Universidade Federal do Rio Grande
XI Jornada de Álgebra - 24 a 27 de abril de 2019

Álgerbas de Hopf: uma introdução

Notas do Minicurso

Alveri Alves Sant'Ana

Porto Alegre, 22 de abril de 2019

Sumário

Introdução **1**

1 Pré requisitos **4**
1.1 Anéis 4
1.2 Módulos. 12
1.3 Produto tensorial 23
1.4 Álgebras 38
1.5 A álgebra de grupo sobre corpos 43

2 Biálgebras **47**
2.1 Coálgebras 47
2.2 O dual de uma coálgebra 55
2.3 O dual finito de uma álgebra 58
2.4 Biálgebras 67
2.5 Quando o produto tensorial de H-módulos é ainda um H-módulo? 71

3 A Álgebra de convolução **75**
3.1 O produto convolução 75
3.2 Inversas convolutivas 76

4 Álgebras de Hopf **79**
4.1 Biálgebras com antípodas 79
4.2 Algumas propriedades da antípoda 83

5 Representações de álgebras de Hopf **87**
5.1 Comódulos 87
5.2 Módulos de Hopf 97

6 Ações e coações de álgebras de Hopf **105**
6.1 Ações e coações 105
6.2 O produto smash 109

Referências Bibliográficas **114**

Introdução

Estas notas foram escritas para servir de apoio a dois minicursos introdutórios sobre o tema, ministrados pelo autor, sendo o primeiro no workshop de verão organizado em conjunto pelos programas de pós-graduação em matemática e matemática aplicada da Universidde Federal do Rio Grande do Sul, ocorrido em Porto Alegre no período de 04 a 08 de fevereiro de 2019, e o segundo, na XI Jornada de àlgebra que ocorreu no período de 24 a 27 de abril de 2019, nas dependências da FURG, em Rio Grande. Como um bom número dos ouvintes inscritos nestes minicursos era formado por alunos de final de graduação, decidimos escrever estas notas.

A ideia aqui foi escrever umas notas o mais auto contidas possível, sendo que isto não é uma tarefa fácil, mas pensamos ter chegado bem próximo de um resultado satisfatório. Também, a escolha do material a ser apresentado em um minicurso de quatro ou cinco aulas se tronou uma tarefa desafiadora, pois como dito antes, a maioria dos ouvintes teria pouca experiência em álgebra, motivo pelo qual, o curso ganha uma visão de um curso de divulgação de área, e esperamos que o desenvolvimento do mesmo ocorra de forma satisfatória no sentido de que os alunos ouvintes se interessem pelo assunto e uma parte deles decidam estudar este tema com maior profundidade no futuro.

Uma álgebra de Hopf sobre um corpo pode ser pensada como uma generalização da álgebra de grupo. Sejam $\Bbbk$ um corpo, G um grupo e $\Bbbk G$ a álgebra de grupo correspondente. Esta álgebra carrega consigo uma estrutura adicional que nos permite enxergar o próprio corpo base como um $\Bbbk G$-módulo, o produto tensorial de $\Bbbk G$-módulos é novamente um $\Bbbk G$-módulo, e o dual de um $\Bbbk G$-módulo é também um $\Bbbk G$-módulo. O nosso estudo das álgebras de Hopf, começa por analisar quais propriedades estas estruturas adicionais podem possuir. Assim nascem os conceitos de coálgebras e de biálgebras. Uma álgebra de Hopf será então uma biálgebra com uma antípoda.

Por se tratar de um texto introdutório, destinado a uma audiência formada por pessoas que não tem muita experiência no tema, o texto aqui apresentado não é original, e em muitos casos, se aproxima bastante daqueles citados nas referências.

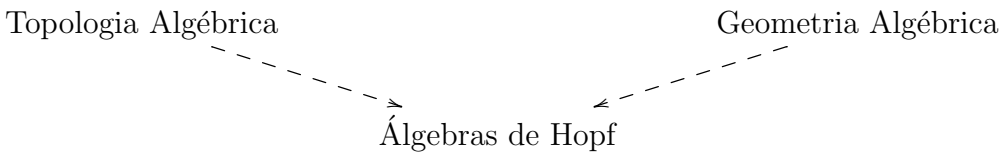
Agradeço às Comissões Organizadoras, tanto do Workshop organizado pelos Programas de Pós-Graduação em Matemática e de Matemática Aplicada como da XI Jornada de

Álgebra, pela oportunidade em ministrar este minicurso nestes eventos. Desde já também quero agradecer a colaboração dos estudantes que vierem a assistir este minicurso, pelas correções necessárias do texto (devem existir muitas ainda!), bem como por sugestões que venham a aprimorá-lo.

Um breve de histórico

Faremos aqui um breve histórico sobre o nascimento e o desenvolvimento inicial da teoria das álgebras de Hopf. Este texto está baseado em [1], onde pode ser encontrado informações mais profundas sobre os temas abordados aqui.

As álgebras de Hopf nasceram da confluência de duas importantes áreas da matemática, a saber, a topologia algébrica e a geometria algébrica.



- A primeira definição formal de uma álgebra de Hopf é devido a **P. Cartier** (1956), (ainda sob o codinome de hiperálgebras).
- O primeiro a usar a nomeclatura *álgebra de Hopf* foi **A. Borel** (1953).

Vertente da topologia algébrica:

H. Hopf (1941): Considera uma variedade M munida de um produto (uma função continua $M \times M \to M$) o qual induz um morfismo $H \to H \otimes H$, onde H é o anel de cohomologia de M. Impondo certas restrições a H, Hopf obtém importantes resultados topológicos sobre M.

A. Borel (1953): Estuda a homologia de um feixe de fibras principais e aplicações a homologia dos espaços homogêneos. Borel chama de álgebra de Hopf uma álgebra que satisfaz as condições de Hopf. Isto não coincide com o que se conhece hoje por álgebras de Hopf.

