1} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t} \oplus Q^r$. Seja agora $s = min\{r_1 s_1, r_2 s_2, ..., r_t s_t\}$. Podemos supor, sem perda de generalidade, que $s = r_1 s_1$. Então,

$$\begin{aligned} W^r &\cong (P_1^{n_1})^{r_1 s_1} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t} \oplus Q^r \cong \\ &\cong ((P_1^{n_1})^s \oplus (P_2^{n_2})^s \oplus \cdots \oplus (P_t^{n_t})^s) \oplus (P_2^{n_2})^{r_2 s_2 - s} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t - s} \oplus Q^r \cong \\ &\cong (P_1^{n_1} \oplus P_2^{n_2} \oplus \cdots \oplus P_t^{n_t})^s \oplus (P_2^{n_2})^{r_2 s_2 - s} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t - s} \oplus Q^r \cong \\ &\cong (A)^s \oplus (P_2^{n_2})^{r_2 s_2 - s} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t - s} \oplus Q^r \end{aligned}$$

Assim, denotamos por $F := A^s$ e $E := (P_2^{n_2})^{r_2 s_2 - s} \oplus \cdots \oplus (P_t^{n_t})^{r_t s_t - s} \oplus Q^r$.
Temos que F é A-livre. Notemos também que W^r tem comprimento finito, em particular W^r é um A-módulo noetheriano, e portanto pelo Lema 2.1.9 temos que todo submódulo de W^r é finitamente gerado. Temos então que E é finitamente gerado como A-módulo à esquerda, pois E é submódulo de W^r. Além disso, P_1 não é isomorfo a nenhum somando direto de E, donde concluímos pela Proposição 2.1.8 que E não é A-fiel. □

2.2 O Teorema de Nichols-Zöeller

Nesta seção provaremos o Teorema de Nichols-Zöeller. Utilizaremos os resultados da seção anterior juntamente com a teoria de Hopf apresentada no capítulo 1 para obtermos os resultados a seguir.

Proposição 2.2.1. *Sejam H uma álgebra de Hopf de dimensão finita e W um H-módulo à esquerda finitamente gerado tal que W^r é um H-módulo livre para algum inteiro positivo r. Então W é um H-módulo livre.*

Demonstração. Como H é uma $\Bbbk$-álgebra de dimensão finita, temos pelo Corolário 2.1.5 que H é um H-módulo à esquerda de comprimento finito. Desta maneira, pelo Teorema de Krull-Schmidt temos que $H = H_1 \oplus H_2 \oplus \cdots \oplus H_n$, onde H_i é um H-submódulo à esquerda indecomponível de H, para $i = 1, 2, ..., n$.

Agora, como H é uma álgebra de Hopf de dimensão finita, então pelo item (iv) do Teorema de Larson-Sweedler 1.3.9, temos que $\dim_{\Bbbk}(\int_H^l) = 1$, e portanto $\int_H^l \neq \{0\}$.

Seja $t \in \int_H^l, t \neq 0$. Então, podemos escrever $t = t_1 + t_2 + \cdots + t_n$, onde $t_i \in H_i$ para cada $i \in \{1, 2, .., n\}$. Consequentemente, para todo $h \in H$, temos as seguintes equivalências:

$$ht = \varepsilon(h)t$$

$$h(t_1 + t_2 + \cdots + t_n) = \varepsilon(h)(t_1 + t_2 + \cdots + t_n)$$

$$ht_1 + ht_2 + \cdots + ht_n = \varepsilon(h)t_1 + \varepsilon(h)t_2 + \cdots + \varepsilon(h)t_n$$

$$ht_1 + ht_2 + \cdots + ht_n = \varepsilon(h)1_H t_1 + \varepsilon(h)1_H t_2 + \cdots + \varepsilon(h)1_H t_n$$

$$(ht_1 + ht_2 + \cdots + ht_n) - (\varepsilon(h)1_H t_1 + \varepsilon(h)1_H t_2 + \cdots + \varepsilon(h)1_H t_n) = 0$$

$$(h - \varepsilon(h)1_H)t_1 + (h - \varepsilon(h)1_H)t_2 + \cdots + (h - \varepsilon(h)1_H)t_n = 0$$

Como cada H_i é um H-submódulo de H e $t_i \in H_i$, temos que $(h - \varepsilon(h)1_H)t_i \in H_i$ para cada $i = 1, 2, ..., n$. Disto, e do fato que

$$(h - \varepsilon(h)1_H)t_1 + (h - \varepsilon(h)1_H)t_2 + \cdots + (h - \varepsilon(h)1_H)t_n = 0$$

onde $H = H_1 \oplus H_2 \oplus \cdots \oplus H_n$, concluímos que $(h - \varepsilon(h)1_H)t_i = 0, \forall i = 1, 2, ..., n$.

Assim, $ht_i - \varepsilon(h)1_H t_i = 0$, e portanto $ht_i = \varepsilon(h)t_i$, isto é, para cada $i = 1, 2, ..., n$, temos $ht_i = \varepsilon(h)t_i, \forall h \in H$. Portanto $t_i \in \int_H^l$, para cada $i = 1, 2, ..., n$. Como $\dim_{\Bbbk}(\int_H^l) = 1$ e $t \neq 0$, temos $t_i = \lambda_i t, \lambda_i \in \Bbbk$, $i \in \{1, 2, ..., n\}$.

Assim, $t = t_1 + t_2 + \cdots + t_n = \lambda_1 t + \lambda_2 t + \cdots + \lambda_n t$. Como $t \neq 0$, então existe $\lambda_i \neq 0$. Desta maneira, $t_i = \lambda_i t$ e segue que $t = \dfrac{1}{\lambda_i} t_i$.

Notemos agora que, para $j \neq i$, temos $t_j = \lambda_j t = \lambda_j \dfrac{1}{\lambda_i} t_i = \dfrac{\lambda_j}{\lambda_i} t_i$, ou seja, $t_j \in H_i$, e com isso $t_j = 0$. Assim,

$$t = \lambda_1 t + \lambda_2 t + \cdots + \lambda_n t = \lambda_i t,$$

ou seja,

$$t = \lambda_i t = \lambda_i \frac{1}{\lambda_i} t_i = t_i.$$

Logo, $t = t_i \in H_i$.

Vejamos agora que o espaço das integrais de H está totalmente contido em H_i. De fato, se $t' \in \int_H^l$, temos $t' = \lambda' t = \lambda' t_i \in H_i$, onde $\lambda' \in \Bbbk$. Afirmamos agora que H_i não é isomorfo a nenhum H_j, $j \neq i$, como H-módulos à esquerda. De fato, suponhamos por absurdo que exista um isomorfismo de H-módulos à esquerda $f : H_i \longrightarrow H_j$, com $i \neq j$. Como $t = t_i$ é um integral à esquerda, $t \neq 0$ e $t = t_i \in H_i$, concluímos que $f(t)$ é um integral à esquerda, pois para qualquer $h \in H$, temos $hf(t) = f(ht) = f(\varepsilon(h)t) = \varepsilon(h)f(t)$. Assim, $f(t) \in H_j$ é um integral à esquerda, e segue que $f(t) \in H_i$, e portanto concluímos que $f(t) = 0$. Como f é isomorfismo, então $t = 0$, o que é um absurdo.

Sejam $P_1 = H_i, P_2, ..., P_s$ os tipos de H-módulos à esquerda indecomponíveis principais de H.

Então $H \cong H_i \oplus P_2^{n_2} \oplus \cdots \oplus P_s^{n_s} := \bigoplus_{j=1}^{s} P_j^{n_j}$. Observe que $n_1 = 1$.

Por hipótese W^r é um H-módulo livre. Como W é finitamente gerado, W^r também é, logo W^r é livre e finitamente gerado, ou seja, possui uma base finita. Portanto concluímos que $W^r \cong H^p$, para algum inteiro positivo p. Assim,

$$W^r \cong H^p \cong (P_1^{n_1} \oplus \cdots \oplus P_s^{n_s})^p \cong P_1^{pn_1} \oplus \cdots \oplus P_s^{pn_s} \tag{2.3}$$

Como W é finitamente gerado, e H é uma álgebra de dimensão finita, segue que W tem comprimento finito, e pelo Teorema de Krull Schmidt ele é soma direta de H-módulos à esquerda indecomponíveis.

Digamos que seja $W = W_1 \oplus W_2 \oplus \cdots \oplus W_t$, com W_i indecomponível para cada $i \in \{1, 2, ..., t\}$.

Temos então a seguinte decomposição de Krull-Schmidt

$$W^r = (W_1 \oplus W_2 \oplus \cdots \oplus W_t)^r \tag{2.4}$$

Por outro lado, temos que

$$W^r \cong \oplus P_1^{pn_1} \oplus \cdots \oplus P_s^{pn_s} \cong \left[\bigoplus_{j=1}^{s} \left(\bigoplus_{k=1}^{n_j} P_j \right) \right]^p \tag{2.5}$$

também é uma decomposição de Krull-Schmidt.

Assim, pelo Teorema de Krull-Schmidt, as decomposições (2.4) e (2.5) têm a mesma quantidade de somandos, e para cada $i = 1, ..., t$, temos que existe $j \in \{1, ..., s\}$ tal que $W_i \cong P_j$, e da mesma forma, para cada P_j, existe um i tal que $P_j \cong W_i$.

Isto que dizer que, como $W = \bigoplus_{i=1}^{t} W_i$, podemos substituir os submódulos W_i pelos P_j's isomorfos, e cada P_j aparece, pelo menos uma vez. Agrupando os submódulos que repetem, obtemos então que

$$W \cong P_1^{m_1} \oplus P_2^{m_2} \oplus \cdots \oplus P_s^{m_s} \tag{2.6}$$

onde $m_1, ..., m_s$ são inteiros positivos.

Disto, obtemos que

$$W^r \cong (P_1^{m_1} \oplus P_2^{m_2} \oplus \cdots \oplus P_s^{m_s})^r \cong \bigoplus_{i=1}^{s} P_i^{rm_i} \tag{2.7}$$

Comparando (2.3) e (2.7), obtemos que

$$W^r \cong \bigoplus_{i=1}^{s} P_i^{pn_i} \cong \bigoplus_{i=1}^{s} P_i^{rm_i}$$

Como P_i's são os tipos de H-módulos à esquerda indecomponíveis principais de H, obtemos que $pn_i = rm_i$, para cada $i = 1, ..., s$.

Em particular, $n_1 = 1$, donde temos que $p = rm_1$. Assim, para $i > 1$, temos que $rm_i = pn_i = (rm_1)n_i$, ou seja, $m_i = m_1 n_i$.

Assim, substituindo os índices em (2.6), obtemos que

$$W \cong P_1^{m_1} \oplus P_2^{m_1 n_1} \oplus \cdots \oplus P_s^{m_1 n_s} \cong (P_1 \oplus P_2^{n_1} \oplus \cdots \oplus P_s^{n_s})^{m_1} = (H)^{m_1}$$

Portanto, W é um H-módulo livre. □

Proposição 2.2.2. *Sejam B uma álgebra de Hopf de dimensão finita e W um B-módulo à esquerda finitamente gerado. Suponha que exista um B-módulo à esquerda fiel e finitamente gerado L tal que $L \otimes W \cong W^{\dim_{\Bbbk}(L)}$ como B-módulos à esquerda. Então W é um B-módulo livre.*

Demonstração. Como B é uma álgebra de Hopf de dimensão finita, temos pela Proposição 1.4.13 que B é injetivo como B-módulo à esquerda e, como W é finitamente gerado, pela Proposição 2.1.10, temos que existe um inteiro positivo r tal que $W^r \cong F \oplus E$, onde F é um B-módulo livre e E é um B-módulo à esquerda que não é B-fiel.

Se mostrarmos que W^r é livre como B-módulo, teremos pela Proposição 2.2.1 que W será um B-módulo livre. Como $W^r \cong F \oplus E$, onde F é um B-módulo livre, nosso trabalho será mostrar que $E = \{0\}$, concluindo assim que $W^r = F$ que é livre.

Visto que L também é finitamente gerado, também pela Proposição 2.1.10, temos que existe um inteiro positivo r' tal que $L^{r'} \cong F' \oplus E'$, como B-módulos à esquerda, onde F' é um B-módulo livre e E' é um B-módulo à esquerda que não é B-fiel.

Notemos que como L é B-fiel, então $L^{r'}$ também é B-fiel, e com isso $F' \neq \{0\}$. Além disso, também temos que

$$L \otimes W^r \cong (L \otimes W)^r \cong (W^{\dim_{\Bbbk}(L)})^r \cong (W^r)^{\dim_{\Bbbk}(L)}$$

Como $W^r \cong F \oplus E$, segue que

$$\begin{aligned} F^{\dim_{\Bbbk}(L)} \oplus E^{\dim_{\Bbbk}(L)} &\cong (F \oplus E)^{\dim_{\Bbbk}(L)} \cong (W^r)^{\dim_{\Bbbk}(L)} \cong \\ &\cong L \otimes W^r \cong L \otimes (F \oplus E) \cong (L \otimes F) \oplus (L \otimes E) \end{aligned}$$

Como F é um B-módulo livre, então temos $F \cong B^q$, para algum inteiro positivo q, e com isso

$$L \otimes F \cong L \otimes B^q \cong (L \otimes B)^q$$

Pela Proposição 2.1.3, temos que $(L \otimes B)^q \cong (B^{\dim_{\Bbbk}(L)})^q$ como B-módulos à esquerda. Assim, temos

$$L \otimes F \cong (L \otimes B)^q \cong (B^{\dim_{\Bbbk}(L)})^q \cong (B^q)^{\dim_{\Bbbk}(L)} \cong F^{\dim_{\Bbbk}(L)},$$

ou seja, $F^{\dim_{\Bbbk}(L)} \oplus E^{\dim_{\Bbbk}(L)} \cong F^{\dim_{\Bbbk}(L)} \oplus (L \otimes E)$.

Desde que $(W^r)^{\dim_{\Bbbk}(L)} \cong F^{\dim_{\Bbbk}(L)} \oplus E^{\dim_{\Bbbk}(L)}$, podemos aplicar o Teorema de Krull-Schmidt, obtendo que $E^{\dim_{\Bbbk}(L)} \cong L \otimes E$.

Desta maneira, temos

$$\begin{aligned}(E^{r'})^{\dim_{\Bbbk}(L)} &\cong (E^{\dim_{\Bbbk}(L)})^{r'} \cong (L \otimes E)^{r'} \cong L^{r'} \otimes E \cong \\ &\cong (F' \oplus E') \otimes E \cong (F' \otimes E) \oplus (E' \otimes E)\end{aligned}$$

Como F' é B-módulo livre e $F' \neq \{0\}$, temos que existe um inteiro positivo s tal que $F' = B^s$.

Agora, suponhamos que seja $E \neq \{0\}$. Vamos chegar a uma contradição, e com isso, teremos que $E = \{0\}$.

Se $E \neq \{0\}$, então pela Proposição 2.1.3 temos que

$$F' \otimes E \cong B^s \otimes E \cong (B \otimes E)^s \cong \left(B^{\dim_{\Bbbk}(E)}\right)^s \cong B^{s \dim_{\Bbbk}(E)}$$

Logo, $F' \otimes E$ é não-nulo e livre como B-módulo, e portanto é B-fiel.

Afirmamos agora que $(E^{r'})^{\dim_{\Bbbk}(L)}$ é B-fiel. De fato, $(E^{r'})^{\dim_{\Bbbk}(L)} \cong (F' \otimes E) \oplus (E' \otimes E)$. Como $F' \otimes E$ é B-fiel, temos que $ann(F' \otimes E) = \{0\}$, e disto obtemos que

$$ann\left((E^{r'})^{\dim_{\Bbbk}(L)}\right) = ann((F' \otimes E) \oplus (E' \otimes E)) \subseteq ann(F' \otimes E) = \{0\}$$

Assim, $(E^{r'})^{\dim_{\Bbbk}(L)}$ é B-fiel, e com isto, temos que E também é B-fiel, donde temos uma contradição, pois E não é B-fiel.

Logo, somos obrigados a concluir que $E = \{0\}$ e então $W^r \cong F \oplus E = F$, que é livre, e portanto segue o resultado. □

No que segue, vamos falar de (H, B)-módulos de Hopf à esquerda.

Sejam H uma álgebra de Hopf e B uma subálgebra de Hopf de H. Diremos que M é um (H, B)-*módulo de Hopf à esquerda* se M é um B-módulo à esquerda, um H-comódulo à esquerda via $\rho : M \longrightarrow H \otimes M$ e tal que ρ seja um homomorfismo de B-módulos à esquerda.

Notemos que a ação de B em $H \otimes M$ é dada pela comultiplicação Δ, conforme fizemos no ínicio deste capítulo.

Considere $m \in M$ e $b \in B$. Então, exigir que ρ seja um homomorfismo de B-módulos à esquerda significa exigir que $\rho(b \cdot_M m) = b \cdot_{H \otimes M} \rho(m)$.

Denotemos $\rho(m) := m^{-1} \otimes m^0$ e $\Delta(b) := b_1 \otimes b_2$.

Como

$$\rho(b \cdot_M m) = (b \cdot_M m)^{-1} \otimes (b \cdot_M m)^0$$

e

$$b \cdot_{H\otimes M} \rho(m) = b \cdot_{H\otimes M} (m^{-1} \otimes m^0) = b_1 m^{-1} \otimes b_2 \cdot_M m^0$$

temos então a seguinte compatibilidade:

$$(b \cdot_M m)^{-1} \otimes (b \cdot_M m)^0 = b_1 m^{-1} \otimes b_2 \cdot_M m^0$$

Exemplo 2.2.3. *O exemplo mais simples de um (H, B)-módulo de Hopf à esquerda é o próprio H. Visto que H é um B-módulo à esquerda, a ação é a multiplicação da álgebra H com os escalares restritos a B. Temos também que H é um H-comódulo à esquerda, onde a coação é dada pela comultiplicação Δ, e a compatibilidade vem pelo fato da comultiplicação ser um homomorfismo de álgebras.*

Proposição 2.2.4. *Sejam H uma álgebra de Hopf de dimensão finita, B uma subálgebra de Hopf de H e M um (H, B)-módulo de Hopf à esquerda. Então $H \otimes M \cong M^{\dim_{\Bbbk}(H)}$ como B-módulos à esquerda.*

Demonstração. Considere $U := H \otimes M$ com estrutura de B-módulo à esquerda com ação dada pelo Δ, isto é, a ação é dada por $b \cdot_U (h \otimes m) = b_1 h \otimes b_2 \cdot_M m$ e $V := H \otimes M$ com estrutura de B-módulo à esquerda com ação trivial, isto é, B age somente na segunda posição tensorial de $H \otimes M$, ou seja, a ação é dada por $b \cdot_V (h \otimes m) = h \otimes b \cdot_M m$, para quaisquer $b \in B$, $h \in H$ e $m \in M$.

Como B age apenas na segunda posição tensorial de V, temos então que $V \cong M^{\dim_{\Bbbk}(H)}$ como B-módulos à esquerda. De fato, suponha que $\dim_{\Bbbk}(H) = n$ e seja $\{h_1, ..., h_n\}$ uma base de H sobre $\Bbbk$.

Note que $H = \bigoplus_{i=1}^n \Bbbk h_i$, e que, para cada i, $M \cong \Bbbk h_i \otimes M$ como B-módulo à esquerda. Assim,

$$V = H \otimes M = \left(\bigoplus_{i=1}^n \Bbbk h_i \right) \otimes M \cong \bigoplus_{i=1}^n (\Bbbk h_i \otimes M) \cong \bigoplus_{i=1}^n M \cong M^n = M^{\dim_{\Bbbk}(H)}$$

onde todos são isomorfismos canônicos de B-módulos à esquerda.

Vamos mostrar agora que $U \cong V$, como B-módulo à esquerda. Antes, lembremos que M é um (H, B)-módulo de Hopf à esquerda, e portanto, em particular, M é um H-comódulo à esquerda. Podemos dizer que essa estrutura é dada via $\rho : M \longrightarrow H \otimes M$, e denotamos a imagem de um elemento $m \in M$ pela aplicação ρ por $\rho(m) := m^{-1} \otimes m^0$. Além disso, como H tem dimensão finita, a antípoda S é bijetora, pelo item (ii) do Teorema de Larson-Sweedler 1.3.9. Desta maneira, existe S^{-1}. Vejamos agora o isomorfismo.

Sejam $f : V \longrightarrow U$ e $g : U \longrightarrow V$ dadas por $f(h \otimes m) = m^{-1} h \otimes m^0$ e $g(h \otimes m) = S^{-1}(m^{-1}) h \otimes m^0$. Temos então que

$$\begin{aligned}
[g \circ f](h \otimes m) &= g(f(h \otimes m)) = g(m^{-1} h \otimes m^0) = S^{-1}((m^0)^{-1}) m^{-1} h \otimes (m^0)^0 = \\
&= S^{-1}(m^{-1}) m^{-2} h \otimes m^0 = S^{-1}((m^{-1})_2)(m^{-1})_1 h \otimes m^0 = \\
&= \varepsilon(m^{-1}) h \otimes m^0 = h \otimes \varepsilon(m^{-1}) m^0 = h \otimes m,
\end{aligned}$$

e também

$$\begin{aligned}[f \circ g](h \otimes m) &= f(g(h \otimes m)) = f(S^{-1}(m^{-1})h \otimes m^0) = ((m^0)^{-1})S^{-1}(m^{-1})h \otimes (m^0)^0 = \\ &= (m^{-1})S^{-1}(m^{-2})h \otimes m^0 = (m^{-1})_2 S^{-1}((m^{-1})_1)h \otimes m^0 = \\ &= \varepsilon(m^{-1})h \otimes m^0 = h \otimes \varepsilon(m^{-1})m^0 = h \otimes m,\end{aligned}$$

ou seja, concluímos que $g \circ f = Id_V$ e $f \circ g = Id_U$. Disto, segue que f e g são bijeções, com $g = f^{-1}$. Resta verificar que f é homomorfismo de B-módulos, e com isso g também será.

De fato, sejam $b \in B$ e $h \otimes m, h' \otimes m' \in H \otimes M$. Então temos $f(b \cdot_V (h \otimes m)) = f(h \otimes bm)$. Por outro lado, temos que $b \cdot_U f(h \otimes m) = b \cdot_U (m^{-1}h \otimes m^0) = b_1(m^{-1}h) \otimes b_2 \cdot_M m^0 = (b_1 m^{-1})h \otimes b_2 \cdot_M m^0$. Agora, pela compatibilidade do (H, B)-módulo de Hopf M, temos que $(bm)^{-1}h \otimes (bm)^0 = (b_1 m^{-1})h \otimes b_2 \cdot_M m^0$, ou seja, temos que vale, $f(b \cdot_V (h \otimes m)) = b \cdot_U f(h \otimes m)$. Além disso,

$$f((h \otimes m) + (h' \otimes m')) = m^{-1}h \otimes m^0 + (m')^{-1}h' \otimes (m')^0 = f(h \otimes m) + f(h' \otimes m'),$$

isto é, $f((h \otimes m) + (h' \otimes m')) = f(h \otimes m) + f(h' \otimes m')$. Concluímos então que f é um homomorfismo de B-módulos à esquerda, e segue que $g = f^{-1}$ também é.

Portanto temos $U \cong V$ como B-módulos.

Como já tínhamos que $V \cong M^{\dim_{\Bbbk}(H)}$ como B-módulos, segue então que $U \cong M^{\dim_{\Bbbk}(H)}$, ou seja, $H \otimes M \cong M^{\dim_{\Bbbk}(H)}$ como B-módulos à esquerda, onde a ação em $H \otimes M$ é dada pelo Δ. □

Lema 2.2.5. *Sejam H uma álgebra de Hopf e $B \subseteq H$ uma subálgebra de Hopf de H de dimensão finita. Então qualquer (H, B)-módulo de Hopf à esquerda M, M não-nulo, contém um (H, B)-módulo de Hopf à esquerda de dimensão finita.*

Demonstração. Seja M é um (H, B)-módulo de Hopf à esquerda, $M \neq \{0\}$. Então, em particular, M é um H-comódulo à esquerda. Como M é um H-comódulo não-nulo, tome $m \in M$, $m \neq 0$. Pelo Teorema Fundamental dos Comódulos 1.2.10, temos que m pertence a um subcomódulo N de dimensão finita.

Afirmamos então que $BN \subseteq M$ é um (H, B)-módulo de Hopf, onde BN tem dimensão finita. Para verificarmos isso, começamos notando que $N \subseteq M$, onde M é um B-módulo à esquerda, e segue que o produto de elementos de N por elementos de B à esquerda está bem definido, e assim BN se torna um B-módulo à esquerda.

Além disso, para $b \in B$ e $n \in N$, temos $\rho(bn) = (bn)^{-1} \otimes (bn)^0$. Como $BN \subseteq M$ e M é um (H, B)-módulo de Hopf à esquerda, vale a compatibilidade $(bn)^{-1} \otimes (bn)^0 = b_1 n^{-1} \otimes b_2 \cdot n^0$. Desde que B é uma subálgebra de Hopf, temos que $\Delta(b) \in B \otimes B$, e pelo fato que N é um subcomódulo de M, temos que $\rho(n) = n^{-1} \otimes n^0 \in H \otimes N$. Assim, $\rho(bn) = b_1 n^{-1} \otimes b_2 \cdot n^0 \in H \otimes BN$, e portanto BN é um

H-comódulo à esquerda. Com isso, vimos também que a compatibilidade é satisfeita trivialmente, já que ela é satisfeita em M e temos $BN \subseteq M$.

Por fim, afirmamos que BN tem dimensão finita sobre $\Bbbk$. De fato, temos que tanto B quanto N tem dimensão finita sobre $\Bbbk$, assim, consideramos $\{b_1, ..., b_n\}$ e $\{n_1, ..., n_k\}$ $\Bbbk$-bases de B e N, respectivamente. Então, o conjunto $\{b_i n_j\}_{i,j}$, $i = 1, ..., n$ e $j = 1, ..., k$, é um conjunto finito e gerador de BN sobre $\Bbbk$, do qual podemos então extrair uma base, o que garante que BN tem dimensão finita sobre $\Bbbk$. □

Proposição 2.2.6. *Sejam H uma álgebra de Hopf e $B \subseteq H$ uma subálgebra de Hopf de H de dimensão finita. Se qualquer (H, B)-módulo de Hopf à esquerda de dimensão finita, não-nulo, é livre como B-módulo à esquerda, então qualquer que seja (H, B)-módulo de Hopf à esquerda é livre como um B-módulo à esquerda.*

Demonstração. Seja M um (H, B)-módulo de Hopf à esquerda não-nulo fixado. Definimos então o conjunto $\mathcal{F}$ consistindo de todo conjunto não-vazio X de M com a propriedade que BX é um (H, B)-módulo de Hopf e B-módulo livre com base X.

Pelo Lema 2.2.5, vimos que podemos considerar N um subcomódulo de dimensão finita de M, e com isso BN é um (H, B)-módulo de Hopf à esquerda, e BN tem dimensão finita sobre $\Bbbk$, donde temos então por hipótese que BN é um B-módulo livre. Assim, ele tem uma base sobre B, e denotando por X essa base, temos que $X \subseteq BN \subseteq M$. Desta maneira, temos que $BN = BX$ como B-módulo, e BX é um (H, B)-módulo de Hopf e B-módulo livre com base X. Logo, $X \in \mathcal{F}$ e assim $\mathcal{F}$ não é vazio.

Considere a ordem em $\mathcal{F}$ dada pela inclusão de conjuntos.

Se $(X_i)_{i \in I}$ é um subconjunto totalmente ordenado de $\mathcal{F}$, e consideramos $X = \cup_{i \in I} X_i$. Temos então que X é uma base sobre B do B-módulo BX. Como $BX = \sum_{i \in I} BX_i \subseteq M$, temos que BX é um (H, B)-módulo de Hopf à esquerda, livre sobre B e com base X, donde segue então que $X \in \mathcal{F}$. Logo, $X \in \mathcal{F}$ é uma cota superior para $(X_i)_{i \in I}$. Assim, pelo Lema de Zorn, temos um elemento maximal $Y \in \mathcal{F}$. Vamos provar que $BY = M$, pois se este é o caso, seguirá pelo fato de $Y \in \mathcal{F}$ que M é um (H, B)-módulo de Hopf e B-módulo livre com base Y.

Se por acaso $BY \neq M$, então M/BY é um (H, B)-módulo de Hopf à esquerda não-nulo. Logo, ele contém um (H, B)-módulo de Hopf de dimensão finita, que digamos ser S/BY, onde $BY \subseteq S \subseteq M$ e S é um (H, B)-módulo de Hopf à esquerda.

Pela hipótese, temos então que S/BY é livre como B-módulo. Considere então Z uma base de S/BY sobre B. Denotemos por Y' o subconjunto de S tal que $\pi(Y') = Z$, onde $\pi : S \longrightarrow S/BY$ é a projeção natural. Notemos que $Y' \neq \emptyset$ e $Y' \neq \{0\}$.

Então S é um B-módulo livre com base $Y \cup Y'$. Logo $Y \cup Y' \in \mathcal{F}$, e $Y \subsetneq Y \cup Y'$, o que contradiz a maximalidade de Y.

Portanto $BY = M$, donde concluímos que M é um B-módulo livre com base Y. □

Teorema 2.2.7. ***(Teorema de Nichols-Zöeller)*** *Sejam H uma álgebra de Hopf de dimensão finita e $B \subseteq H$ uma subálgebra de Hopf. Então qualquer (H, B)-módulo de Hopf à esquerda é um B-módulo livre.*

Em particular, H é B-módulo livre e $\dim_{\Bbbk}(B) | \dim_{\Bbbk}(H)$.

Demonstração. A Proposição 2.2.6 vista anteriormente mostra que é suficiente provarmos que a afirmação é válida para qualquer (H, B)-módulo de Hopf com dimensão finita.

Seja M um (H, B)-módulo de Hopf à esquerda com dimensão finita sobre $\Bbbk$. Em particular, M é um B-módulo finitamente gerado. Então, pela Proposição 2.2.4, temos que $H \otimes M \cong M^{\dim_{\Bbbk}(H)}$ como B-módulo à esquerda.

Além disso, como H tem dimensão finita, e B é uma subálgebra de Hopf de H, então B também tem dimensão finita.

Notemos que H é finitamente gerado e fiel como B-módulo à esquerda. Segue portanto da Proposição 2.2.2, tomando H como L e M como W na proposição, que M é B-módulo livre, como queríamos.

Em particular, pelo Exemplo 2.2.3, vimos que H é um (H, B)-módulo de Hopf à esquerda. Desta maneira, concluímos que H é um B-módulo livre.

Por último, do fato de H ser B-livre, existe um inteiro positivo q tal que $H \cong B^q$, como B-módulo. Assim, $H \cong B^q$ como $\Bbbk$-espaço vetorial, e segue que $\dim_{\Bbbk}(H) = \dim_{\Bbbk}(B^q) = q \dim_{\Bbbk}(B)$. Logo, $\dim_{\Bbbk}(B) | \dim_{\Bbbk}(H)$. □

Para encerrar, obtemos como colorário do Teorema de Nichols-Zöeller o Teorema de Lagrange para grupos finitos. Precisamente:

Corolário 2.2.8. ***(Teorema de Lagrange)*** *Sejam G um grupo finito e T um subgrupo de G. Então* $|T| \Big| |G|$.

Demonstração. Sejam G um grupo finito e T um subgrupo de G. Então $\Bbbk G$ é uma álgebra de Hopf de dimensão finita e $\Bbbk T$ é uma subálgebra de Hopf de $\Bbbk G$. Pelo Teorema de Nichols-Zöeller, temos que $\dim_{\Bbbk}(\Bbbk T) | \dim_{\Bbbk}(\Bbbk G)$.

Desde que $\dim_{\Bbbk}(\Bbbk G) = |G|$ e $\dim_{\Bbbk}(\Bbbk T) = |T|$, concluímos que $|T| \Big| |G|$.

□

Apêndice A

Apêndice: Teoria de Anéis e Módulos e o Teorema de Krull-Schmidt

O objetivo deste apêndice é apresentar o Teorema de Krull-Schmidt, um resultado clássico que afirma que todo módulo de comprimento finito tem uma decomposição em soma direta de submódulos indecomponíveis e que essa soma é única, a menos de isomorfismo. Todos os conceitos envolvidos são apresentados e provados ao longo do capítulo.

Neste capítulo, A sempre denotará um anel com unidade 1_A, não necessariamente comutativo e, além disso, $1_A \neq 0_A$. Nos referiremos a M como sendo simplesmente um A-módulo, para significar indistintamente que M é um A-módulo à esquerda ou um A-módulo à direita, quando não for dito explicitamente no contexto uma destas situações, e observamos que os resultados apresentados valem tanto para A-módulos à esquerda quanto para A-módulos à direita, onde as demonstrações são realizadas de forma análoga. Além disso, sempre consideramos M um módulo não nulo, isto é, $M \neq \{0\}$, exceto quando mencionado explicitamente que $M = \{0\}$.

A.1 Definições e Resultados Iniciais

Definição A.1.1. *Sejam A um anel e M um A-módulo. Definimos o* anel dos endomorfismos de M *como sendo o conjunto*

$$End(M) = End_A(M) = \{f : M \longrightarrow M | f \text{ é uma aplicação } A\text{-linear}\}$$

Notemos que $End(M)$ tem estrutura de anel, onde a soma é pontual e a multiplicação é dada pela composição de aplicações. Além disso, a unidade deste anel é dada pela identidade, isto é, $1_{End(M)} = Id_M$.