J. Milnor & J. Moore (1959/1965): Neste trabalho os autores definem explicitamente uma álgebra de Hopf como sendo o que hoje se conhece por uma biálgebra graduada. Se o espaço homogêneo de grau zero for unidimensional, é mostrado a existência de uma antípoda. Eles generalizam resultados de Hopf, Borel e outros.

Vertente da geometria algébrica:

J. Dieudonné (1954): Desejando estender o dicionário *Grupos de Lie - Álgebras de Lie* em característica positiva, Dieudonné associa uma álgebra associativa a um grupo de Lie, chamada de hiperálgebra, a qual reflete as propriedades estruturais deste grupo. Esta álgebra é munida de um coproduto cuja dualização é o produto do grupo, e coincide com a envolvente universal da álgebra de Lie de G, no caso de característica zero.

P. Cartier (1956): Apresenta uma definição formal de uma hiperálgebra abstrata, a qual coincide com uma biálgebra cocomutativa com filtração coradical. Esta filtração induz a existência de uma antípoda, fato não mencionado por Cartier. Assim, as hiperálgebras de Cartier são as nossas álgebras de Hopf cocomutativas.

B. Konstanz (1966): Aparece pela primeira vez a definição de uma álgebra de Hopf como a conhecemos hoje. Boa parte da nomeclatura usada atualmente no contexto das álgebras de Hopf é devido a Konstanz, como por exemplo *elementos group-like*.

Ganhando vida própria...

M. Sweedler (1969): Foi a partir da publicação do livro de Sweedler que as álgebras de Hopf ganharam independência como área de pesquisa. Sweedler apresenta um exemplo de uma álgebra de Hopf não comutativa, de dimensão 4 sobre um corpo de característica distinta de 2.

V. Drinfel'd (1987): A partir dos trabalhos de Drinfel'd esta área de pesquisa vivencia um extraordinário avanço, com mudanças radicais em termos de métodos, abordagens e interação com outros ramos da matemática.

Capítulo 1

Pré requisitos

Neste capítulo apresentaremos alguns dos pré-requisitos necessários ao entendimento do texto. Aqui serão tratados temas como anéis, módulos, álgebras, produto tensorial entre outros. Os leitores mais experientes podem passar diretamente aos capítulos seguintes.

1.1 Anéis

Neste texto estaremos sempre interessados em anéis com unidadade, motivo pelo qual já introduziremos um axioma da unidade na definição de anel, mas chamamos a atenção do leitor que é possível desenvolver uma teoria de anéis sem unidade.

Definição 1.1.1. *Dizemos que um conjunto R, munido de duas operações binárias, chamadas soma $(+)$ e multiplicação $(\cdot)$, é um anel, se valem as seguintes propriedades:*

(i) $(R,+)$ *é um grupo abeliano, isto é,* $+$ *é associativa, possui elemento neutro, possui elemento simétrico e é comutativa,*

(ii) $\cdot$ *é associativa,*

(iii) $\cdot$ *possui elemento neutro.*

(iv) $+$ *e* $\cdot$ *são compatíveis, isto é, para todos* $a,b,c \in R$ *vale que*

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad e \quad (a+b)\cdot c = a\cdot c + b\cdot c,$$

Lembramos que uma operação $\star$ definida em um conjunto A nada mais é do que uma função $\star : A\times A \to A$. Além disso, dizemos que:

- $\star$ é *associativa*, se $a\star(b\star c) = (a\star b)\star c$, $\forall a,b,c \in A$;

- $\star$ *possui elemento neutro*, se existir um elemento $e \in A$ tal que $e \star a = a = a \star e$, $\forall a \in A$;

- $\star$ *possui elemento simétrico*, se $\forall a \in A, \exists a' \in A$ tal que $a \star a' = e = a' \star a$, onde e é um elemento neutro de $\star$.

- $\star$ é *comutativa*, se $a \star b = b \star a$, $\forall a, b \in A$.

É possível mostrar que elementos neutros e simétricos, quando existem, são unicamente determinados. Assim, estes elementos podem ser denotados por algum símbolo especial. No caso de anéis, denotaremos o elemento neutro da soma sempre por 0, e o chamaremos de *elemento zero* do anel, já o elemento neutro da multiplicação será denotado por 1, e o chamaremos de elemento unidade do anel. Também, denotaremos por $-a$ o simétrico aditivo do elemento a.

Notaremos um anel por $(R, +, \cdot)$, mas quando não houver possibilidade de confusão, escreveremos apenas R em lugar de $(R, +, \cdot)$, sem especificar as operações consideradas. Também, vamos escrever ab em lugar de $a \cdot b$, quando estivermos nos referindo ao elemento dado pela multiplicação de a por b.

Exemplo 1.1.2. *Os conjuntos $\mathbb{Z}$ (dos números inteiros), $\mathbb{Q}$ (dos números racionais), $\mathbb{R}$ (dos números reais) e $\mathbb{C}$ (dos números complexos), com as operações usuais de soma e multiplicação, são exemplos de anéis.*

Exemplo 1.1.3. *Se R é um anel, então o conjunto $\mathcal{M}_n(R)$, das matrizes $n \times n$ com entradas em R, com as operações usuais de soma e multiplicação de matrizes, é um anel.*

A partir destes exemplos podemos construir novos, através das seguintes técnicas: Se $R_1, R_2, ..., R_n$ são anéis, então o produto cartesiano $\mathcal{R} = R_1 \times R_2 \times \cdots \times R_n$ é um anel, onde as operações são definidas componente a componente. Se $(R, +, \cdot)$ é um anel, então pode-se mostrar que $R^{op} = (R, +, \bullet)$ também é um anel, onde $\bullet$ é definida por: $a \bullet b = b \cdot a, \forall a, b \in R$. R^{op} é chamado de *anel oposto de R*.

O exemplo acima foi obtido fazendo a restrição das operações do anel $\mathbb{Z}$ ao subconjunto $n\mathbb{Z}$. Isto sugere uma nova definição.