Definição A.1.2. *Seja A um anel. Dizemos que $a \in A$ é um elemento*

(*i*) nilpotente *se existe um inteiro positivo n tal que $a^n = 0$;*

(*ii*) inversível à direita *se existe $b \in A$ tal que $a \cdot b = 1_A$. Neste caso, dizemos que b é um inverso à direita para a;*

(*iii*) inversível à esquerda *se existe $b \in A$ tal que $b \cdot a = 1_A$. Neste caso, dizemos que b é um inverso à esquerda para a;*

(*iv*) inversível *se a é inversível à esquerda e à direita. Denotamos o conjunto dos elementos inversíveis de A por $U(A)$.*

Como consequência da definição anterior, temos a seguinte proposição:

Proposição A.1.3. *Seja A um anel. Temos:*

(*i*) *Se um elemento a é inversível à esquerda e à direita, então os inversos à direita e à esquerda coincidem.*

(*ii*) *Se um elemento a é inversível, então o inverso é único. Neste caso, denotamos por a^{-1} o inverso de a.*

Demonstração. (*i*) Seja b_1 um inverso à esquerda e b_2 um inverso à direita para a.
Então $b_1 a = 1 = ab_2$. Assim, $b_1 = b_1 1 = b_1(ab_2) = (b_1 a)b_2 = 1b_2 = b_2$.

(*ii*) Sejam b e b' inversos de a. Então $ba = 1 = ab$ e também $ab' = 1 = b'a$. Em particular, temos que b é um inverso à esquerda para a e b' é um inverso à direita para a, donde segue pelo item anterior que $b = b'$.

□

Definição A.1.4. *Seja A um anel. Definimos o* radical de A *como sendo a interseção de todos os ideais à esquerda maximais de A, e denotamos por $rad(A)$, ou seja, $rad(A) = \bigcap \mathfrak{M}$, onde $\mathfrak{M}$ percorre todos ideais à esquerda maximais de A.*

Observamos que em nossa definição de radical, estamos utilizando ideais maximais à esquerda, mas a mesma construção pode ser feita com ideais maximais à direita. Além disso, veremos que o radical é um ideal bilateral, e então, na verdade, as duas construções, à esquerda e à direita, nos levam exatamente ao mesmo ideal bilateral. Para mais informações sobre este assunto, indicamos [6].

Observação A.1.5. *Notemos que a contenção $rad(A) \subseteq (A \setminus U(A))$ sempre é válida. De fato, seja $y \in rad(A)$. Queremos provar que $y \in (A \setminus U(A))$. Suponhamos por absurdo que $y \in U(A)$. Então existe $a \in A$ tal que $ay = 1$. Desde que $y \in rad(A)$, temos que $y \in \mathfrak{M}$, para todo ideal à esquerda maximal $\mathfrak{M}$. Assim, $ay = 1 \in \mathfrak{M}$, para todo ideal à esquerda maximal $\mathfrak{M}$, ou seja, $\mathfrak{M} = A$ para todo ideal à esquerda maximal $\mathfrak{M}$, o que é um absurdo. Logo $y \notin U(A)$, e portanto $y \in (A \setminus U(A))$.*

Proposição A.1.6. *Sejam A um anel e $y \in A$. São equivalentes:*

(i) $y \in rad(A)$;

(ii) $1 - xy$ *é inversível à esquerda para qualquer* $x \in A$;

(iii) $yM = \{y \cdot m \mid m \in M\} = \{0\}$ *para qualquer A-módulo à esquerda simples M.*

Demonstração. $[(i) \implies (ii)]$ Seja $y \in rad(A)$. Suponha por absurdo que existe $x \in A$ tal que $1 - xy$ não é inversível à esquerda. Então existe $\mathfrak{M}_0$ ideal à esquerda maximal de A tal que $1 - xy \in \mathfrak{M}_0$. Como $y \in rad(A) = \bigcap \mathfrak{M}$, para todo $\mathfrak{M}$ ideal maximal à esquerda de A, temos que $y \in \mathfrak{M}_0$, e portanto $xy \in \mathfrak{M}_0$. Logo, $1 = (1-xy)+xy \in \mathfrak{M}_0$, o que é um absurdo. Portanto, $1-xy$ é inversível à esquerda para qualquer $x \in A$.

$[(ii) \implies (iii)]$ Sejam $1 - xy$ inversível à esquerda, para qualquer $x \in A$, e M um A-módulo à esquerda simples. Suponha por absurdo que exista $m \in M$ tal que $y \cdot m \neq 0$.

Como $A(y \cdot m) = \{x \cdot (y \cdot m) = (xy) \cdot m \quad | \quad x \in A\}$ é um submódulo de M, onde M é um A-módulo simples, temos que $A(y \cdot m) = \{0\}$ ou $A(y \cdot m) = M$. Como $y \cdot m \in A(y \cdot m)$ e $0 \neq y \cdot m$, concluímos que $A(y \cdot m) = M$. Assim, existe $x \in A$ tal que $m = xy \cdot m$, e com isso, $(1 - xy) \cdot m = 0$.

Por hipótese, temos que $1-xy$ é inversível, e então $1 \cdot m = (1-xy)^{-1}(1-xy) \cdot m = (1-xy)^{-1} \cdot 0 = 0$, ou seja, $m = 1 \cdot m = 0$. Portanto $y \cdot m = y \cdot 0 = 0$, uma contradição, pois $y \cdot m \neq 0$. Logo, $yM = \{0\}$ para qualquer A-módulo à esquerda M simples.

$[(iii) \implies (i)]$ Suponhamos que $yM = \{0\}$ para qualquer A-módulo à esquerda M simples. Note que, para qualquer $\mathfrak{M}$ ideal à esquerda maximal de A, temos que $A/\mathfrak{M}$ é um A-módulo à esquerda simples. De fato, desde que todo A-submódulo de $A/\mathfrak{M}$ é da forma $P/\mathfrak{M}$ onde P é um ideal à esquerda de A que contém $\mathfrak{M}$, e desde que $\mathfrak{M}$ é um ideal à esquerda maximal, temos que $P = A$ ou $P = \mathfrak{M}$, e portanto $P/\mathfrak{M} = A/\mathfrak{M}$ ou $P/\mathfrak{M} = \mathfrak{M}/\mathfrak{M} = \{0\}$. Logo, os únicos submódulos de $A/\mathfrak{M}$ são os triviais e com isso ele é um A-módulo simples. Então, pela hipótese temos que $y \cdot A/\mathfrak{M} = \{0_{A/\mathfrak{M}}\} = \{0 + \mathfrak{M}\}$.

Portanto, para todo $x \in A$, $y \cdot (x + \mathfrak{M}) = yx + \mathfrak{M} \in \{0 + \mathfrak{M}\}$. Assim, $yx + \mathfrak{M} = 0 + \mathfrak{M}$, e portanto $yx \in \mathfrak{M}$, donde temos que $y \in \mathfrak{M}$, tomando em particular $x = 1$. Como $\mathfrak{M}$ é um ideal à esquerda maximal qualquer de A, temos que $y \in \bigcap \mathfrak{M}$, onde $\mathfrak{M}$ percorre todos ideais à esquerda maximais de A, ou seja, $y \in rad(A)$. □

Definição A.1.7. *Sejam A um anel e M um A-módulo à esquerda. Definimos o* anulador *de M em A como sendo o conjunto*

$$ann_A(M) = \{a \in A \quad | \quad a \cdot m = 0, \quad \forall m \in M\}$$

Notemos que para qualquer A-módulo M, o $ann_A(M)$ é um ideal bilateral de A. De fato, $ann_A(M) \subseteq A$ e para quaisquer $a \in A$, $x, y \in ann_A(M)$ e $m \in M$ temos que $0_A, x - y \in ann_A(M)$:

- $0_A \cdot m = 0$;
- $(x - y) \cdot m = (x \cdot m) - (y \cdot m) = 0 - 0 = 0$.

E também temos que $ax, xa \in ann_A(M)$:

- $(ax) \cdot m = a \cdot (x \cdot m) = a \cdot 0 = 0$;
- $(xa) \cdot m = x \cdot (a \cdot m) = x \cdot n = 0$, onde $n := a \cdot m \in M$.

Corolário A.1.8. *Seja A um anel. Temos que $rad(A) = \bigcap ann_A(M)$, onde M percorre todos os A-módulos à esquerda simples. Em particular, temos que $rad(A)$ é um ideal bilateral de A.*

Demonstração. Este fato resulta imediatamente das condições (i) e (iii) da Proposição A.1.6. De fato, se $y \in rad(A)$, então pela Proposição A.1.6, temos que $yM = \{0\}$ para qualquer A-módulo à esquerda simples M, isto é, $y \in ann_A(M)$, para todo A-módulo à esquerda simples M, e portanto $y \in \bigcap ann_A(M)$, onde M percorre todos os A-módulos à esquerda simples.

Por outro lado, se $y \in \bigcap ann_A M$, onde M percorre todos os A-módulos à esquerda simples, então $y \in ann_A(M)$, para todo A-módulo à esquerda simples M, isto é, $yM = \{0\}$, para todo A-módulo à esquerda simples M. Então, pela Proposição A.1.6, temos que $y \in rad(A)$.

Em particular, como $rad(A) = \bigcap ann_A(M)$, temos que $rad(A)$ é um ideal bilateral de A, visto que é a interseção de ideais bilaterais. □

Lema A.1.9. *Seja A um anel. Então $a \in U(A)$ se, e somente se, $a + rad(A) \in U(A/rad(A))$.*

Demonstração. [$\Longrightarrow$] Seja $a \in U(A)$. Portanto existe $b \in A$ tal que $ab = ba = 1$. Então, passando ao quociente, temos que $(a + rad(A))(b + rad(A)) = (b + rad(A))(a + rad(A)) = 1 + rad(A)$. Logo, $a + rad(A) \in U(A/rad(A))$.

[$\Longleftarrow$] Suponhamos que $a + rad(A) \in U(A/rad(A))$. Então existe $b \in A$ tal que

$$(a + rad(A))(b + rad(A)) = (b + rad(A))(a + rad(A)) = 1 + rad(A).$$

Assim, $ab + rad(A) = ba + rad(A) = 1 + rad(A)$, e portanto

$$(1 + rad(A)) - (ba + rad(A)) = 0_{(A/rad(A)} = (1 + rad(A)) - (ab + rad(A)),$$

ou seja, $(1 - ba) + rad(A) = 0_{(A/rad(A)} = (1 - ab) + rad(A)$. Portanto,$1 - ba$ e $1 - ab \in rad(A)$, ou seja, $ba, ab \in 1 + rad(A)$.

Afirmamos agora que $1 + rad(A) \subseteq U(A)$. De fato, seja $1 + r \in 1 + rad(A)$. Pelo item (ii) da Proposição A.1.6, tomando $x = -1$ temos que $1 + r$ é inversível à esquerda. Seja $v \in A$ tal que $v(1 + r) = 1$. Temos então que v é inversível à direita. De $v(1 + r) = 1$, temos que $v + vr = 1$,

e portanto $v = 1 - vr$. Novamente pelo item (ii) da Proposição A.1.6, temos que v é inversível à esquerda. Portanto, $v \in U(A)$. Assim, multiplicando à esquerda $v(1 + r) = 1$ por v^{-1}, temos que $1 + r = v^{-1} \in U(A)$.

Logo, $ba, ab \in U(A)$. Em particular, existem $c, d \in A$ tais que $c(ba) = 1 = (ab)d$. Logo, a é inversível à esquerda e à direita, isto é, $a \in U(A)$. □

Proposição A.1.10. *Para qualquer anel A, as seguintes afirmações são equivalentes:*

(i) *A tem um único ideal à esquerda maximal;*

(ii) *$A/rad(A)$ é um anel de divisão;*

(iii) *$A \setminus U(A)$ é um ideal de A;*

(iv) *$A \setminus U(A)$ é um grupo com a operação de soma de A;*

(v) *Para qualquer inteiro positivo n, se $a_1 + a_2 + \cdots + a_n \in U(A)$, então $a_i \in U(A)$ para algum $i \in \{1, 2, ..., n\}$;*

(vi) *Se $a + b \in U(A)$, então $a \in U(A)$ ou $b \in U(A)$.*

Demonstração. $[(i) \implies (ii)]$ Suponha que $\mathfrak{M}$ seja o único ideal à esquerda maximal de A. Assim, $rad(A) = \mathfrak{M}$, e portanto $rad(A)$ é um ideal à esquerda maximal de A. Se I é um ideal à esquerda de $A/rad(A)$, temos que existe N um ideal à esquerda de A tal que $I = N/rad(A)$, com $rad(A) \subseteq N \subseteq A$. Mas pelo fato de $rad(A)$ ser maximal, temos que $N = rad(A)$ ou $N = A$, e portanto $I = \{0\}$ ou $I = A/rad(A)$. Logo, $A/rad(A)$ só tem os ideais à esquerda triviais, e portanto é um anel de divisão.

$[(ii) \implies (i)]$ Suponha que $A/rad(A)$ é um anel de divisão. Considere $\mathfrak{M}$ um ideal à esquerda maximal em A. Como $rad(A) \subseteq \mathfrak{M}$, temos que $\mathfrak{M}/rad(A)$ é um ideal à esquerda em $A/rad(A)$. Como $A/rad(A)$ é um anel de divisão, ele só tem ideais à esquerda triviais, logo $\mathfrak{M}/rad(A) = \{0\}$ ou $\mathfrak{M}/rad(A) = A/rad(A)$, ou seja $\mathfrak{M} = rad(A)$ ou $\mathfrak{M} = A$. Como $\mathfrak{M}$ é ideal à esquerda maximal, temos que $\mathfrak{M} \neq A$, donde concluímos então que $\mathfrak{M} = rad(A)$. Como $\mathfrak{M}$ foi qualquer, temos que A tem um único ideal à esquerda maximal, a saber $rad(A)$.

$[(ii) \implies (iii)]$ Suponha que $A/rad(A)$ é um anel de divisão. Vamos provar que $A \setminus U(A) = rad(A)$, e segue que $A \setminus U(A)$ é um ideal de A. Já sabemos que $rad(A) \subseteq (A \setminus U(A))$. Seja então $a \in (A \setminus U(A))$. Então $a \notin U(A)$. Então, pela Proposição A.1.9, $a + rad(A)$ não é inversível. Agora, por hipótese, $A/rad(A)$ é um anel de divisão, ou seja, todo elemento não-nulo é inversível. Logo, concluímos que $a + rad(A) = 0_{A/rad(A)}$. Assim, $a \in rad(A)$.

Com isso, temos que $A \setminus U(A) = rad(A)$, e portanto o resultado segue.

$[(iii) \implies (iv)]$ Se $A \setminus U(A)$ é um ideal de A, então, em particular, ele é um grupo com a operação de soma de A.

$[(iv) \Longrightarrow (v)]$ Seja n um inteiro positivo e suponha que $a_1 + a_2 + \cdots + a_n \in U(A)$. Supondo por absurdo que $a_i \notin U(A)$ para todo $i = 1, ..., n$, então $a_1 + a_2 + \cdots + a_n \notin U(A)$, pois por hipótese $A \setminus U(A)$ é um grupo com a soma, o que é um absurdo. Logo, existe $j \in \{1, ..., n\}$ tal que $a_j \in U(A)$.

$[(v) \Longrightarrow (vi)]$ Tomando em particular $i = 2$ no item (v), obtemos (vi).

$[(vi) \Longrightarrow (ii)]$ Suponhamos que se $x + y \in U(A)$, então $x \in U(A)$ ou $y \in U(A)$, para quaisquer $x, y \in A$.

Seja $a + rad(A) \in A/rad(A)$ tal que $a + rad(A) \neq 0$. Então $a \notin rad(A)$. Assim, existe um ideal maximal à esquerda $\mathfrak{M}$ de A tal que $a \notin \mathfrak{M}$.

Com isso, $\mathfrak{M} + Aa$ é um ideal à esquerda de A tal que $\mathfrak{M} \subsetneq \mathfrak{M} + Aa$, portanto $\mathfrak{M} + Aa = A$. Assim, existem $m \in \mathfrak{M}$ e $b \in A$ tais que $m + ba = 1$.

Como $m \notin U(A)$, concluímos pela hipótese que $ba \in U(A)$. Em particular, ba é inversível à esquerda. Seja $c \in A$ tal que $c(ba) = 1$, isto é, $(cb)a = 1$. Então, passando ao quociente, temos que $1 + rad(A) = (cb + rad(A))(a + rad(A))$, ou seja, $a + rad(A)$ é inversível à esquerda.

Temos também que $a + rad(A)$ é inversível à direita. De fato, note que $cb + rad(A) \neq 0$, então pela mesma construção que fizemos, existe $x \in A$ tal que $(x + rad(A))(cb + rad(A)) = 1 + rad(A)$. Observamos que $x + rad(A)$ é inversível à direita, e com isso

$$\begin{aligned}[(x + rad(A))(cb + rad(A))](a + rad(A)) &= (x + rad(A))[(cb + rad(A))(a + rad(A))] = \\ &= (x + rad(A))(1 + rad(A)) = (x + rad(A))\end{aligned}$$

Por outro lado, $[(x + rad(A))(cb + rad(A))](a + rad(A)) = (1 + rad(A))(a + rad(A)) = a + rad(A)$. Concluímos então que $a + rad(A) = x + rad(A)$, e portanto $a + rad(A)$ é inversível à direita.

Logo, qualquer elemento não-nulo de $A/rad(A)$ é inversível.