Definição 1.1.4. *Sejam $(R, +, \cdot)$ um anel e $\emptyset \neq S \subseteq R$. Então dizemos que S é um subanel de R, se as restrições das operações de R em S estão bem definidas e $(S, +_{|S}, \cdot_{|S})$ é um anel eventualmente sem unidade, isto é, $(S, +_{|S}, \cdot_{|S})$ satisfaz os axiomas $(i), (ii)$ e (iv) da Definição 1.1.1.*

Antes de prosseguir, desejamos dar uma palavrinha a respeito de restringirmos a existência de unidade em subanéis. Isto se deve ao fato de que mais adiante estaremos

interessados nos subanéis para os quais podemos considerar estruturas quocientes, com as operações induzidas pelas operações do anel, os quais serão chamados de ideais. Vamos ver que ideais contendo unidade coincidem com o próprio anel e não poderíamos chamar estes subanéis especiais (os ideais) de subanéis, se exigíssemos a presença da unidade em subanéis. Sempre que estudamos alguma estrutura algébrica estamos interessados naquelas subestruturas que nos permitem construir estruturas quocientes. No caso de anéis, estas subestruturas são os ideais. Na teoria de grupos, por exemplo, os subgrupos que nos permitem construir grupos quocientes são os subgrupos normais.

Se consideramos as imersões canônicas $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, então podemos ver $\mathbb{Q}$ como um subanel de $\mathbb{R}$ e de $\mathbb{C}$, assim como $\mathbb{R}$ se torna um subanel de $\mathbb{C}$. Se S é um subanel de R, então é fácil verificar que $\mathcal{M}_n(S)$ é um subanel de $\mathcal{M}_n(R)$. Se R é um anel, então o subconjuto $\mathcal{Z}(R) := \{a \in R : ax = xa, \forall x \in R\}$ é um subanel de R (verifique isto!), chamado *centro de* R. Além disso, é fácil verificar que o conjunto dos múltiplos de um inteiro n fixo, denotado por $n\mathbb{Z}; = \{na : a \in \mathbb{Z}\}$, é um subanel de $\mathbb{Z}$. É possível mostrar que todos os subanéis de $\mathbb{Z}$ são desta forma.

Os próximos exercícios nos fornecem propriedades básicas das operações de um anel, que serão usadas livremente no texto.

Exercício 1.1.5. *Mostre que elementos neutros e simétricos, quando existem, estão unicamente determinados.*

Exercício 1.1.6. *Sejam R um anel e $a, b, c \in R$. Mostre que:*

(i) $0 \cdot a = a \cdot 0 = 0$,

(ii) $-(ab) = (-a)b = a(-b)$,

(iii) $(-a)(-b) = ab$.

(iv) $(-1)a = a(-1) = -a$,

(v) $(-1)(-1) = 1$,

(vi) $(-1)(-a) = a$.

Também é um exercício de fácil verificação o seguinte resultado, o qual nos dá uma caracterização dos subconjuntos de um anel que são seus subanéis.

Proposição 1.1.7. *Sejam R um anel e S um subconjunto de R. Então S é um subanel de R se, e somente se, as seguintes condições se verificam:*

(i) $0 \in S$;

(ii) $x, y \in S \Rightarrow x - y \in S$;

(iii) $x, y \in S \Rightarrow xy \in S$.

Dado um anel R, dizemos que R é um *anel comutativo* se a multiplicação de R é uma operação comutativa, isto é, se $xy = yx$, para todos elementos $x, y \in R$. Os anéis $\mathbb{Z}, n\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de anéis comutativos. Os anéis de matrizes em geral são não comutativos. É fácil verificar que R é um anel comutativo se, e somente se, $R = R^{op}$.

Um elemento a em um anel R é chamado de *divisor de zero* se existir $0 \neq b \in R$ tal que $ab = 0 = ba$. Já um elemento u em um anel R é dito um *elemento invertível* se existir $v \in R$ tal que $uv = 1 = vu$.

Um anel comutativo sem divisores de zero, além do próprio elemento 0, é dito um *domínio de integridade* (ou simplesmente um domínio). Um anel com unidade em que todo elemento não nulo é invertível é chamado de um *anel de divisão*. Por fim, um anel de divisão comutativo é chamado um *corpo*.

É fácil ver que $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos, que $\mathbb{Z}$ é um domínio (que não é um corpo). Também é fácil obter exemplos de divisores de zero em anéis de matrizes.

Vamos agora apresentar um exemplo de um anel de divisão que não é um corpo. Lembramos que o *anel dos quatérnios* $\mathbb{H}$ sobre os reais está definido como sendo o espaço vetorial 4-dimensional sobre $\mathbb{R}$ gerado pelos elementos $1, i, j, k \in \mathbb{H}$, com a multiplicação dada pelas seguintes relações: $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -k, kj = -i$ e $ik = -j$.

Quando se estuda uma certa estrutura algébrica, precisamos considerar as funções entre elas, que tem a propriedade de preservar a dada estrutura. Como as estruturas algébricas estão definidas em função de certas operações, precisamos então considerar as funções que preservam estas operações. Estas funções levam o nome de *homomorfismos*. Vamos apresentar uma definição mais precisa, para o caso de anéis.

Definição 1.1.8. *Sejam $R = (R, +_R, \cdot_R)$ e $S = (S, +_S, \cdot_S)$ dois anéis. Uma função $f : R \to S$ é dita um homomorfismo de anéis, se:*

- $f(a +_R b) = f(a) +_S f(b), \forall a, b \in R$,
- $f(a \cdot_R b) = f(a) \cdot_S f(b), \forall a, b \in R$.

Antes de apresentarmos exemplos de homomorfismos de anéis, vejamos algumas propriedades que decorrem diretamente da definição.

Proposição 1.1.9. *Sejam R e S anéis e $f : R \to S$ um homomorfismo de anéis. Então valem as seguintes propriedades:*

(i) $f(0_R) = 0_S$,

(ii) $f(-a) = -f(a), \forall a \in R$,

(iii) $f(R)$ *é um subanel de* S.