Portanto $A/rad(A)$ é um anel de divisão. □

Definição A.1.11. *Dizemos que um anel A é* local *se A satisfaz alguma, e portanto todas, das condições da Proposição A.1.10 acima.*

Definição A.1.12. *Sejam A um anel e I um ideal à esquerda de A. Dizemos que I é um* nil ideal à esquerda *se todo elemento de I é nilpotente.*

Proposição A.1.13. *Sejam A um anel e $x \in A$ um elemento nilpotente. Então $1 - x$ é inversível.*

Demonstração. Seja $x \in A$ um elemento nilpotente. Seja então n um inteiro positivo tal que $x^n = 0$. Note que $a := \sum_{i=0}^{n-1} x^i = 1 + x + x^2 + \cdots + x^{n-1}$ é o inverso de $1 - x$. De fato, temos

$$a(1 - x) = \left(\sum_{i=0}^{n-1} x^i\right)(1 - x) = \left(\sum_{i=0}^{n-1} x^i\right) - \left(\sum_{i=1}^{n} x^i\right) = x^0 - x^n = x^0 - 0 = x^0 = 1$$

E também vale

$$(1-x)a = (1-x)\left(\sum_{i=0}^{n-1} x^i\right) = \left(\sum_{i=0}^{n-1} x^i\right) - \left(\sum_{i=1}^{n} x^i\right) = x^0 - x^n = x^0 - 0 = x^0 = 1$$

Logo, $1-x$ é inversível, com $(1-x)^{-1} = \sum_{i=0}^{n-1} x^i = 1 + x + \cdots + x^{n-1}$. □

Proposição A.1.14. *Seja I um nil ideal à esquerda de A. Então $I \subseteq rad(A)$.*

Demonstração. Seja $y \in I$. Como I é um nil ideal de A, temos que y é nilpotente. Em particular, I é ideal à esquerda de A, portanto, para cada $a \in A$, temos que $ay \in I$, e portanto ay também é nilpotente. Assim, pela Proposição A.1.13, $1-ay$ é inversível, e em particular é inversível à esquerda, para todo $a \in A$. Portanto, pela Proposição A.1.6, temos que $y \in rad(A)$. Logo, $I \subseteq rad(A)$. □

Proposição A.1.15. *Seja A um anel tal que cada $a \in (A \setminus U(A))$ é nilpotente. Então A é um anel local.*

Demonstração. Suponhamos que a é nilpotente, para todo $a \in (A \setminus U(A))$.

Vamos provar que $(A \setminus U(A)) \subseteq rad(A)$. Seja $x \in (A \setminus U(A))$. Temos então que x é nilpotente. Consideremos então o menor inteiro positivo k tal que $x^k = 0$.

Afirmamos que $Ax = \{ax \mid a \in A\} \subseteq (A \setminus U(A))$. De fato, suponha que exista $a \in A$ tal que $ax \in U(A)$. Então existe $b \in A$ tal que $b(ax) = 1$. Por outro lado, temos que $ax(x^{k-1}) = ax^k = a0 = 0$, ou seja, $ax(x^{k-1}) = 0$, e portanto $b(ax(x^{k-1})) = 0$.

Mas por outro lado, $b(ax(x^{k-1})) = (b(ax))x^{k-1} = 1x^{k-1} = x^{k-1}$, o que contradiz o fato de k ser o menor inteiro positivo tal que $x^k = 0$. Logo, para todo $a \in A$ temos que $ax \notin U(A)$, ou seja, $ax \in (A \setminus U(A))$. Portanto, $Ax \subseteq (A \setminus U(A))$. Como todos elementos de Ax estão em $A \setminus U(A)$, e por hipótese todos elementos de $A \setminus U(A)$ são nilpotentes, temos que todos elementos de Ax são nilpotentes. Assim, temos que Ax é um nil ideal à esquerda. Então, pela Proposição A.1.14, temos que $Ax \subseteq rad(A)$. Como $x \in Ax$, temos que $x \in rad(A)$. Logo, $(A \setminus U(A)) \subseteq rad(A)$.

Como vimos na Observação A.1.5, sempre temos que $rad(A) \subseteq (A \setminus U(A))$. Portanto, temos que $(A \setminus U(A)) = rad(A)$.

Como vimos no Corolário A.1.8, temos que $rad(A)$ é um ideal de A, donde concluímos que $A \setminus U(A)$ é um ideal de A.

Segue então da condição (iii) da Proposição A.1.10 que A é um anel local. □

Definição A.1.16. *Seja $\mathcal{C} := \{C_i | i \in I\}$ uma família de subconjuntos de um conjunto C. Notemos que podemos considerar $\mathcal{C}$ como um conjunto parcialmente ordenado com a relação de ordem $\leq_1$ dada pela inclusão de conjuntos ou pela relação de ordem $\leq_2$ dada pela contenção de conjuntos. Isto é,*

$C_i \leq_1 C_j$ *se* $C_i \subseteq C_j$, *e* $C_i \leq_2 C_j$ *se* $C_i \supseteq C_j$. *Dizemos que um subconjunto* $\mathcal{S}$ *de* $\mathcal{C}$, $\mathcal{S}$ *não-vazio, é uma* cadeia *se* $\mathcal{S} = \{C_j | j \in J \subseteq \mathbb{N}\} \subseteq \mathcal{C}$ *é um conjunto enumerável e totalmente ordenado pela relação de ordem* $\leq_k, k \in \{1, 2\}$. *Isto é, se* $C_i, C_j \in \mathcal{S}$, *então* $C_i \subseteq C_j$ *ou* $C_j \subseteq C_i$. *Mais precisamente, dizemos que* $\mathcal{S}$ *é uma* cadeia ascendente *se estamos considerando* $\mathcal{S}$ *totalmente ordenado pela relação* $\leq_1$, *e dizemos que* $\mathcal{S}$ *é uma* cadeia descendente *se estamos considerando* $\mathcal{S}$ *totalmente ordenado pela relação* $\leq_2$. *Além disso, se* $C_i \neq C_j$, *para* $i \neq j$, *onde* $C_i, C_j \in \mathcal{S}$, *dizemos que a cadeia* $\mathcal{S}$ *é* estrita, *e quando* $\mathcal{S}$ *é um conjunto finito, dizemos que a cadeia é* finita.

Definição A.1.17. *Dizemos que uma família de subconjuntos* $\{C_i | i \in I\}$ *de um conjunto* C *satisfaz a* Condição de Cadeia Ascendente, *ou simplesmente que satisfaz* ACC *(do inglês Ascending Chain Condition), se não existe uma cadeia ascendente infinita com as inclusões estritas*

$$C_{i_1} \subsetneq C_{i_2} \subsetneq \cdots$$

nesta família.

Temos as seguintes equivalências:

Proposição A.1.18. *Seja* $\mathcal{C} := \{C_i | i \in I\}$ *uma família de subconjuntos de um conjunto* C. *São equivalentes:*

(*i*) $\mathcal{C}$ *satisfaz ACC;*

(*ii*) *Para qualquer cadeia ascendente em* $\mathcal{C}$,

$$C_{i_1} \subseteq C_{i_2} \subseteq \cdots$$

existe um inteiro positivo n *tal que* $C_{i_n} = C_{i_{n+1}} = \cdots$. *Neste caso, dizemos que a cadeia é* estacionária, *ou ainda que ela* estabiliza*;*

(*iii*) *Em qualquer subconjunto* $\mathcal{S}$ *de* $\mathcal{C}$, $\mathcal{S}$ *não-vazio, existe um elemento maximal com relação a ordem dada por* $\leq_1$. *Isto é, existe um elemento* $C_j \in \mathcal{S}$ *tal que se* $C_j \leq_1 C_k$, *então* $C_k = C_j$, *onde* $C_k \in \mathcal{S}$. *Isto significa que existe um elemento* $C_j \in \mathcal{S}$ *tal que se* $C_j \subseteq C_k$, *então* $C_k = C_j$, *onde* $C_k \in \mathcal{S}$.

Neste caso, dizemos que C_j *é um* elemento maximal de $\mathcal{S}$.

Demonstração. $[(i) \Longrightarrow (ii)]$

Provaremos a contrapositiva desta afirmação, isto é, se $\mathcal{C}$ não satisfaz a condição (ii), então também não satisfaz a condição (i).

Suponhamos que $\mathcal{C}$ não satisfaça a condição (ii).

Então existe uma cadeia ascendente em $\mathcal{C}$, digamos

$$C_{i_1} \subseteq C_{i_2} \subseteq \cdots$$

tal que, para qualquer inteiro positivo n, existe um k tal que $C_{i_n} \neq C_{i_{n+k}}$. Assim, para $n = 1$, existe k_1 tal que $C_{i_1} \neq C_{i_{1+k_1}}$. Para $n = 1 + k_1$, existe k_2 tal que $C_{i_{1+k_1}} \neq C_{i_{1+k_1+k_2}}$. Procedendo indutivamente desta forma, obtemos a seguinte cadeia ascendente infinita com as inclusões estritas

$$C_{i_1} \subsetneq C_{i_{1+k_1}} \subsetneq C_{i_{1+k_1+k_2}} \subsetneq \cdots$$

Assim, concluímos que $\mathcal{C}$ não satisfaz a condição (i).

$[(ii) \Longrightarrow (iii)]$

Seja $\mathcal{S} \neq \emptyset$ um subconjunto de $\mathcal{C}$. Tome um elemento qualquer C_1 em $\mathcal{S}$. Se não existe $C_{j_1} \neq C_1$ em $\mathcal{S}$ tal que $C_1 \subseteq C_{j_1}$, temos então que C_1 é um elemento maximal de $\mathcal{S}$. Agora, se existe um elemento $C_{j_1} \neq C_1$ em $\mathcal{S}$ tal que $C_1 \subseteq C_{j_1}$, consideramos a cadeia

$$C_1 \subseteq C_{j_1}$$

Repetimos então o argumento para C_{j_1}, isto é, se não existe $C_{j_2} \neq C_{j_1}$ em $\mathcal{S}$ tal que $C_{j_1} \subseteq C_{j_2}$, temos então que C_{j_1} é um elemento maximal de $\mathcal{S}$. Agora, se existe um elemento $C_{j_2} \neq C_{j_1}$ em $\mathcal{S}$ tal que $C_{j_1} \subseteq C_{j_2}$, consideramos a cadeia

$$C_1 \subseteq C_{j_1} \subseteq C_{j_2}$$

Este processo não pode se repetir infinitamente, isto é, em algum momento encontramos um elemento maximal de $\mathcal{S}$. De fato, se nunca encontrássemos um elemento maximal de $\mathcal{S}$, encontraríamos uma cadeia infinita da forma

$$C_1 \subseteq C_{j_1} \subseteq C_{j_2} \subseteq \cdots$$

Então, pela condição (ii), existe um inteiro positivo n tal que $C_{j_n} = C_{j_{n+1}} = \cdots$, o que é uma contradição devido a construção dos C_{j_k}'s, que garantem $C_{j_k} \neq C_{j_{k+1}}$ para todo inteiro positivo k.

$[(iii) \Longrightarrow (i)]$

Também provaremos a contrapositiva, isto é, se $\mathcal{C}$ não satisfaz a condição (i), então também não pode satisfazer a condição (iii).

Suponhamos então que $\mathcal{C}$ não satisfaz ACC. Isto é, existe uma cadeia ascendente infinita com as inclusões estritas da forma

$$C_{i_1} \subsetneq C_{i_2} \subsetneq \cdots$$

Considere então o subconjunto $\mathcal{S} = \{C_{i_j}, j = 1, 2, ...\}$.

Temos que $\mathcal{S} \neq \emptyset$ e é tal que não existe um elemento maximal em $\mathcal{S}$, desde que para todo inteiro positivo k temos $C_{i_k} \subsetneq C_{i_{k+1}}$. □

Analogamente ao que foi feito com uma cadeia ascendente, temos para uma cadeia descendente. Isto é:

Definição A.1.19. *Dizemos que uma família de subconjuntos $\{C_i | i \in I\}$ de um conjunto C satisfaz a* Condição de Cadeia descendente*, ou simplesmente que satisfaz* DCC *(do inglês Descending Chain Condition), se não existe uma cadeia descendente infinita com as contenções estritas*

$$C_{i_1} \supsetneq C_{i_2} \supsetneq \cdots$$

nesta família.

Temos também as seguintes equivalências:

Proposição A.1.20. *Seja $\mathcal{C} := \{C_i | i \in I\}$ uma família de subconjuntos de um conjunto C. São equivalentes:*

(*i*) *$\mathcal{C}$ satisfaz DCC;*

(*ii*) *Para qualquer cadeia descendente em $\mathcal{C}$,*

$$C_{i_1} \supseteq C_{i_2} \supseteq \cdots$$

existe um inteiro positivo n tal que $C_{i_n} = C_{i_{n+1}} = \cdots$. Neste caso, também dizemos que a cadeia é estacionária*, ou ainda que ela* estabiliza*;*

(*iii*) *Em qualquer subconjunto $\mathcal{S}$ de $\mathcal{C}$, $\mathcal{S}$ não-vazio, existe um elemento maximal com relação a ordem dada por $\leq_2$. Isto é, existe um elemento $C_j \in \mathcal{S}$ tal que se $C_j \leq_2 C_k$, então $C_k = C_j$, onde $C_k \in \mathcal{S}$. Isto significa que existe um elemento $C_j \in \mathcal{S}$ tal que se $C_j \supseteq C_k$, então $C_k = C_j$, onde $C_k \in \mathcal{S}$.*

Neste caso, dizemos que C_j é um elemento minimal de $\mathcal{S}$.

Demonstração. $[(i) \Longrightarrow (ii)]$

Provaremos a contrapositiva desta afirmação, isto é, se $\mathcal{C}$ não satisfaz a condição (ii), então também não satisfaz a condição (i).

Suponhamos que $\mathcal{C}$ não satisfaça a condição (ii).

Então existe uma cadeia descendente em $\mathcal{C}$, digamos

$$C_{i_1} \supseteq C_{i_2} \supseteq \cdots$$

tal que, para qualquer inteiro positivo n, existe um k tal que $C_{i_n} \neq C_{i_{n+k}}$. Assim, para $n = 1$, existe k_1 tal que $C_{i_1} \neq C_{i_{1+k_1}}$. Para $n = 1 + k_1$, existe k_2 tal que $C_{i_{1+k_1}} \neq C_{i_{1+k_1+k_2}}$. Procedendo indutivamente desta forma, obtemos a seguinte cadeia ascendente infinita com as contenções estritas

$$C_{i_1} \supsetneq C_{i_{1+k_1}} \supsetneq C_{i_{1+k_1+k_2}} \supsetneq \cdots$$

Assim, concluímos que $\mathcal{C}$ não satisfaz a condição (i).

$[(ii) \Longrightarrow (iii)]$

Seja $\mathcal{S} \neq \emptyset$ um subconjunto de $\mathcal{C}$. Tome um elemento qualquer C_1 em $\mathcal{S}$. Se não existe $C_{j_1} \neq C_1$ em $\mathcal{S}$ tal que $C_1 \supseteq C_{j_1}$, temos então que C_1 é um elemento minimal de $\mathcal{S}$. Agora, se existe um elemento $C_{j_1} \neq C_1$ em $\mathcal{S}$ tal que $C_1 \supseteq C_{j_1}$, consideramos a cadeia

$$C_1 \supseteq C_{j_1}$$

Repetimos então o argumento para C_{j_1}, isto é, se não existe $C_{j_2} \neq C_{j_1}$ em $\mathcal{S}$ tal que $C_{j_1} \supseteq C_{j_2}$, temos então que C_{j_1} é um elemento minimal de $\mathcal{S}$. Agora, se existe um elemento $C_{j_2} \neq C_{j_1}$ em $\mathcal{S}$ tal que $C_{j_1} \supseteq C_{j_2}$, consideramos a cadeia

$$C_1 \supseteq C_{j_1} \supseteq C_{j_2}$$

Este processo não pode se repetir infinitamente, isto é, em algum momento encontramos um elemento minimal de $\mathcal{S}$. De fato, se nunca encontrássemos um elemento minimal de $\mathcal{S}$, encontraríamos uma cadeia infinita da forma

$$C_1 \supseteq C_{j_1} \supseteq C_{j_2} \supseteq \cdots$$

Então, pela condição (ii), existe um inteiro positivo n tal que $C_{j_n} = C_{j_{n+1}} = \cdots$, o que é uma contradição devido a construção dos C_{j_k}'s, que garantem $C_{j_k} \neq C_{j_{k+1}}$ para todo inteiro positivo k.

$[(iii) \Longrightarrow (i)]$

Também provaremos a contrapositiva, isto é, se $\mathcal{C}$ não satisfaz a condição (i), então também não pode satisfazer a condição (iii).

Suponhamos então que $\mathcal{C}$ não satisfaz ACC. Isto é, existe uma cadeia descendente infinita com as contenções estritas da forma

$$C_{i_1} \supsetneq C_{i_2} \supsetneq \cdots$$

Considere então o subconjunto $\mathcal{S} = \{C_{i_j}, j = 1, 2, ...\}$.