Demonstração. (i) Basta observar que $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$, de onde segue que $f(0_R) = 0_S$, pois $f(0_R)$ e 0_S são ambas soluções da equação $f(0_R) + X = f(0_R)$ em S.

(ii) Temos que mostrar que $f(-a) + f(a) = 0_S$. Mas isto segue diretamente do item anterior, pois $f(-a) + f(a) = f(-a + a) = f(0_R) \overset{(i)}{=} 0_S$. Logo, $f(-a)$ é o simétrico de $f(a)$ em S.

(iii) Por (i), temos que $0_S \in \mathcal{I}m\, f$. Dados $x, y \in \mathcal{I}m\, f$, segue que existem $a, b \in R$ tais que $f(a) = x$ e $f(b) = y$. Assim, $x - y = f(a) - f(b) = f(a - b)$ e $xy = f(a)f(b) = f(ab)$ e, consequentemente, $x - y, xy \in \mathcal{I}m\, f$. Segue então da Proposição 1.1.7 que $\mathcal{I}m\, f$ é um subanel de S. □

Seja $f : R \to S$ um homomorfismo de anéis. Dizemos que f é um *monomorfismo* se f for injetor. Neste caso, S é dito uma *extensão* de R. Dizemos que f é um *epimorfismo* se f for sobrejetor. No caso em que f é bijetor, então dizemos que f é um *isomorfismo*. Neste último caso, R e S são cópias um do outro, como anéis, e dizemos que eles são anéis isomorfos, notando por $R \simeq S$. Cabe observar que se $f : R \to S$ é um monomorfismo de anéis, então f é um isomorfismo sobre sua imagem e, neste caso, S contém um subanel que é uma cópia de R. Identificando estes anéis, podemos então dizer que R é um subanel de S. Isto é o que se faz, por exemplo, quando se diz que $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, pois neste caso, estamos considerando o homomorfismo $f : \mathbb{Z} \to \mathbb{Q}$ definido por $f(a) = \frac{a}{1} \in \mathbb{Q}$, para todo $a \in \mathbb{Z}$.

Exemplo 1.1.10. *Sejam R e S dois anéis quaisquer. A função $f : R \to S$ definida por $f(a) = 0$, para todo elemento $a \in R$, é um homomofismo de anéis, chamado homomorfismo nulo. A função $id_R : R \to R$, dada por $id_R(a) = a$, é um homomorfismo de anéis, chamado homomorfismo identidade.*

O próximo exemplo mostra que pode não existirem muitos homomorfismos entre dois anéis.

Exemplo 1.1.11. *Se $f : \mathbb{Z} \to \mathbb{Z}$ é um homomorfismo de anéis, então f é o homomorfismo nulo ou f é o homomorfismo identidade.*

De fato, pois se $n \in \mathbb{Z} \setminus \{0\}$, então $n = 1 + 1 + \cdots + 1$ (n vezes, se $n > 0$) ou $n = -1 + (-1) + \cdots + (-1)$ ($-n$ vezes, se $n < 0$). Suponhamos, sem perda de generalidade,

que $n > 0$. Então, $f(n) = f(1) + f(1) + \cdots + f(1)$ (n vezes). Portanto, para se definir um homomorfismo cujo domínio é $\mathbb{Z}$, basta definir $f(1)$. Claramente, se $f(1) = 0$ então f é o homomorfiso nulo. Por outro lado, observamos que $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$, ou seja, $f(1)(1 - f(1)) = 0$, de onde segue que $f(1) = 0$ ou $f(1) = 1$. Consequentemente, devemos ter que f é o homomorfismo nulo ou f é o homomorfismo identidade. Este resultado pode ser generalizado para domínios de integridade quaisquer, como mostra o próximo exercício.

Definição 1.1.12. *Seja $f : R \to S$ um homomorfismo de anéis. Chamamos de núcleo de f ao conjunto $\mathcal{N}uc\, f = \{a \in R : f(a) = 0\}$.*

O núcleo de um homomorfismo tem propriedades bastante interessantes. Começamos por observar que se $f : R \to S$ é um homomorfismo de anéis e $f(a) = f(b)$, para certos elementos $a, b \in R$, então devemos ter $f(a - b) = f(a) - f(b) = 0$ em S, ou seja, $a - b \in \mathcal{N}uc\, f$. Isto nos diz que se dois elementos de R têm a mesma imagem por um homomorfismo, então a diferença deles deve estar no seu núcleo. Assim, homomorfismos com núcleo nulo devem ser injetores. A recíproca deste fato é claramente verdadeira, de modo que temos o seguinte resultado.

Proposição 1.1.13. *Um homomorfismo de anéis $f : R \to S$ é injetor se, e somente se, $\mathcal{N}uc\, f = \{0\}$.*

Assim, o núcleo de um homomorfismo nos dá uma medida de quão longe de ser injetor este homomorfismo está. Mais ainda, o núcleo de um homomorfismo é um subanel. De fato, pois se $f : R \to S$ é um homomorfismo de anéis, então $f(0_R) = 0_S$, ou seja, $0_R \in \mathcal{N}uc\, f$. Tomando-se $x, y \in \mathcal{N}uc\, f$, temos claramente que $f(x - y) = 0$ e $f(xy) = 0$, de onde segue que $x - y, xy \in \mathcal{N}uc\, f$. Segue então da Proposição 1.1.7 que $\mathcal{N}uc\, f$ é um subanel de R. Este subanel tem uma propriedade especial, a saber, a absorção da multiplicação tanto pela esquerda como pela direita. Mais precisamente, se $f : R \to S$ é um homomorfismo de anéis, $x \in \mathcal{N}uc\, f$ e $a \in R$, então $ax, xa \in \mathcal{N}uc\, f$. De fato, pois $f(ax) = f(a)f(x) = f(a)0 = 0$. Analogamente, $f(xa) = 0$. Isto induz a seguinte definição.

Definição 1.1.14. *Dado um anel R, dizemos que um subanel I de R é um:*

(i) ideal à esquerda de R, se $xa \in I$, sempre que $x \in R$ e $a \in I$,

(ii) ideal à direita de R, se $ax \in I$, sempre que $x \in R$ e $a \in I$,

(iii) ideal de R, se I é um ideal à esquerda e à direita de R.

Vamos usar as seguintes notações para representar estes tipos de ideais: escreveremos $I \lhd R$, para dizer que I é um ideal de R; notaremos por $I \lhd_r R$ os ideais à direita e por $I \lhd_l R$ os ideais à esquerda de R.

Como vimos acima, núcleos de homomorfismos são exemplos de ideais, mas nem todo subanel é um ideal, pois é fácil ver que $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ que não é um ideal de $\mathbb{Q}$. Também é fácil ver que se I é um ideal à esquerda de R, então I é um ideal à direita de R^{op}. Assim, os três conceitos acima coincidem num anel comutativo. Vejamos alguns exemplos destas estruturas em anéis não comutativos, onde elas diferem.

Exemplo 1.1.15. *Seja R um anel e consideremos $S = \mathcal{M}_n(R)$ o anel de matrizes $n \times n$ com entradas em R. Então, fixando-se $k \in \{1, 2, ..., n\}$, temos que:*

- *$\mathcal{I}_k := \{(a_{ij}) \in S : a_{ij} = 0, \text{ se } j \neq k\}$ é um ideal à esquerda de S, que não é um ideal à direita de S.*
- *$\mathcal{J}_k := \{(a_{ij}) \in S : a_{ij} = 0, \text{ se } i \neq k\}$ é um ideal à direita de S, que não é um ideal à esquerda de S.*

Vamos classificar os ideais de $\mathbb{Z}$ usando conhecimentos da aritmética dos números inteiros.

Já sabemos que para cada $n \in \mathbb{Z}$, o conjunto $I = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ é um subanel de $\mathbb{Z}$. Vamos ver que estes conjuntos são na verdade, ideais de $\mathbb{Z}$. De fato, pois se $x \in \mathbb{Z}$, então $x(na) = (na)x = n(xa) \in n\mathbb{Z}$. Reciprocamente, se I é um ideal de $\mathbb{Z}$ e $a \in I$ é o menor inteiro positivo em I, então $I = a\mathbb{Z}$. Isto decorre da divisão euclidiana, já que se $x \in I$, então existem elementos unicamente determinados $q, r \in \mathbb{Z}$ tais que $x = aq + r$, com $0 \leq r < a$. Mas então, devemos ter $r = x - aq \in I$, de onde segue que $r = 0$, pela minimalidade de a em I. Logo, $x = aq \in a\mathbb{Z}$, o que conclui nosso raciocínio.

Uma outra aplicação dos ideais na teoria de anéis são os anéis quocientes. Veremos abaixo que os ideais são exatamente os subanéis para os quais podemos induzir uma estrutura de anel no conjunto quociente, tal como se faz com a aritmética modular dos inteiros. Se $n \in \mathbb{Z}$, então a relação dada por:

$$x, y \in \mathbb{Z},\ x \equiv y \overset{def}{\Leftrightarrow} x - y \in n\mathbb{Z}$$

é uma relação de equivalência e o conjunto quociente $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$ tem uma estrutura de anel $(\mathbb{Z}/n\mathbb{Z}, \overline{+}, \overline{\cdot})$, dada por:

- $\overline{a} \ \overline{+} \ \overline{b} := \overline{a + b}, \forall a, b \in \mathbb{Z}$,
- $\overline{a} \ \overline{\cdot} \ \overline{b} := \overline{a \cdot b}, \forall a, b \in \mathbb{Z}$

As igualdades acima podem ser facilmente verificadas, usando propriedades dos restos da divisão euclidiana em $\mathbb{Z}$, pois se $x - y \in n\mathbb{Z}$, então existe $q \in \mathbb{Z}$ tal que $x - y = nq$, ou seja, $x = nq + y$. Agora é só observar que se x e y estão relacionados pela equação acima, então ambos deixam o mesmo resto na divisão euclidiana por n.

Vamos generalizar estas ideias para anéis quaisquer. Sejam R um anel e I um subanel de R. Não é difícil verificar que a relação definida em R por:

$$x, y \in R, x \equiv_I y \overset{def}{\Leftrightarrow} x - y \in I$$

é uma relação de equivalência em R. O que não se consegue mostrar é que a aplicação $\dot{\cdot} : R/I \times R/I \to R/I$ definida por

$$\overline{x} \dot{\cdot} \overline{y} := \overline{x \cdot y}, \forall x, y \in R$$

está bem definida. Para que esta aplicação esteja bem definida, e portanto ser uma operação em R/I, é necessário exigir que o subanel I seja de fato um ideal de R. Deixamos este fato para ser mostrado no seguinte exercício.

Exercício 1.1.16. *Sejam R um anel, I um subanel de R e $\equiv_I$ a relação de equivalência dada por: $x, y \in R$; $x \equiv_I y \Leftrightarrow x - y \in I$. Mostre que*

$$\dot{\cdot} : R/I \times R/I \to R/I,$$

definida por $\dot{\cdot}(\overline{a}, \overline{b}) := \overline{a \cdot b}$, é uma função se, e somente se, I é um ideal de R.

Além disso, precisamos ver que as propriedades de associatividade, comutatividade, existência de neutro e de simétrico são herdadas por operações induzidas em conjuntos quocientes, mas isto também é de fácil verificação e será deixada ao encargo do leitor.