Temos que $\mathcal{S} \neq \emptyset$ e é tal que não existe um elemento minimal em $\mathcal{S}$, desde que para todo inteiro positivo k temos $C_{i_k} \supsetneq C_{i_{k+1}}$. □

Definição A.1.21. *Sejam A um anel e M um A-módulo. Dizemos que M é* noetheriano *se a família dos submódulos de M satisfaz ACC.*

Definição A.1.22. *Sejam A um anel e M um A-módulo. Dizemos que M é* artiniano *se a família dos submódulos de M satisfaz DCC.*

Note que o módulo nulo $M = \{0\}$ satisfaz trivialmente ACC e DCC.

Observação A.1.23. *Se M é um A-módulo que satisfaz ACC, respectivamente DCC, e $N \subseteq M$ é um submódulo de M, então N também satisfaz ACC, respectivamente DCC. Isto é claro, desde que todo submódulo de N é também um submódulo de M, e desde que não haja uma cadeia ascendente infinita com contenções estritas na família dos submódulos de M, também não pode haver na família dos submódulos de N, desde que a família dos submódulos de N está contida na família dos submódulos de M, portanto N satisfaz ACC. Respectivamente, se não há uma cadeia descendente infinita com as contenções estritas na família dos submódulos de M, também não pode haver na família dos submódulos de N, portanto N satisfaz DCC.*

Observação A.1.24. *Observamos que a partir de qualquer cadeia da forma*

$$\{0\} = M_k \subseteq M_{k-1} \subseteq \cdots \subseteq M_0 = M \qquad (C)$$

podemos obter uma nova cadeia (C'), onde as inclusões são estritas

$$\{0\} = M_t \subsetneq M_{t-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (C')$$

simplesmente eliminando os módulos iguais. Neste caso, $t \leq k$

Definição A.1.25. *Seja M um A-módulo e considere*

$$\{0\} = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (S)$$

uma cadeia estrita e finita de submódulos de M. Dizemos que a cadeia

$$\{0\} = N_s \subseteq N_{s-1} \subseteq \cdots \subseteq N_0 = M \qquad (S')$$

é um refinamento *para (S) se para cada $i \in \{0, 1, ..., r\}$ existe $j \in \{0, 1, ..., s\}$ tal que $M_i = N_j$. Além disso, dizemos que (S') é um* refinamento próprio *de (S) se existe $j \in \{0, 1, ..., s\}$ tal que $N_j \neq M_i$ para todo $i \in \{0, 1, ..., r\}$.*

Em outras palavras, um refinamento de uma cadeia consiste em inserir submódulos nela, contudo, nada nos impediria de repetir um submódulo que já estivesse na cadeia, pois no refinamento não exigimos que as inclusões sejam próprias. Para evitar este tipo de situação, definimos então um refinamento próprio. Isto é, uma cadeia admite um refinamento próprio se conseguirmos inserir algum submódulo nela que seja diferente dos que já estão lá.

Definição A.1.26. *Seja M um A-módulo. Dizemos que a cadeia estrita e finita*

$$\{0\} = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (S)$$

é uma série de composição *se ela não admite um refinamento próprio. Neste caso, dizemos que o* comprimento *de (S) é r, isto é, a quantidade de inclusões estritas existentes na cadeia.*

Como vimos acima, a cadeia não admite um refinamento próprio quando não é possível inserir nenhum submódulo novo nela. Desta forma, uma série de composição é precisamente a maior cadeia que conseguiremos com os submódulos em questão. Podemos convencionar que o módulo nulo $M = \{0\}$ tem uma única série de composição, dada pelo próprio módulo, e esta tem comprimento 0.

Definição A.1.27. *Dizemos que um A-módulo M é* simples *se os únicos submódulos de M são os triviais. Isto é, se $N \subseteq M$ é um submódulo de M, então $N = \{0\}$ ou $N = M$.*

Obviamente, $\{0\}$ é um A-módulo simples.

A proposição a seguir nos fornece um método para verificar quando que uma dada cadeia é uma série de composição.

Proposição A.1.28. *Seja M um A-módulo. Então*

$$\{0\} = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (S)$$

é uma série de composição se, e somente se, o quociente M_{i-1}/M_i é um A-módulo simples, para cada $i = 1, 2, ...r$.

Demonstração. [$\Longrightarrow$] Suponhamos que (S) seja uma série de composição. Então (S) não admite um refinamento próprio. Queremos provar que M_{i-1}/M_i é um módulos simples, para cada $i = 1, 2, ..., r$. Suponhamos por absurdo que existe $j \in \{1, 2, ..., r\}$ tal que M_{j-1}/M_j não seja simples. Então existe $P \subsetneq M_{j-1}/M_j$ submódulo próprio de M_{j-1}/M_j e $P \neq \{0\}$. Então, temos que $P = N/M_j$, onde $N \subsetneq M_{j-1}$ é um submódulo próprio de M_{j-1} que contém propriamente M_j, isto é, $M_j \subsetneq N$ é submódulo de N.

Formamos então a seguinte cadeia, supondo sem perda de generalidade que $1 < j < r - 1$,

$$\{0\} = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_j \subsetneq N \subsetneq M_{j-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (S')$$

e vemos que (S') é um refinamento próprio para (S), o que é um absurdo. Logo, M_{i-1}/M_i é um módulo simples, para cada $i = 1, 2, ..., r$.

[$\Longleftarrow$] Suponhamos agora que M_{i-1}/M_i é um A-módulo simples para cada $i \in \{1, 2, ..., r\}$. Vamos provar que a cadeia (S) não admite um refinamento próprio, e assim então (S) será uma série de composição. Podemos, sem perda de generalidade, considerar um refinamento de (S) da seguinte forma

$$\{0\} = M_r \subsetneq M_{r-1} \subsetneq \cdots \subsetneq M_j \subseteq N \subseteq M_{j-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (S')$$

Então $N/M_j \subseteq M_{j-1}/M_j$, e como M_{j-1}/M_j é um A-módulo simples, temos $N/M_j = \{0\}$ ou $N/M_j = M_{j-1}/M_j$, isto é, $N = M_j$ ou $N = M_{j-1}$. Assim, (S') não é um refinamento próprio para (S). Como todo refinamento de (S) pode ser analisado como analisamos (S') numa quantidade finita de vezes, concluímos que nenhum refinamento para (S) pode ser um refinamento próprio, donde segue então que (S) é uma série de composição. □

Um módulo pode ter mais de uma série de composição. Vejamos o seguinte exemplo:

Exemplo A.1.29. *Considere $\mathbb{Z}_{30}$ como $\mathbb{Z}$-módulo. Note que*

$$\{0\} \subsetneq \bar{10}\mathbb{Z}_{30} \subsetneq \bar{5}\mathbb{Z}_{30} \subsetneq \mathbb{Z}_{30} \qquad (S.1)$$

e

$$\{0\} \subsetneq \bar{15}\mathbb{Z}_{30} \subsetneq \bar{3}\mathbb{Z}_{30} \subsetneq \mathbb{Z}_{30} \qquad (S.2)$$

são duas séries de composições distintas.

De fato, todo $\mathbb{Z}$-submódulo de $\mathbb{Z}_{30}$ é da forma $\bar{n}\mathbb{Z}_{30}$, com $n = 0, 1, 2.., 29$.

Além disso, $\bar{n}\mathbb{Z}_{30}$ é submódulo de $\bar{m}\mathbb{Z}_{30}$ se e somente se $m|n$.

E mais, $\bar{n}\mathbb{Z}_{30} = \overline{mdc\{n, 30\}}\mathbb{Z}_{30}$.

Com isso, vemos que tanto $(S.1)$ quanto $(S.2)$ não admitem refinamento próprio, e são portanto séries de composição.

No exemplo anterior, exibimos duas séries de composição distintas para $\mathbb{Z}_{30}$ como $\mathbb{Z}$-módulo, entretanto, ambas possuem o mesmo comprimento, a saber 3. Veremos a seguir que podemos falar em comprimento de módulo, definindo como sendo o comprimento de alguma série de composição, e estará bem definido, pois veremos que duas séries de composição quaisquer de um dado módulo possuem o mesmo comprimento. Antes, vejamos uma observação que nos será útil para a prova deste resultado.

Observação A.1.30. *Sejam M um A-módulo, $M' \subseteq M$ e $N \subseteq M$ dois A-submódulos de M. Considere $N' = N \bigcap M'$ e defina $\iota : N/N' \longrightarrow M/M'$ por $\iota(x + N') = x + M'$, para $x \in N$. Vemos que ι está bem definida, pois se $x + N' = y + N'$, para $x, y \in N$, então $x - y \in N' = N \cap M'$, e assim $x - y \in M'$, donde concluímos que $x + M' = y + M'$. Além disto, vamos provar que esta aplicação ι é um homomorfismo de A-módulos injetor, e isto nos permitirá ver $\frac{N}{N'}$ como submódulo de $\frac{M}{M'}$, já que $\frac{N}{N'} \cong \iota(\frac{N}{N'})$, pois ι é um A-homomorfismo injetor, e $\iota(\frac{N}{N'}) \subseteq \frac{M}{M'}$ é submódulo de $\frac{M}{M'}$. Vamos provar que de fato ι é um homomorfismo de A-módulos injetor. Sejam $x + N', y + N' \in N/N'$ e $a \in A$. Então:*

(*i*) $\underline{\iota((x + N') + (y + N')) = \iota(x + N') + \iota(y + N') :}$

$\iota((x+N')+(y+N')) = \iota((x+y)+N') = (x+y)+M' = (x+M')+(y+M') = \iota(x+N')+\iota(y+N').$

(*ii*) $\underline{\iota(a \cdot (x + N')) = a \cdot \iota(x + N') :}$

$\iota(a \cdot (x + N')) = \iota(ax + N') = ax + M' = a \cdot (x + M') = a \cdot \iota(x + N').$

(*iii*) $\underline{\iota \text{ é injetor:}}$

Suponha que $\iota(x+N') = \iota(y+N')$. Isto significa que $x+M' = y+M'$, e portanto $x-y \in M'$. Como $x, y \in N$, e N é submódulo de M, temos $x-y \in N$. Assim $x-y \in N \cap M' = N'$, e portanto $x+N' = y+N'$.

Proposição A.1.31. *Se um A-módulo M tem uma série de composição de comprimento r, então toda série de composição de M tem comprimento r e qualquer cadeia com t inclusões estritas, é tal que $t \leq r$ e pode ser estendida a uma série de composição.*

Demonstração. Suponha que M tenha uma série de composição (T) de comprimento r. Denotemos por $l(M)$ o menor comprimento de uma série de composição de M. Então temos que

$$l(M) \leq r. \tag{A.1}$$

Afirmação 1: Se $N \subsetneq M$ é um submódulo próprio de M, então $l(N) < l(M)$.

De fato, seja $l(M) = s$ e

$$\{0\} = M_s \subsetneq M_{s-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (S)$$

uma série de composição que satisfaça esse comprimento. Então, pela Proposição A.1.28 temos que M_{i-1}/M_i é um módulo simples, para cada $i = 1, 2, ..., s$. Consideramos agora os submódulos de N dados por $N_i = N \cap M_i$, para $i = 0, 1, ..., s$. Formamos então a seguinte cadeia

$$\{0\} = N_s \subseteq N_{s-1} \subseteq \cdots \subseteq N_0 = N \qquad (S')$$

Pela Observação A.1.30, temos que para cada $i = 1, 2, ...s$, fixado, podemos identificar $N_{i-1}/N_i \cong \iota(N_{i-1}/N_i)$ através do homomorfismo injetor ι, e como $\iota(N_{i-1}/N_i) \subseteq M_{i-1}/M_i$, onde M_{i-1}/M_i é um módulo simples, nós temos então que $\iota(N_{i-1}/N_i) = \{0\}$ ou $\iota(N_{i-1}/N_i) = M_{i-1}/M_i$, isto é $N_{i-1}/N_i = \{0\}$, e neste caso $N_{i-1} = N_i$, ou $N_{i-1}/N_i \cong M_{i-1}/M_i$, e neste caso então N_{i-1}/N_i é simples. Assim, podemos eliminar os submódulos que se repetem na cadeia (S'), e a cadeia que resta é uma série de composição para N, pois os quocientes dos módulos restantes são simples. Neste caso, esta série de composição que resulta tem comprimento $k = s - j$, onde j é a quantidade de módulos repetidos que aparecem em (S'). Como, por definição, $l(N)$ é o comprimento da menor série de composição de N, temos $l(N) \leq k \leq s = l(M)$.

Logo, concluímos que $l(N) \leq l(M)$.

Suponhamos agora que seja $l(N) = l(M)$. Vamos provar então que $N = M$, o que é um absurdo, visto que estamos supondo que N seja um submódulo próprio de M. Como $l(N) = l(M)$, temos $k = s$ e portanto $j = 0$, isto é, não existem módulos repetidos em (S'). Já temos $N_s = \{0\} = M_s$. Note que, como $N_{s-1} = N \cap M_{s-1}$, temos $N_{s-1} \subseteq M_{s-1}$. E como não temos módulos repetidos em $(S'), N_{s-1} \neq N_s$. Temos então, $N_{s-1} = M_{s-1}$. De fato, se tivessemos $N_{s-1} \subsetneq M_{s-1}$, conseguiríamos um refinamento próprio de (S), dado por

$$\{0\} = M_s \subsetneq N_{s-1} \subsetneq M_{s-1} \subsetneq \cdots \subsetneq M_0 = M \qquad (R)$$

o que seria um absurdo, pois (S) é uma série de composição e portanto não admite refinamento próprio. Logo, temos $N_{s-1} = M_{s-1}$. Procedento indutivamente, obtemos $N_i = M_i$ para todo $i = s, s-1, ..., 1, 0$, donde obtemos $N = N_0 = M_0 = M$, o que contradiz o fato de N ser um submódulo próprio de M.

Com isso, provamos a Afirmação 1. Precisamente, concluímos que se $N \subseteq M$ é um submódulo, então $l(N) \leq l(M)$, onde a igualdade só ocorre se $N = M$. Ou seja, se $N \subsetneq M$ é um submódulo próprio, então $l(N) < l(M)$.

Afirmação 2: Qualquer cadeia com t inclusões estritas, é tal que $t \leq l(M)$.

De fato, seja

$$M_t \subsetneq M_{t-1} \subsetneq \cdots \subsetneq M_0$$

uma cadeia com t inclusões estritas. Podemos refinar esta cadeia para a seguinte

$$\{0\} \subseteq M_t \subsetneq M_{t-1} \subsetneq \cdots \subsetneq M_0 \subseteq M$$

Então, pela **Afirmação 1**, nós temos

$$l(M) \geq l(M_0) > l(M_1) > \cdots > l(M_t) \geq l(\{0\}) = 0.$$

Assim,

$$l(M_t) \geq 0, l(M_{t-1}) \geq 1, ..., l(M_1) \geq t-1, l(M_0) \geq t, l(M) \geq l(M_0).$$

Portanto, $l(M) \geq t$.

Com isso, provamos nossa afirmação, ou seja, qualquer cadeia com t inclusões estritas é tal que $t \leq l(M)$.

Note que a série de composição (T) é, em particular, uma cadeia com r inclusões estritas. Então, pela **Afirmação 2**, temos

$$r \leq l(M). \tag{A.2}$$

Segue portanto de (A.1) e (A.2) a igualdade $r = l(M)$.

Portanto, toda série de composição tem o mesmo comprimento $l(M)$. Por último, vejamos que toda cadeia com t inclusões estritas, e portanto $t \leq l(M)$ pela **Afirmação 2**, pode ser estendida a uma série de composição.

Considere (S) uma cadeia qualquer. Pela Observação A.1.24, podemos pensar que esta cadeia tem somente inclusões estritas. Digamos que ela tem t inclusões estritas. Se $t = l(M)$, então ela é uma série de composição. De fato, se ela não é uma série de composição, então ela admite um refinamento próprio, e a cadeia resultante terá $t+1$ inclusões próprias, e então pela **Afirmação 2**,

temos $t+1 \leq l(M) = t$, um absurdo. Também pela **Afirmação 2**, não podemos ter $t > l(M)$. Se $t < l(M)$, então ela não é uma série de composição, pois se fosse já mostramos que seria $t = l(M)$. Assim, a cadeia admite um refinamento próprio, e a cadeia resultante terá r inclusões estritas, com $r \geq t+1$. Analisamos agora essa cadeia resultante, donde concluímos também que, se $r = l(M)$, então ela é uma série de composição, e como não podemos ter $r > l(M)$, se $r \neq l(M)$, então $r < l(M)$ e com isso concluímos que ela também não é uma série de composição, donde tomamos então um refinamento próprio, e obtemos uma nova cadeia, e assim indutivamente até que tenhamos obtido uma série de composição para nossa cadeia original. □

A proposição acima nos permite falar em comprimento de um módulo, já que quando este possui uma série de composição de comprimento r, então qualquer outra série de composição também terá comprimento r. Assim, temos a seguinte definição:

Definição A.1.32. *Dizemos que um A-módulo M tem comprimento finito r se M tem uma série de composição de comprimento r.*

Observação A.1.33. *Observe que a **Afirmação 2** do teorema anterior nos garante que, quando um módulo M tem comprimento finito, então quaquer submódulo $N \subseteq M$ também tem comprimento finito. E mais do que isso, se $N \subsetneq M$, então o comprimento de N é estritamente menor que o comprimento de M.*

Vejamos agora que exigir que um módulo M tenha comprimento finito é equivalente a exigir que este módulo seja artiniano e noetheriano.