Portanto, se I é um ideal de R, então podemos considerar o anel quociente R/I. Assim, fica definido um homomorfismo de anéis $\pi : R \to R/I$, por $\pi(a) = \overline{a} := a + I = \{a + x : x \in I\}$, o qual é chamado de *projeção canônica em relação ao ideal I*. É fácil ver que este homomorfismo é sobrejetor e que seu núcleo é exatamente o ideal I. Isto mostra que todo ideal é o núcleo de algum homomorfismo de anéis. Assim, podemos caracterizar os ideais como sendo aqueles subanéis que são núcleos de homomorfismos.

Outra observação pertinente é que se $f : R \to S$ é um homomorfismo de anéis, então os elementos de R que tem mesma imagem por f são identificados no anel quociente $R/\mathcal{N}uc\, f$. Assim, deveríamos poder mergulhar este anel quociente em S. De fato, isto é possível, como mostra o próximo resultado.

Teorema 1.1.17. (Teorema dos Homomorfismos para anéis) *Sejam R, S anéis e $f : R \to S$ um homomorfismo de anéis. Então existe um único monomorfismo de anéis $\overline{f} : R/\mathcal{N}uc\, f \to S$ tal que $\overline{f} \circ \pi = f$*

Demonstração. Basta definir $\overline{f}(\overline{a}) = f(a)$, para todo $\overline{a} \in R/\mathcal{N}uc\, f$. Vejamos que assim $\overline{f}$ está bem definida. De fato, pois se $\overline{a} = \overline{b}$ em $R/\mathcal{N}uc\, f$, então $a - b \in \mathcal{N}uc\, f$, ou seja,

$f(a-b)=0$, de modo que $f(a)=f(b)$, pois f é um homomorfismo de anéis. Assim temos $\overline{f}(\overline{a})=\overline{f}(\overline{b})$. Além disso, por definição, temos que $f(a)=\overline{f}(\overline{a})=\overline{f}(\pi(a))=\overline{f}\circ\pi(a)$, para todo $a\in R$, ou seja, $\overline{f}\circ\pi=f$.

Afirmamos que $\overline{f}$ é injetora. De fato, pois se $\overline{a}\in\mathcal{N}uc\,\overline{f}$, então $\overline{f}(\overline{a})=0$, ou seja, $0=\overline{f}(\overline{a})=f(a)$, de onde segue que $a\in\mathcal{N}uc\,f$, o que nos diz que $\overline{a}=\overline{0}$. Resta mostrar a unicidade de $\overline{f}$. Para tal, suponhamos que $g: R/\mathcal{N}uc\,f\to S$ é tal que $g\circ\pi=f$. Mas então, para cada $\overline{a}\in R/\mathcal{N}uc\,f$, temos $g(\overline{a})=g\circ\pi(a)=f(a)=\overline{f}(\overline{a})$, e segue que $g=\overline{f}$. □

A seguinte consequência do resultado acima é imediata.

Corolário 1.1.18. *Com as notações do Teorema anterior, se f é um epimorfismo, então $R/\mathcal{N}uc\,f\simeq S$ como anéis.*

Vamos discutir o próximo exemplo a luz dos nossos resultados. Consideremos $R=\left\{\begin{bmatrix} a & x\\ 0 & a\end{bmatrix}: a\in\mathbb{Z}, x\in\mathbb{Q}\right\}$. É fácil verificar que R, com as operações usuais de matrizes, é um anel comutativo com unidade (verifique isto!). Afirmamos que $J:=\left\{\begin{bmatrix} 0 & x\\ 0 & 0\end{bmatrix}: x\in\mathbb{Q}\right\}$ é um ideal de R. Faremos isto mostrando que J é o núcleo de um homomorfismo de anéis (mostre isto diretamente). De fato, basta definir o homomorfismo $\varphi: R\to\mathbb{Z}$, por $\varphi\left(\begin{bmatrix} a & x\\ 0 & a\end{bmatrix}\right)=a$. É fácil ver que φ é um homomorfismo de anéis e que $J=\mathcal{N}uc\,\varphi$, de onde segue que J é um ideal de R. Mais ainda, como φ é sobrejetor, segue que $R/J\simeq\mathbb{Z}$.

1.2 Módulos.

Pretendemos nesta seção apresentar fatos básicos da teoria de módulos, os quais serão essenciais ao entendimento do texto. Grosso modo, um módulo é um *espaço vetorial* sobre um anel. O fato de a estrutura de anel ser menos rígida que a de um corpo faz com que a teoria de módulos seja bastante distinta da teoria de espaços vetoriais, mas chamamos a atenção do leitor para que o mesmo, ao ler uma definição ou um resultado sobre módulos, ele imediatamente pense o que aquilo significa no caso de espaços vetoriais, para facilitar o entendimento do que se apresenta em cada momento.

Começamos com o seguinte conceito.

Definição 1.2.1. *Seja R um anel (com unidade). Dizemos que $(M,+_M)$ é um R-módulo à esquerda, se $(M,+_M)$ for um grupo abeliano (i. é, $+_M$ é associativa, possui neutro, possui simétrico e é comutativa) e, além disso, existir uma aplicação $\bullet: R\times M\to M$ (chamada de ação de R em M), satisfazendo as seguintes propriedades:*

(i) $1_R \bullet m = m, \forall m \in M$,

(ii) $r \bullet (m_1 +_M m_2) = r \bullet m_1 +_M r \bullet m_2; \forall r \in R, \forall m_1, m_2 \in M$,

(iii) $r_1 \bullet (r_2 \bullet m) = (r_1 \cdot r_2) \bullet m; \forall r_1, r_2 \in R, \forall m \in M$,

(iv) $(r_1 + r_2) \bullet m = (r_1 \bullet m) +_M (r_2 \bullet m); \forall r_1, r_2 \in R, \forall m \in M$.

Analogamente, podemos definir um R-módulo à direita, bastando considerar uma ação de R em M pela direita, ou seja, uma aplicação $\bullet : M \times R \to M$, satisfazendo os mesmos axiomas acima, devidamente adaptados. Notaremos um R-módulo à esquerda por ${}_RM$ e por M_R, um R-módulo à direita.

Na definição acima, escrevemos $+_M$ para denotar a soma de M, e não confundir com a soma $+$ de R. O mesmo foi feito em relação as notações da ação de R em M, denotada por $\bullet$ e a multiplicação de R. Mas no que segue, vamos denotar tanto a soma de R quanto a soma de M por $+$, e a multiplicação de R bem como a ação de R em M, por justaposição dos elementos, ou seja, se $r_1, r_2 \in R$ e $m \in M$, escreveremos $r_1 r_2$ para denotar a multiplicação de r_1 por r_2 em R e também, $r_1 m$ para denotar a ação de r_1 em m, pois não haverá perigo de confusão.

Antes de apresentar exemplos, gostaríamos de observar que se M é um R-módulo à esquerda, então M é um R^{op}-módulo à direita, e vice-versa, como é fácil verificar. Assim, a teoria de módulos é completamente simétrica e todo resultado que vale para módulos à esquerda também vale para módulos à direita, de modo que podemos fixar os adjetivos "à esquerda"ou "à direita" para desenvolvermos nossa teoria. Além disso, se R é um anel comutativo, então os conceitos de módulos à direita e de módulos à esquerda coincidem e, neste caso, escreveremos apenas R-módulo.

Exemplo 1.2.2. *Seja $\Bbbk$ um corpo. Então um $\Bbbk$-módulo nada mais é do que um $\Bbbk$-espaço vetorial.*

Exemplo 1.2.3. *Todo grupo abeliano é um $\mathbb{Z}$-módulo.*

De fato, se $(G, +)$ é um grupo abeliano (aditivo), então basta considerar a ação dada por:

- $0_{\mathbb{Z}} g = 0_G$
- $ng = g + g + \cdots + g (n \text{ vezes })$, se $n > 0$
- $ng = (-g) + (-g) + \cdots + (-g) (-n \text{ vezes })$, se $n < 0$.

Exemplo 1.2.4. *Todo anel é um módulo sobre si mesmo, tanto à esquerda quanto à direita, com a ação dada pela própria multiplicação.*

Com relação ao exemplo acima, o R-módulo à esquerda ${}_RR$ é chamado de *módulo regular à esquerda*, e o R-módulo à direita R_R é chamado de *módulo regular à direita*. Observamos neste momento que se R não for comutativo, então a estrutura destes dois módulos regulares não precisam necessariamente coincidirem, de modo que muitas vezes o módulo regular à esquerda possui uma propriedade que o módulo regular à direita não possui e vice-versa. Vamos ver exemplos deste fato mais adiante.

Exemplo 1.2.5. *Consideremos S o anel de matrizes $n \times n$ com entradas num anel R. Seja N o conjunto de todas as matrizes $n \times 1$ com entradas em R. Então N é um grupo abeliano aditivo com a soma de matrizes. Assim, N torna-se um S-módulo à esquerda via a multiplicação usual de matrizes. De modo análogo se mostra que o conjunto L das matrizes $1 \times n$, com entradas em R, é um S-módulo à direita.*

O seguinte exemplo é usado livremente no texto.

Exemplo 1.2.6. *Sejam R e S anéis e $f : R \to S$ um homomorfismo de anéis. Então todo S-módulo à esquerda possui uma estrutura de R-módulo à esquerda. De fato, se M é um S-módulo à esquerda via uma ação $\triangleright : S \otimes M \to M$, $(s, m) \mapsto s \triangleright m$, então basta definir a ação de R em M por $\cdot : R \otimes M \to M$, onde $r \cdot m := f(r) \triangleright m$. Note que neste caso, $1_R \cdot m = f(1_R) \triangleright m = 1_S \triangleright m = m$, $r \cdot (m_1 + m_2) = f(r) \triangleright (m_1 + m_2) = f(r) \triangleright m_1 + f(r) \triangleright m_2 = r \cdot m_1 + r \cdot m_2$ e que $r_1 \cdot (r_2 \cdot m) = f(r_1) \triangleright (f(r_2) \triangleright m) = (f(r_1) f(r_2) \triangleright m = f(r_1 r_2) \triangleright m = (r_1 r_2) \cdot m$, sempre que $r, r_1, r_2 \in R$, $m, m_1, m_2 \in M$. Os demais axiomas de definição de um módulo seguem do fato que M é um grupo abeliano e da linearidade de f.*

Como dito antes, uma vez que estamos estudando módulos, queremos estudar as funções que preservam esta estrutura e também estudar as subestruturas bem como estruturas quocientes dos módulos. Passaremos a definir estes objetos mais precisamente.

Definição 1.2.7. *Sejam R um anel e M um R-módulo à esquerda. Dizemos que um subconjunto não vazio N de M é um submódulo de M (ou um R-submódulo de M), se $(N, +)$ é um subgrupo de $(M, +)$ e a restrição da ação de R em N induz uma estrutura de R-módulo em N.*

Vamos escrever $N \leq M$ para dizer que N é um submódulo de M. O próximo resultado caracteriza os subconjuntos de um módulo que são submódulos deste.

Proposição 1.2.8. *Sejam R um anel, M um R-módulo à esquerda e $N \subseteq M$. Então N é um submódulo de M se, e somente se:*

(i) $0 \in N$,

(ii) $\forall n_1, n_2 \in N \Rightarrow n_1 + n_2 \in N$,

(iii) $\forall r \in R, n \in N \Rightarrow rn \in N$.

A demonstração da proposição acima será deixada como um exercício. Vejamos alguns exemplos.

Exemplo 1.2.9. *Os submódulos de um módulo regular à esquerda (resp. à direita) são exatamente os ideais à esquerda (resp. à direita) do anel base.*

O exemplo acima nos diz que podemos estudar a estrutura dos ideais de um anel, estudando a estrutura de submódulos de um módulo. Assim, toda propriedade válida para módulos pode ser traduzida para a linguagem de anéis, via ideais à esquerda (ou à direita).