Proposição A.1.34. *Um A-módulo M tem comprimento finito se, e somente se, é noetheriano e artiniano.*

Demonstração. Note que se $M = \{0\}$ a equivalência é satisfeita. Suponhamos então $M \neq \{0\}$.

[$\Longrightarrow$] Suponha que M tenha comprimento finito. Então M admite uma série de composição de comprimento finito r. Suponha agora por absurdo que M não é artiniano ou noetheriano. Ou seja, M não satisfaz ACC ou DCC.

Se M não é artiniano, existe uma cadeia estrita e infinita da forma

$$M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_{r+1} \supsetneq \cdots$$

de onde conseguimos extrair a seguinte cadeia finita de contenções estritas

$$M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_{r+1} \supsetneq \{0\}$$

Note que esta cadeia tem $r+1$ inclusões estritas, donde pela **Afirmação 2** da Proposição A.1.31 obtemos que $r+1 \leq r$, um absurdo.

Se M não é noetheriano, existe uma cadeia estrita e infinita da forma

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{r+1} \subsetneq \cdots$$

de onde conseguimos extrair a seguinte cadeia finita de inclusões estritas

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{r+1} \subsetneq M$$

Note que esta cadeia tem $r+1$ inclusões estritas, donde segue novamente pela **Afirmação 2** da Proposição A.1.31 que $r+1 \leq r$, um absurdo.

Como ambos casos nos levam a um absurdo, temos que M é artiniano e noetheriano.

[$\Longleftarrow$] Suponha que M é artiniano e noetheriano. Então M satisfaz ACC e DCC. Considere agora a família $\mathcal{S}$ de todos submódulos de M, isto é, $\mathcal{S} = \{N \subseteq M \mid \text{N é submódulo de M}\}$.

Construímos agora, $\mathcal{S}_0 := \{N \subsetneq M \mid \text{N é submódulo de M}\}$.

Note que $\mathcal{S}_0 \subseteq \mathcal{S}$ e $\mathcal{S}_0 \neq \emptyset$, pois $\{0\} \in \mathcal{S}_0$. Como M satisfaz ACC, pelo item (iii) da Proposição A.1.18, temos que $\mathcal{S}_0$ tem um elemento maximal, digamos M_1.

Seja agora $\mathcal{S}_1 := \{N \subsetneq M_1 \mid \text{N é submódulo de } M_1\}$. Se $\mathcal{S}_1 \neq \emptyset$, então, como M_1 também satisfaz ACC pela Observação A.1.23, existe M_2 submódulo maximal em $\mathcal{S}_1$. Procedendo indutivamente desta forma, obtemos a seguinte cadeia

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$$

Agora, como M satisfaz DCC, esta cadeia precisa ser finita. Digamos

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_r \qquad (S)$$

Afirmamos agora que, sem perda de generalidade, podemos considerar um inteiro r tal que $M_r = \{0\}$.

De fato, se $M_r \neq \{0\}$, então $\{0\} \in \mathcal{S}_r$, donde teríamos $\mathcal{S}_r \neq \emptyset$ e portanto teríamos M_{r+1} elemento maximal de $\mathcal{S}_r$ e estenderíamos nossa cadeia à

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_r \supsetneq M_{r+1}$$

Assim, se $M_{r+1} \neq \{0\}$, repetiríamos o processo, obtendo M_{r+2} e a cadeia

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_r \supsetneq M_{r+1} \supsetneq M_{r+2}$$

e assim indutivamente, e como esse processo não pode se repetir infinitamente, pois nesse caso teríamos uma cadeia infinita, existe um inteiro positivo k tal que $\mathcal{S}_{r+k} = \emptyset$, donde $M_{r+k} = \{0\}$ e consideraríamos então

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_r \supsetneq \cdots \supsetneq M_{r+k} = \{0\}$$

Portanto, consideremos nossa cadeia inicial (S), onde já estamos admitindo que $M_r = \{0\}$.

Afirmamos agora que (S) é uma série de composição para M, garantindo assim que M tenha comprimento finito r.

Para provarmos isso, vamos provar que M_i/M_{i+1} é simples, para cada $i = 0, 1, ..., r-1$,, donde o resultado segue então pela Proposição A.1.28.

Suponhamos por absurdo que exista $j \in \{0, 1, ..., r-1\}$ tal que M_j/M_{j+1} não seja simples. Então temos que existe P tal que $\{0\} \subsetneq P \subsetneq M_j/M_{j+1}$, donde temos que existe N tal que $P = N/M_{j+1}$ com $M_{j+1} \subsetneq N \subsetneq M_j$, mas isto contradiz o fato de M_{j+1} ser um elemento maximal da família $\mathcal{S}_j$.

Logo, M_i/M_{i+1} é simples para cada $i = 0, 1, ..., r-1$.

Portanto, pela Proposição A.1.28, (S) é uma série de composição para M. □

Teorema A.1.35. ***(Decomposição Fitting)*** *Sejam A um anel e M um A-módulo à esquerda de comprimento finito. Para qualquer endomorfismo $f \in E := End_A(M)$, nós temos*

$$M = ker(f^n) \oplus im(f^n)$$

para qualquer inteiro n suficientemente grande.

Demonstração. Temos as duas cadeias de submódulos seguintes:

$$M \supseteq im(f) \supseteq im(f^2) \supseteq \cdots$$

e

$$\{0\} \subseteq ker(f) \subseteq ker(f^2) \subseteq \cdots .$$

De fato, como $f : M \longrightarrow M$, temos $im(f) \subseteq M$ e para qualquer inteiro positivo k temos que, se $y \in im(f^k)$, então existe $x \in M$ tal que $f^k(x) = y$, e portanto $y = f^{k-1}(f(x))$, ou seja, $y \in im(f^{k-1})$. Temos $\{0\} \subseteq ker(f)$, e se $y \in ker(f^k)$, então $f^k(y) = 0$, e segue que $f^{k+1}(y) = f(f^k(y)) = f(0) = 0$, e portanto $y \in ker(f^{k+1})$.

Como M tem comprimento finito, então pela Proposição A.1.34, M satisfaz ACC e DCC, e portanto ambas cadeias precisam estabilizar. Assim, existem r, s inteiros positivos tais que

$$im(f^r) = im(f^{r+1}) = \cdots$$

e

$$ker(f^s) = ker(f^{s+1}) = \cdots$$

Seja n um inteiro positivo tal que $n \geq \max\{r, s\}$, isto é, $n \geq r$ e $n \geq s$. Note que ambas cadeias estabilizam para esse n, isto significa que

$$im(f^n) = im(f^{n+1}) = \cdots \qquad \text{e} \qquad ker(f^n) = ker(f^{n+1}) = \cdots$$

Afirmamos que $M = ker(f^n) \oplus im(f^n)$.

Mostraremos primeiro que a interseção é nula. Seja $a \in ker(f^n) \cap im(f^n)$. Como $a \in ker(f^n)$, temos que $f^n(a) = 0$, e como $a \in im(f^n)$, temos que existe $b \in M$ tal que $a = f^n(b)$. Assim, $f^{2n}(b) = f^n(f^n(b)) = f^n(a) = 0$, ou seja, $b \in ker(f^{2n}) = ker(f^n)$, e então, $a = f^n(b) = 0$, pois $b \in ker(f^n)$. Logo, $ker(f^n) \cap im(f^n) = \{0\}$.

Provaremos agora que $ker(f^n) + im(f^n) = M$. Seja $c \in M$. Então $f^n(c) \in im(f^n) = im(f^{2n})$. Tome $d \in M$ tal que $f^{2n}(d) = f^n(c)$. Note que

$$f^n(c - f^n(d)) = f^n(c) - f^n(f^n(d)) = f^n(c) - f^{2n}(d) = f^n(c) - f^n(c) = 0,$$

isto é, $c - f^n(d) \in ker(f^n)$.

Portanto, temos $c = (c - f^n(d)) + f^n(d) \in ker(f^n) + im(f^n)$. □

Definição A.1.36. *Um A-módulo M é dito* indecomponível *se $M \neq \{0\}$ e não existirem submódulos não triviais N_1, N_2 tais que $M = N_1 \oplus N_2$. Isto é, M é indecomponível se $M \neq \{0\}$ e $M = N_1 \oplus N_2$, então $N_1 = \{0\}$ ou $N_2 = \{0\}$.*

Definição A.1.37. *Dizemos que um A-módulo $M \neq \{0\}$ é* decomponível *se não for indecomponível. Equivalentemente, significa dizer que existem submódulos $N_1, N_2 \subseteq M, N_1 \neq \{0\}, N_2 \neq \{0\}$ tais que $M = N_1 \oplus N_2$.*

Notemos que as definições de módulo simples e módulo indecomponível são muito próximas, porém vemos através da observação a seguir que a propriedade de ser simples é mais forte que ser indecomponível, visto que todo módulo não-nulo simples é também um módulo indecomponível. Precisamente, temos:

Observação A.1.38. *Se $M \neq \{0\}$ é um A-módulo simples, então M é um A-módulo indecomponível. De fato, suponhamos que $M \neq \{0\}$ e $M = N_1 \oplus N_2$, onde $N_1, N_2 \subseteq M$ são submódulos de M. Como M é simples, temos $N_1 = \{0\}$ ou $N_1 = M$. Se $N_1 = \{0\}$, então M é indecomponível, e se $N_1 = M$, então temos $M = N_1 \oplus N_2 = M \oplus N_2$, e portanto temos $N_2 = \{0\}$, ou seja, M é indecomponível também neste caso.*

O exemplo a seguir ilustra que a recíproca da observação acima não é verdadeira. Isto é, nem todo módulo indecomponível é simples.

Exemplo A.1.39. *Considere $\mathbb{Z}$ como $\mathbb{Z}$-módulo. Sabemos que $\mathbb{Z}$ não é simples como $\mathbb{Z}$-módulo, pois existem submódulos não triviais. De fato, sabemos que todo $\mathbb{Z}$-submódulo de $\mathbb{Z}$ é da forma $n \cdot \mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$, onde $n \in \{0, 1, 2, ...\}$. Contudo, $\mathbb{Z}$ é indecomponível como $\mathbb{Z}$-módulo. De fato, suponha que existem submódulos $N_1, N_2 \subseteq \mathbb{Z}$ tais que $\mathbb{Z} = N_1 \oplus N_2$. Então, existem n_1,n_2 inteiros tais que $N_1 = n_1 \cdot \mathbb{Z}$ e $N_2 = n_2 \cdot \mathbb{Z}$. Seja $m = n_1 n_2 = n_2 n_1$. Então, obviamente temos que $m \in N_1$ e*

$m \in N_2$, *portanto* $m = 0$. *Assim,* $n_1 n_2 = 0$, *e isto significa que* $n_1 = 0$ *ou* $n_2 = 0$, *e portanto* $N_1 = \{0\}$ *ou* $N_2 = \{0\}$.

Ou seja, $\mathbb{Z}$ *como* $\mathbb{Z}$*-módulo é indecomponível, mas não é simples.*

Quando um A-módulo M, $M \neq \{0\}$, pode ser escrito como uma soma direta da forma $M = M_1 \oplus M_2 \oplus \cdots \oplus M_r$, onde os M_i's são submódulos não-nulos de M, para $i = 1, 2, ..., r$, definimos então, para cada i, o homomorfismo $\pi_i : M \longrightarrow M_i$ dado por $\pi_i(x) = x_i$, onde $x = x_1 + x_2 + \cdots + x_r$, com $x_i \in M_i$. Neste caso, para cada i, chamamos π_i de *homomorfismo sobrejetor canônico* associado a decomposição de M. Desde que M é soma direta dos M_i's, temos que a escrita de $x \in M$ na forma $x = x_1 + x_2 + \cdots + x_r$, com $x_i \in M_i$, é única, donde temos então que estes homomorfismos estão bem definidos.

Verifiquemos que estas aplicações são de fato homomorfismos sobrejetores de A-módulos.

Sejam $x, y \in M$ e $a \in A$. Temos:

- $\pi_i(x + y) = \pi_i(x) + \pi_i(y)$:

  Desde que $x = x_1 + \cdots + x_r$ e $y = y_1 + y_2 + \cdots + y_r$, temos que $x + y = (x_1 + y_1) + \cdots + (x_r + y_r)$. Assim, $\pi_i(x + y) = x_i + y_i = \pi_i(x) + \pi_i(y)$.

- $\pi_i(a \cdot x) = a \cdot \pi_i(x)$:

  Desde que $x = x_1 + \cdots + x_r$, temos que $a \cdot x = (a \cdot x_1) + \cdots + (a \cdot x_r)$. Assim, $\pi_i(a \cdot x) = a \cdot x_i = a \cdot \pi_i(x)$.

- π_i é sobrejetora:

  Seja $z \in M_i$. Como $M_i \subseteq M$, temos que $z \in M$, e $z = x_1 + \cdots + x_r$, com $x_j = 0$ para $j = 1, ..., i-1, i+1, ..., r$ e $x_i = z$. Segue que $\pi_i(z) = \pi_i(x_1 + \cdots + x_r) = x_i = z$. Logo, π_i é sobrejetora.

Estes homomorfismos sobrejetores canônicos dão origem aos seguintes endomorfismos, que chamamos de *projeções*: Para cada $i = 1, ..., r$, definimos $\alpha_i : M \longrightarrow M$ por $\alpha_i(x) = \pi_i(x)$. Notemos que $\alpha_i \in End_A(M)$. Além disso, estas projeções satisfazem:

Proposição A.1.40. *Sejam* α_i, $i = 1, 2, ..., r$, *como construídas acima. Valem as seguintes igualdades:*

(i) $\alpha_i^2 = \alpha_i$;

(ii) $\alpha_i \circ \alpha_j = 0$, *se* $i \neq j$;

(iii) $Id_M = \sum_{i=1}^{r} \alpha_i = \alpha_1 + \alpha_2 + \cdots + \alpha_r$.

Demonstração. (i) $\alpha_i^2 = \alpha_i$:

De fato, seja $x \in M$. Então $x = x_1 + \cdots + x_r$. Assim,

$$\alpha_i^2(x) = \alpha_i(\alpha_i(x)) = \alpha_i(\pi_i(x)) = \alpha_i(x_i) = \pi_i(x_i) = x_i$$

Por outro lado,

$$\alpha_i(x) = \pi_i(x) = x_i$$

Logo, $\alpha_i^2 = \alpha_i$.

(*ii*) $\alpha_i \circ \alpha_j = 0$, se $i \neq j$:

De fato, seja $x \in M$. Então $x = x_1 + \cdots + x_r$. Assim, se $i \neq j$, temos

$$\alpha_i \circ \alpha_j(x) = \alpha_i(\alpha_j(x)) = \pi_i(\pi_j(x_1 + \cdots + x_r)) = \pi_i(x_j) = 0$$

Como $x \in M$ foi qualquer, temos que $\alpha_i \circ \alpha_j = 0$, quando $i \neq j$.

(*iii*) $Id_M = \sum_{i=1}^r \alpha_i = \alpha_1 + \alpha_2 + \cdots + \alpha_r$:

De fato, seja $x \in M$. Então $x = x_1 + \cdots + x_r$. Como para cada $i = 1, 2, ..., r$, α_i é homomorfismo, e $\alpha_i(x) = x_i$, temos que

$$\left(\sum_{i=1}^r \alpha_i\right)(x) = \sum_{i=1}^r \alpha_i(x) = \sum_{i=1}^r x_i = x = Id_M(x)$$

Como $x \in M$ foi qualquer, temos que $\sum_{i=1}^r \alpha_i = Id_M$.

□

Definição A.1.41. *Um A-módulo à esquerda M é dito ser* fortemente indecomponível *se $End_A(M)$ é um anel local.*

Definição A.1.42. *Seja A um anel. Um elemento $a \in A$ é dito* idempotente *se $a^2 = a$.*

Observação A.1.43. *Temos que todo anel A possui ao menos dois idempotentes, a saber 0_A e 1_A. Por essa razão, estes idempotentes são chamados de triviais.*

Proposição A.1.44. *Seja A um anel local. Então A tem apenas idempotentes triviais, isto é, se $a \in A$ é tal que $a^2 = a$, então $a = 0$ ou $a = 1$.*

Demonstração. Seja $a \in A$ tal que $a^2 = a$. Então temos $a - a^2 = 0$, ou seja, $(1 - a)a = 0$.

Suponhamos agora que $a \neq 0$. Devemos mostrar então que $a = 1$.

Sendo $a \neq 0$, obtemos então que $1 - a$ não é inversível à esquerda, pois se fosse existiria $b \in A$ tal que $1 = b(1 - a)$, e disto seguiria que $a = 1a = [b(1 - a)]a = b[(1 - a)a] = b0 = 0$, o que seria uma contradição.

Logo, $1-a$ não é inversível à esquerda, e portanto não é inversível. Assim, temos que $(1-a) \notin U(A)$, ou seja, $(1-a) \in (A \setminus U(A))$.

Afirmamos então que a é inversível. De fato, se a não for inversível, então $a \in (A \setminus U(A))$. Como, por hipótese, A é um anel local, temos que $A \setminus U(A)$ é um ideal de A. Assim, $1 = (1-a)+a \in (A \setminus U(A))$, e portanto $A = (A \setminus U(A))$, o que é um absurdo, já que $1 \in U(A)$, e portanto $1 \notin (A \setminus U(A))$, e obviamente $1 \in A$.

Portanto, a é inversível. Assim, existe $b \in A$ tal que $ab = 1$. Então,

$$1 - a = (1-a)1 = (1-a)(ab) = [(1-a)a]b = 0b = 0,$$

ou seja, $1 - a = 0$, donde segue que $a = 1$, como queríamos. □

Proposição A.1.45. *Um A-módulo M, $M \neq \{0\}$, é indecomponível se, e somente se, $End_A(M)$ contém apenas idempotentes triviais.*

Vamos na verdade provar a contrapositiva desta afirmação, ou seja, provaremos a afirmação equivalente:

Proposição A.1.46. *Um A-módulo M, $M \neq \{0\}$, é decomponível se, e somente se, $End_A(M)$ contém algum idempotente não-trivial, isto é, existe $f \in End_A(M)$ tal que $f^2 = f$ e $f \neq 1, f \neq 0$.*

Aqui, estamos denotando por 1 a aplicação Id_M, que é a unidade em $End_A(M)$.

Demonstração. [$\Longrightarrow$] Seja $M \neq \{0\}$ um A-módulo decomponível. Então existem submódulos $M_1 \neq \{0\}$ e $M_2 \neq \{0\}$ tais que $M = M_1 \oplus M_2$. Tomemos então as projeções α_1 e α_2. Isto é, para $i \in \{1, 2\}$, temos $\alpha_i : M \longrightarrow M$ dada por $\alpha_i(x) = x_i$, onde $x = x_1 + x_2$ com $x_i \in M_i$.

Vamos provar que α_1 é um idempotente não-trivial. Da mesma forma, prova-se também que α_2 é um idempotente não-trivial.

Temos que $\alpha_1 \in End_A(M)$, e do item (i) da Proposição A.1.40, temos que $\alpha_1^2 = \alpha_1$. Resta verificar apenas que $\alpha_1 \neq 0$ e $\alpha_1 \neq 1$:

- $\underline{\alpha_1 \neq 0}$:

  Como $M_1 \neq \{0\}$, tomemos $x \in M_1$, $x \neq 0$. Assim, $\alpha_1(x) = x \neq 0$, donde segue que $\alpha_1 \neq 0$.

- $\underline{\alpha_1 \neq 1}$:

  Como $M_2 \neq \{0\}$, tomemos $y \in M_2$, $y \neq 0$. Assim, $\alpha_1(y) = 0 \neq y = Id_M(y)$, donde segue que $\alpha_1 \neq 1$.

Logo, α_1 é um idempotente não-trivial.

[$\Longleftarrow$] Suponhamos agora que $M \neq \{0\}$ é um A-módulo e que $End_A(M)$ contém algum idempotente nao-trivial. Seja $f \in End_A(M)$ este idempotente. Temos então que $f : M \longrightarrow M$, $f^2 = f$, $f \neq 0$ e $f \neq 1$.

Vamos provar que $M = im(f) \oplus ker(f)$, onde $im(f) \neq \{0\}$ e também $ker(f) \neq \{0\}$, e com isso concluímos então que M é decomponível.

Primeiro, vejamos que $M = im(f) + ker(f)$.

Seja $x \in M$. Note que $x = f(x) + (x - f(x))$, onde temos que $f(x) \in im(f)$ e $(x - f(x)) \in ker(f)$. De fato, obviamente temos que $f(x) \in im(f)$, e do fato que f é um homomorfismo tal que $f^2 = f$, temos que

$$f(x - f(x)) = f(x) - f(f(x)) = f(x) - f^2(x) = f(x) - f(x) = 0,$$

ou seja, $(x - f(x)) \in ker(f)$.

Agora, vejamos que $im(f) \cap ker(f) = \{0\}$.

Seja $y \in im(f) \cap ker(f)$. Do fato que $y \in ker(f)$, temos que $f(y) = 0$, e do fato que $y \in im(f)$, temos que existe $x \in M$ tal que $f(x) = y$. Assim, $f(f(x)) = f(y)$, ou seja, $f^2(x) = f(y)$. Como $f^2 = f$ e $f(y) = 0$, temos que $y = f(x) = f^2(x) = f(y) = 0$, ou seja, $y = 0$ e segue que $im(f) \cap ker(f) = \{0\}$.

Com isso, concluímos que $M = im(f) \oplus ker(f)$.

Por último, verifiquemos que $im(f) \neq \{0\}$ e também $ker(f) \neq \{0\}$.

Se $im(f) = \{0\}$, temos que $M = im(f) \oplus ker(f) = \{0\} \oplus ker(f) = ker(f)$, donde segue que $f = 0$, uma contradição, já que $f \neq 0$. Logo, $im(f) \neq \{0\}$.

Se $ker(f) = \{0\}$, temos que $M = im(f)$. Então, para $y \in M$, temos que existe $x \in M$ tal que $y = f(x)$. Assim, $f(y) = f(f(x)) = f^2(x) = f(x)$, e portanto $f(y) - f(x) = 0$, ou seja, $f(y - x) = 0$. Logo, $y - x \in ker(f) = \{0\}$, e portanto $x = y$. Com isso, temos que $y = f(x) = f(y)$ e segue que $f = 1$, uma contradição, já que $f \neq 1$. Logo, $ker(f) \neq \{0\}$. □

Corolário A.1.47. *Se $M \neq \{0\}$ é um A-módulo fortemente indecomponível, então M é indecomponível.*

Demonstração. Este resultado segue diretamente da Proposição A.1.44 e da Proposição A.1.45.

De fato, se $M \neq \{0\}$ é um A-módulo fortemente indecomponível, então, por definição, $End_A(M)$ é um anel local. Então, pela Proposição A.1.44, $End_A(M)$ só tem os idempotentes triviais. Segue portanto da Proposição A.1.45 que M é indecomponível. □

O exemplo a seguir mostra que a recíproca do corolário acima não é verdadeira. Isto é, nem todo módulo indecomponível é fortemente indecomponível.

Exemplo A.1.48. *Considere $\mathbb{Z}$ como um $\mathbb{Z}$-módulo. Sabemos do* Exemplo A.1.39 *que $\mathbb{Z}$ é indecomponível.*

Vejamos agora que $End_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ como $\mathbb{Z}$-módulos, donde segue que $\mathbb{Z}$ não é fortemente indecomponível como $\mathbb{Z}$-módulo, já que $\mathbb{Z}$ não é anel local, visto que todo ideal da forma $p\mathbb{Z}$, onde p é um número primo, é um ideal maximal de $\mathbb{Z}$. Portanto, $End_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ também não é local.

Note que, para $f \in End_{\mathbb{Z}}(\mathbb{Z})$, temos que f está unicamente determinado pelo valor que assume em 1, já que para qualquer inteiro n, $f(n) = f(n \cdot 1) = n \cdot f(1)$.

Assim, $\varphi : End_{\mathbb{Z}}(\mathbb{Z}) \longrightarrow \mathbb{Z}$ dado por $\varphi(f) = f(1)$ está bem definido. Além disso, para cada número inteiro k, a aplicação $f_k : \mathbb{Z} \longrightarrow \mathbb{Z}$ tal que $f_k(1) = k$, é um homomorfismo de $\mathbb{Z}$-módulos.

Com isso, garantimos que φ é um isomorfismo de $\mathbb{Z}$-módulos. De fato, para toda $f, g \in End_{\mathbb{Z}}(\mathbb{Z})$ e $n \in \mathbb{Z}$, temos:

- *$\underline{\varphi(f+g) = \varphi(f) + \varphi(g)}$:*

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

- *$\underline{\varphi(n \cdot f) = n \cdot \varphi(f)}$:*

$$\varphi(n \cdot f) = (n \cdot f)(1) = n \cdot f(1) = n \cdot \varphi(f)$$

- *$\underline{\varphi \text{ é injetora:}}$ Sejam $f, g \in End_{\mathbb{Z}}(\mathbb{Z})$ tais que $\varphi(f) = \varphi(g)$. Então $f(1) = g(1)$. Donde segue que para todo $n \in \mathbb{Z}$ temos*

$$f(n) = f(n \cdot 1) = n \cdot f(1) = n \cdot g(1) = g(n \cdot 1) = g(n)$$

  Portanto $f = g$.

- *$\underline{\varphi \text{ é sobretora:}}$ Seja $k \in \mathbb{Z}$. Tome $f_k \in End_{\mathbb{Z}}(\mathbb{Z})$. Então, $\varphi(f_k) = f_k(1) = k$.*

A.2 O Teorema de Krull-Schmidt

Nesta seção provaremos o clássico Teorema de Krull-Schmidt, que garante que todo A-módulo M de comprimento finito tem uma decomposição em soma direta de submódulos indecomponíveis. E mais, esta decomposição é única a menos de isomorfismo. Desta forma, este é um teorema de existência e unicidade. Veremos que a prova da existência é um tanto quanto simples, enquanto que a prova da unicidade é um pouco mais elaborada.

A existência de uma tal decomposição é dada pela proposição a seguir. Ressaltamos que não é necessário exigir que o módulo M tenha comprimento finito, que como vimos na Proposição A.1.34 é equivalente a exigir que M seja artiniano e noetheriano, isto é, que satisfaça ACC e DCC. De fato, é suficiente exigirmos que M satisfaça apenas uma dessas duas condições. Vejamos:

Proposição A.2.1. *Sejam A um anel e $M \neq \{0\}$ um A-módulo à esquerda cujos submódulos satisfazem ou ACC ou DCC. Então M pode ser decomposto em uma soma direta finita de módulos indecomponíveis. Dizemos, neste caso, que M tem uma* decomposição de Krull-Schmidt.

Demonstração. Seja $M \neq \{0\}$ um A-módulo cujos submódulos satisfazem ACC ou DCC.

Afirmação 1: Qualquer submódulo indecomponível $N \subseteq M$ tem uma decomposição de Krull-Schmidt. De fato, $N = \oplus_{i=1}^{1} N_i$, com $N_1 = N$, e temos N indecomponível.

Afirmação 2: Se $N_1, N_2 \subseteq M$ são dois submódulos de M tais que ambos tem uma decomposição de Krull-Schmidt e, além disso, temos também que vale $N_1 \cap N_2 = \{0\}$, então $N_1 + N_2 = N_1 \oplus N_2$ também tem uma decomposição de Krull-Schmidt. De fato, sejam $N_1 = \bigoplus_{i=1}^{s} P_i$ e $N_2 = \bigoplus_{j=1}^{t} T_j$, onde P_i e T_j são indecomponíveis para cada $i = 1, ..., s$ e $j = 1, ..., t$. Então, temos

$$N_1 + N_2 = N_1 \oplus N_2 = \left(\bigoplus_{i=1}^{s} P_i \right) \oplus \left(\bigoplus_{j=1}^{t} T_j \right) = \bigoplus_{k=1}^{t+s} R_k$$

onde $R_k = P_k$, para $k \in \{1, ..., s\}$ e $R_k = T_{k-s}$ para $k \in \{s+1, ..., s+t\}$. Note que R_k é indecomponível para cada $k = 1, .., t + s$, ou seja, $N_1 + N_2$ tem uma decomposição de Krull-Schmidt.

Vamos provar agora que $M \neq \{0\}$ tem um decomposição de Krull-Schmidt. Suponhamos por absurdo que $M \neq \{0\}$ não possua uma decomposição de Krull-Schmidt. Então, pela Afirmação 1, temos que $M \neq \{0\}$ não pode ser indecomponível, pois se ele fosse então ele teria uma decomposição de Krull-Schmidt, ou seja, $M \neq \{0\}$ é decomponível. Seja então $M_1, M_1' \subseteq M$ submódulos de M tais que $M = M_1 \oplus M_1'$, com $M_1 \neq \{0\}$ e também $M_1' \neq \{0\}$. Pela **Afirmação 2**, M_1 ou M_1' não pode ter uma decomposição de Krull-Schmidt, pois se os dois tivessem, então M também teria. Podemos supor sem perda de generalidade que M_1 não tem uma decomposição de Krull-Schmidt. Note que temos $M_1 \subsetneq M$ submódulo de M. Repetindo o argumento que usamos para M, mas agora para M_1, concluímos que $M_1 = M_2 \oplus M_2'$, onde $M_2 \neq \{0\}, M_2' \neq \{0\}$, e sem perda de generalidade, temos também que M_2 não possui uma decomposição de Krull-Schmidt. Note que temos $M_2 \subsetneq M_1$ submódulo de M_1 e também que $M = M_1 \oplus M_1' = (M_2 \oplus M_2') \oplus M_1'$, e portanto $M_1' \oplus M_2' \subsetneq M$ submódulo de M.

Repetindo indutivamente este processo, obtemos as seguintes duas cadeias infinitas

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$$

e

$$\{0\} \subsetneq M_1' \subsetneq (M_1' \oplus M_2') \subsetneq (M_1' \oplus M_2' \oplus M_3') \subsetneq \cdots$$

e portanto M não satisfaz nem ACC e nem DCC nos submódulos, um absurdo. Logo, M tem uma decomposição de Krull-Schmidt, isto é,

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

onde $M_i \subseteq M$ é um submódulo indecomponível, para cada $i = 1, 2, ..., n$. □

Vamos agora caminhar em direção a demonstração da unicidade da decomposição de Krull-Schmidt. Começamos vendo alguns resultados que nos serão úteis para tal objetivo.

Proposição A.2.2. *Seja $M \neq \{0\}$ um A-módulo à esquerda indecomponível de comprimento finito r. Então $E := End_A(M)$ é um anel local. Em outras palavras, M é um A-módulo fortemente indecomponível.*

Demonstração. Notemos que pela Proposição A.1.15, é suficiente mostrarmos que qualquer endomorfismo $f \in (E \setminus U(E))$ é nilpotente, pois isto implicará que E é um anel local. Seja $f \in (E \setminus U(E))$. Para mostrar que f é nilpotente, fixe um inteiro $m > 0$ tal que $M = ker(f^m) \oplus im(f^m)$, que sabemos existir pelo Teorema de Decomposição Fitting A.1.35. Como M é indecomponível e temos $M = ker(f^m) \oplus im(f^m)$, temos então que $ker(f^m) = \{0\}$ ou $im(f^m) = \{0\}$. Suponhamos, por absurdo, que $ker(f^m) = \{0\}$, então $im(f^m) = M$. Assim, por $ker(f^m) = \{0\}$ temos f^m injetiva e por $im(f^m) = M$ temos f^m sobrejetiva, logo f^m é um isomorfismo e portanto $f^m \in U(E)$. Seja $g \in E$ tal que $f^m \circ g = g \circ f^m = Id_M$. Assim, $f \circ (f^{m-1} \circ g) = (g \circ f^{m-1}) \circ f = Id_M$, e portanto $f \in U(E)$, o que é um absurdo. Com isso, concluímos que $im(f^m) = \{0\}$, e portanto $f^m \equiv 0$, ou seja, f é nilpotente.

Assim, para qualquer endomorfismo $f \in (E \setminus U(E))$, concluímos que f é nilpotente, como queríamos. □

O teorema a seguir é conhecido como Teorema de Krull-Schmidt-Azumaya, e é uma reformulação mais atual do Teorema de Krull-Schmidt dada por Azumaya em 1950. Apresentamos a prova deste teorema com detalhes, rigor e formalismo, e com isso ela se torna a prova mais trabalhosa e cansativa deste capítulo. Contudo, este trabalho é recompensado logo a seguir, no momento em que provamos o Teorema de Krull-Schmidt, principal resultado deste capítulo e que seguirá facilmente como consequência imediata dos resultados provados anteriormente, sobretudo deste teorema.

Teorema A.2.3. ***(Krull-Schmidt-Azumaya)*** *Seja A um anel e suponha que um A-módulo à esquerda $M \neq \{0\}$ tem as seguintes duas decomposições em submódulos:*

$$M = M_1 \oplus \cdots \oplus M_r = N_1 \oplus \cdots \oplus N_s$$

onde os $N_i's$ são indecomponíveis e os $M_i's$ são fortemente indecomponíveis. Então $r = s$, e reindexando os índices se necessário, temos $M_i \cong N_i$, para cada $i = 1, 2, ...r$.

Demonstração. Sejam $\pi_i : M \longrightarrow M_i \subseteq M$ e $p_j : M \longrightarrow N_j \subseteq M$ os homomorfismos sobrejetores canônicos sobre os M_i's e os N_j's associados com as duas decomposições de Krull-Schmidt dadas. Definimos então as projeções $\alpha_i, \beta_j \in E := End_A(M)$, dadas por $\alpha_i(x) = \pi_i(x)$ e $\beta_j(x) = p_j(x)$, para

$x \in M$. Assim, nós temos

$$\alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s = Id_M := 1_M,$$

isto é, $1_M = \beta_1 + \cdots + \beta_s$, e então multiplicando essa igualdade por α_1 em ambos os lados à esquerda, temos

$$\alpha_1 = \alpha_1 1_M = \alpha_1(\beta_1 + \cdots + \beta_s) = \alpha_1\beta_1 + \cdots + \alpha_1\beta_s \in E$$

Notemos que para $x \in M$, $\alpha_1\beta_j(x) = \alpha_1(\beta_j(x)) = \pi_1(\beta_j(x)) \in M_1$, ou seja, $\alpha_1\beta_j$ manda M em M_1. Definimos então o homomorfismo $\alpha_{1j} : M \longrightarrow M_1$ por $\alpha_{1j}(x) = \alpha_1\beta_j(x)$. Temos então que $\alpha_{1j}|_{M_1} : M_1 \longrightarrow M_1 \in End(M_1)$.

Assim, para $y \in M_1$ temos

$$y = 1_{M_1}(y) = Id_{M_1}(y) = \pi_1|_{M_1}(y) = \alpha_1|_{M_1}(y) = \left(\sum_{j=1}^{s} \alpha_1\beta_j\right)\Bigg|_{M_1}(y) =$$

$$= \left(\sum_{j=1}^{s} \alpha_{1j}\right)\Bigg|_{M_1}(y) = \left(\sum_{j=1}^{s} \alpha_{1j}|_{M_1}\right)(y) = \sum_{j=1}^{s} \alpha_{1j}|_{M_1}(y)$$

Portanto, $\sum_{j=1}^{s} \alpha_{1j}|_{M_1} = Id_{M_1} := 1_{M_1} \in End(M_1)$.

Como, por hipótese, M_1 é fortemente indecomponível, isto é, $End_A(M_1)$ é um anel local, então pelo menos um dos somandos acima é necessariamente um automorfismo de M_1. De fato, 1_{M_1} é inversível, então pelo item (v) da Proposição A.1.10, para algum $j, \alpha_{1j}|_{M_1}$ é inversível, isto é, $\alpha_{1j}|_{M_1}$ é um automorfismo. Podemos dizer sem perda de generalidade que $\alpha_{11}|_{M_1}$ é este automorfismo.

Provemos agora então que $M_1 \cong N_1$, via $p_1|_{M_1} : M_1 \longrightarrow N_1$.

Já temos que $p_1|_{M_1}$ é um homomorfismo, vamos verificar que é de fato um isomorfismo.

Notemos que $p_1|_{M_1}(x) = \beta_1|_{M_1}(x)$, para $x \in M_1$.

Vamos provar primeiro que $p_1|_{M_1}$ é injetora. Sejam $x, y \in M_1$ tais que $p_1|_{M_1}(x) = p_1|_{M_1}(y)$. Então $p_1(x) = p_1(y)$, ou seja, $\beta_1(x) = \beta_1(y)$. Assim, $\alpha_1\beta_1(x) = \alpha_1\beta_1(y)$, e portanto $\alpha_{11}(x) = \alpha_{11}(y)$. Disto e do fato que $x, y \in M_1$, temos $\alpha_{11}|_{M_1}(x) = \alpha_{11}|_{M_1}(y)$. Agora, como $\alpha_{11}|_{M_1}$ é automorfismo, temos que $x = y$. Logo, $p_1|_{M_1}$ é injetora.

Vamos provar agora que $p_1|_{M_1}$ é sobrejetora.

Afirmamos que $N_1 = im(p_1|_{M_1}) \oplus ker(\pi_1|_{N_1})$.

De fato, como $p_1|_{M_1} : M_1 \longrightarrow N_1$, temos que $im(p_1|_{M_1}) \subseteq N_1$, e também temos $\pi_1|_{N_1} : N_1 \longrightarrow M_1$, logo $ker(\pi_1|_{N_1}) \subseteq N_1$, e portanto temos que $im(p_1|_{M_1}) + ker(\pi_1|_{N_1}) \subseteq N_1$.

Verifiquemos primeiro que de fato temos $N_1 = im(p_1|_{M_1}) + ker(\pi_1|_{N_1})$.

Seja $n \in N_1$. Como $N_1 \subseteq M$, temos $n \in M$, e assim, aplicando α_1, temos que $\alpha_1(n) = \pi_1(n) \in M_1$.

Como $\alpha_{11}|_{M_1} : M_1 \longrightarrow M_1$ é automorfismo, existe $m \in M_1$ tal que $\alpha_{11}|_{M_1}(m) = \pi_1(n)$, ou seja, $\alpha_{11}(m) = \pi_1(n)$.

Por fim, note que $n = p_1|_{M_1}(m) + (n - p_1|_{M_1}(m))$, onde temos que $p_1|_{M_1}(m) \in im(p_1|_{M_1})$ e $n - p_1|_{M_1}(m) \in ker(\pi_1|_{N_1})$, pois temos $n \in N_1$ e $p_1|_{M_1} : M_1 \longrightarrow N_1$, logo $n - p_1|_{M_1}(m) \in N_1$ e vale

$$\pi_1|_{N_1}(n - p_1|_{M_1}(m)) = \pi_1(n - p_1(m)) = \pi_1(n) - \pi_1(p_1(m)) =$$
$$= \pi_1(n) - \alpha_1(\beta_1(m)) = \pi_1(n) - \alpha_{11}(m) = \pi_1(n) - \pi_1(n) = 0$$

Logo, temos que $N_1 \subseteq im(p_1|_{M_1}) + ker(\pi_1|_{N_1})$, e vale a igualdade $N_1 = im(p_1|_{M_1}) + ker(\pi_1|_{N_1})$.

Verifiquemos agora que a interseção é nula.

Seja $y \in im(p_1|_{M_1}) \cap ker(\pi_1|_{N_1})$. Em particular, $y \in N_1$. Do fato de $y \in im(p_1|_{M_1})$, temos que existe $x \in M_1$ tal que $p_1|_{M_1}(x) = p_1(x) = y$, ou seja $\beta_1(x) = y$, e do fato que $y \in ker(\pi_1|_{N_1})$, temos que $\pi_1|_{N_1}(y) = \pi_1(y) = 0$, ou seja $\alpha_1(y) = 0$.

Assim, $0 = \alpha_1(y) = \alpha_1(\beta_1(x)) = \alpha_{11}(x)$. Como $x \in M_1$, temos $\alpha_{11}|_{M_1}(x) = \alpha_{11}(x) = 0$, e do fato que $\alpha_{11}|_{M_1}$ é automorfismo, temos que $x = 0$, e portanto $y = p_1(x) = p_1(0) = 0$. Logo, $im(p_1|_{M_1}) \cap ker(\pi_1|_{N_1}) = \{0\}$.

Com isso, concluímos que $N_1 = im(p_1|_{M_1}) \oplus ker(\pi_1|_{N_1})$.

Agora, do fato de N_1 ser indecomponível, temos $im(p_1|_{M_1}) = \{0\}$ ou $ker(\pi_1|_{N_1}) = \{0\}$. Como $M_1 \neq \{0\}$ e $p_1|_{M_1}$ é injetora, temos $p_1|_{M_1}(M_1) = im(p_1|_{M_1}) \neq \{0\}$, e portanto $ker(\pi_1|_{N_1}) = \{0\}$, ou seja, $im(p_1|_{M_1}) = N_1$, donde concluímos que $p_1|_{M_1} : M_1 \longrightarrow N_1$ é sobrejetora.

Segue então que $p_1|_{M_1} : M_1 \longrightarrow N_1$ é um isomorfismo, donde temos $M_1 \cong N_1$.

Agora, afirmamos que

$$M = M_1 \oplus N_2 \oplus \cdots \oplus N_s$$

Vamos provar primeiro que $M_1 \cap (N_2 \oplus \cdots \oplus N_s) = \{0\}$. Seja $x \in M$, tal que $x \in M_1 \cap (N_2 \oplus \cdots \oplus N_s)$. Como $M = M_1 \oplus \cdots \oplus M_r = N_1 \oplus \cdots \oplus N_s$, temos que existem únicos $x_i^M \in M_i, 1 \leq i \leq r$, e $x_j^N \in N_j, 1 \leq j \leq s$, tais que $x = x_1^M + \cdots + x_r^M = x_1^N + \cdots + x_s^N$. Como $x \in M_1$, então $x_i^M = 0$ para $i \geq 2$. Isto é, $x = x_1^M$. E como $x \in N_2 \oplus \cdots \oplus N_s$, temos $x_1^N = 0$. Vimos que $p_1|_{M_1} : M_1 \longrightarrow N_1$ é um isomorfismo, e como

$$p_1|_{M_1}(x_1^M) = p_1|_{M_1}(x) = p_1(x) = p_1(x_1^N + x_2^N + \cdots + x_s^N) = x_1^N = 0$$

temos então que $x_1^M = 0$, ou seja $x = 0$.

Provemos agora que $M = M_1 + N_2 + \cdots + N_s$.

Obviamente, temos $M_1 + N_2 + \cdots + N_s \subseteq M$, resta apenas verificar que $M \subseteq M_1 + N_2 + \cdots + N_s$.

Observe que se provarmos que $N_1 \subseteq M_1 + N_2 + \cdots + N_s$, então

$$M = N_1 + N_2 + \cdots + N_s \subseteq (M_1 + N_2 + \cdots + N_s) + N_2 + \cdots + N_s = M_1 + N_2 + \cdots + N_s,$$

donde concluiremos o desejado.

Seja então $a \in N_1$. Como $p_1|_{M_1} : M_1 \longrightarrow N_1$ é isomorfismo, seja $b \in M_1$ tal que $p_1|_{M_1}(b) = a$. Temos $p_1(a-b) = p_1(a) - p_1(b) = p_1(a) - p_1|_{M_1}(b) = a - a = 0$. Então $a - b \in ker(p_1) = N_2 \oplus \cdots \oplus N_s$. Agora, adicionando b ao termo $a - b$ obtemos o resultado, isto é, $a = b + (a - b) \in M_1 + N_2 + \cdots + N_s$.

Com isto, concluímos que $N_1 \subseteq M_1 + N_2 + \cdots + N_s$ e portanto $M = M_1 \oplus N_2 \oplus \cdots \oplus N_s$.

Agora, por final, notemos que

$$M_2 \oplus \cdots \oplus M_r \cong \frac{M_1 \oplus M_2 \oplus \cdots \oplus M_r}{M_1} = \frac{M}{M_1} =$$
$$= \frac{M_1 \oplus N_2 \oplus \cdots \oplus N_s}{M_1} \cong N_2 \oplus \cdots \oplus N_s$$

Assim,

$$M_2 \oplus \cdots \oplus M_r \cong N_2 \oplus \cdots \oplus N_s$$

Em resumo, obtemos que $M_1 \cong N_1$ e $M_2 \oplus \cdots \oplus M_r \cong N_2 \oplus \cdots \oplus N_s$.

Seja $\varphi : N_2 \oplus \cdots \oplus N_s \longrightarrow M_2 \oplus \cdots \oplus M_r$ a aplicação que realiza este isomorfismo. Note que $\varphi(N_2 \oplus \cdots \oplus N_s) = M_2 \oplus \cdots \oplus M_r$, e portanto $\varphi(N_2) \oplus \cdots \oplus \varphi(N_s) = M_2 \oplus \cdots \oplus M_r$. Denotando por $\bar{N}_i = \varphi(N_i), i = 2, ..., s$ e $\bar{M} = M_2 \oplus \cdots \oplus M_r = \bar{N}_2 \oplus \cdots \oplus \bar{N}_s$, podemos aplicar o mesmo raciocínio, desde o início da demonstração, obtendo então que

$$M_2 \cong \bar{N}_2 = \varphi(N_2) \cong N_2 \quad \text{e} \quad M_3 \oplus \cdots \oplus M_r \cong \bar{N}_3 \oplus \cdots \oplus \bar{N}_s \cong N_3 \oplus \cdots \oplus N_s.$$

Assim, no caso em que $s \geq r$, repetimos o argumento até obtermos $M_{r-1} \cong N_{r-1}$ e também que $M_r \cong N_r \oplus N_{r+1} \oplus \cdots \oplus N_s$, e então finalmente obtemos $M_r \cong N_r$ e $\{0\} \cong N_{r+1} \oplus \cdots \oplus N_s$, concluindo por fim que $r = s$, visto que os módulos N_i's são não-nulos.

No caso em que $r \geq s$, repetimos o argumento até obtermos $M_{s-1} \cong N_{s-1}$ e também que $M_s \oplus M_{s+1} \oplus \cdots \oplus M_r \cong N_s$, e então finalmente obtemos $M_s \cong N_s$ e $M_{s+1} \oplus \cdots \oplus M_r \cong \{0\}$, concluindo por fim que $r = s$, visto que os módulos M_i's são não-nulos. □

Teorema A.2.4. ***(Krull-Schmidt)*** *Todo módulo $M \neq \{0\}$ de comprimento finito tem uma decomposição em soma direta de submódulos*

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_r \qquad (D)$$

onde cada M_i é um submódulo indecomponível de M, para $i = 1, 2, ..., r$. Além disso, essa decomposição é única a menos de isomorfismo, isto é, se tivermos também

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_s \qquad (D')$$

onde cada N_j é um submódulo indecomponível de M, para $j = 1, 2, ..., s$, então $r = s$ e, reindexando os índices se necessário, nós temos $M_i \cong N_i$, para cada $i = 1, 2, ..., r$.

A demonstração do teorema segue dos resultados provados anteriormente. Vejamos:

Demonstração. Seja $M \neq \{0\}$ um A-módulo de comprimento finito.

Primeiro veremos que existe tal decomposição como dada em (D). Notemos que pela Proposição A.1.34, M satisfaz ACC e DCC, e então pela Proposição A.2.1 M possui uma decomposição de Krull-Schmidt, isto é, M possui uma decomposição em soma direta de submódulos indecomponíveis como dada em (D).

Agora, vejamos que esta decomposição é única a menos de isomorfismo.

Seja então

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_s \qquad (D')$$

outra decomposição de Krull-Schmidt. Note que, como M tem comprimento finito, então pela Observação A.1.33, cada M_i que aparece em (D) também tem comprimento finito, para $i = 1, 2, ..., r$. Além disso, já temos que cada M_i é indecomponível, segue então pela Proposição A.2.2 que cada M_i é, de fato, fortemente indecomponível. Segue agora, pela Proposição A.2.3 a unicidade da decomposição, a menos de isomorfismo, isto é, da Proposição A.2.3 temos que $r = s$ e, reindexando os índices se necessário, temos $M_i \cong N_i$, para cada $i = 1, 2, ..., r$. □

Referências Bibliográficas

[1] E. Abe, *Hopf Algebras*, Cambridge Univ. Press, 1977.

[2] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison - Wesley Publishing Company, Massachusetts, 1969.

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

[4] N. Jacobson, *Basic Algebra I*, W.H. Freeman and Company, New York, 1985.

[5] I. Kaplansky, *Bialgebras*, Lecture Notes in Mathematics, University of Chicago, 1975.

[6] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics 131, Springer-Verlag, New York, 2001.

[7] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics 189, Springer-Verlag, New York, 1999.

[8] R. G. Larson, M. E. Sweedler, *An associative orthogonal form for Hopf algebra*, Amer. J. Math. 91: 75-93, 1969.

[9] G. Martini, *Sobre a Semissimplicidade de Álgebras de Hopf Finito-Dimensionais e o Duplo de Drinfeld*, Porto Alegre, Instituto de Matemática da UFRGS, 2013.[Dissertação de Mestrado].

[10] F. C. P. Milies, *Anéis e Módulos*, USP, São Paulo, 1972.

[11] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS, Regional Conference Series in Mathematics 82, Providence, 1993.

[12] W. D. Nichols, M. B. Zöeller, *A Hopf algebra freeness theorem*, Amer. J. Math. 111: 381-385, 1989.

[13] W. D. Nichols, M. B. Zöeller, *Finite dimensional Hopf algebras are free over grouplike subalgebras*, J. Pure Appl. Algebra 56: 51-57, 1989.

[14] U. Oberst, H.-J. Schneider, *Untergruppen formeller Gruppen von endlichem Index*, J. Algebra, 31: 10-44, 1974.

[15] D. E. Radford, *Finiteness conditions for a Hopf algebra with a non-zero integral*, J. Algebra 46: 189-195, 1977.

[16] D. E. Radford, *Freeness (Projectivity) criteria for Hopf algebras over Hopf subalgebras*, J. Pure Appl. Algebra 11: 15-28, 1977.

[17] J. Rotman, *An Introduction to Homological Algebra*, Academic Press, 1979.

[18] M. E. Sweedler, *Hopf algebras*, W. A. Benjamin Inc., New York, 1969.

[19] M. E. Sweedler, *Integrals for Hopf algebras*, Ann. of Math. 89: 323-335, 1969.

[20] M. B. Zöeller, *Freeness of Hopf algebras over semisimple grouplike subalgebras*, J. Algebra, 118: 102-108, 1988.