Exemplo 1.2.10. *Os submódulos de um espaço vetorial são exatamente os seus subespaços vetoriais.*

Exemplo 1.2.11. *Os subgrupos de um grupo abeliano G são os $\mathbb{Z}$-submódulos de G.*

O próximo exemplo nos dá uma receita de como obtermos novos submódulos a partir de outros já conhecidos.

Exemplo 1.2.12. *Sejam M um R-módulo à esquerda e $\mathcal{F} = \{N_i\}_{i \in I}$ uma família de R-submódulos de M. é fácil verificar que $N = \cap_{i \in I} N_i$ é um submóduo de M.*

Num primeiro curso de álgebra linear vemos que a união de subespaços não é, em geral, um espaço vetorial, pois esta não é fechada para a soma. O mesmo fenômeno ocorre no contexto de módulos. Assim, tal como no caso dos espaços vetoriais, nasce o conceito de submódulo gerado por um conjunto, para contornar este problema.

Definição 1.2.13. *Sejam R um anel, M um R-módulo à esquerda e $K \subseteq M$. Chamamos de submódulo de M gerado por K, e denotamos por $< K >$, ao menor submódulo de M que contém K.*

Do exemplo anterior, se $K \subseteq {}_RM$, então $< K >= \cap\{N \leq M : N \supseteq K\}$. Afirmamos que este último conjunto é igual ao conjunto $\mathcal{K} = \{\sum_{i=1}^{n} r_i x_i : n \in \mathbb{N}, r_i \in R \text{ e } x_i \in K, 1 \leq i \leq n\}$. De fato, pois segue facilmente que $\mathcal{K}$ é um R-submódulo de M que contém K, de onde decorre que $< K > \subseteq \mathcal{K}$. Por outro lado, todo submódulo de M que contém K deve conter todas as somas finitas de múltiplos escalares de elementos de K, de onde segue que $\mathcal{K} \subseteq < K >$.

Quando K é um subconjunto finito de M, digamos $K = \{x_1, x_2, ..., x_n\}$, vamos escrever $< x_1, x_2, ..., x_n >$, em lugar de $< \{x_1, x_2, ..., x_n\} >$, para denotar o submódulo de M gerado pelo conjunto $\{x_1, x_2, ..., x_n\}$. Os elementos $x_1, x_2, ..., x_n$ serão chamados de *geradores* do

submódulo $< K >$. Quando $K = \{y\}$ é um conjunto unitário, então diremos que $< y >$ é um *módulo cíclico.*

Mais ainda, dizemos que um módulo M é *finitamente gerado*, se existir um conjunto finito $\{m_1, m_2, ..., m_t\} \subseteq M$ tal que $M =< m_1, m_2, ..., m_t >$. Pela argumentação acima, se M é um R-módulo à esquerda e $m_1, m_2, ..., m_t \in M$, então segue que $< m_1, m_2, ..., m_t >= \{\sum_{i=1}^{t} r_i m_i : r_i \in R, 1 \leq i \leq t\}$, e neste caso, o módulo $< m_1, m_2, ..., m_t >$ será denotado por $\sum_{i=1}^{t} Rm_i$. Assim, o R-módulo à esquerda cíclico gerado por um elemento x será denotado por Rx. Vamos observar neste momento que se R é um anel e $x \in R$, então o submódulo cíclico do módulo regular à esquerda (resp. à direita) Rx (resp. xR) é chamado de *ideal principal à esquerda (resp. à direita) de* R.

Analogamente, se $\{N_i\}_{i \in I}$ é uma família de R-submódulos de um R-módulo à esquerda M, então o R-submódulo de M gerado por $\cup_{i \in I} N_i$ será denotado por $\sum_{i \in I} N_i$ e seus elementos serão somas finitas de elementos de N_i, quando i percorre o conjunto de índices I. Quando a família de submódulos for finita, escreveremos $N_1 + N_2 + \cdots + N_t$ em lugar daquela notação de somatório. Assim, se N e L são dois módulos, teremos que $N + L = \{x + y : x \in N, y \in L\}$ também é um módulo. Quando ocorrer que $N \cap L = 0$, diremos que o módulo soma $N + L$ é uma *soma direta* de N e L, e escreveremos $N \oplus L$. Mais geralmente, temos a seguinte definição.

Definição 1.2.14. *Seja M um R-módulo à esquerda e $\{M_i\}_{i \in I}$ uma família de submódulos de M. Então dizemos que M é a soma direta da família $\{M_i\}_{i \in I}$, e notamos por $M = \oplus_{i \in I} M_i$, se:*

(i) Todo elemento $m \in M$ pode ser escrito como uma soma $m = \sum_{i \in I} m_i$, com $m_i \in M_i$ e $m_i = 0$, exceto para um número finito de índices.

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

Uma outra caracterização de uma soma direta que pode ser bastante conveniente é dada no próximo exercício.

Exercício 1.2.15. *Sejam R um anel e M um R-módulo à esquerda. Mostre que $M = \oplus_{i \in I} M_i$ se, e somente se, todo elemento $m \in M$ pode ser escrito de modo único como uma soma finita $m = \sum_{i \in I} m_i$, com $m_i \in M_i$, onde $m_i = 0$, exceto para um número finito de índices.*

Esta última caracterização de soma direta nos permite introduzir o conceito de independência linear sobre o anel R. Se M é um R-módulo à esquerda, então dizemos que a família $\{m_i\}_{i \in I} \subseteq M$ é linearmente independente sobre R se a única maneira de escrever o elemento nulo de M como uma combinação linear finita de elementos desta família é tomando os coeficientes todos nulos em R, isto é, se sempre que $\sum_{j=1}^{k} r_j m_j = 0$, então $r_j = 0$

para todo $0 \leq j \leq k$. Pelo exercício acima, segue que a família $\{m_i\}_{i\in I}$ é linearmente independente sobre R se, e somente se, $\sum_{i\in I} Rm_i = \oplus_{i\in I} Rm_i$. Conjuntos geradores e linearmente independentes serão chamados de base de um R-módulo e um R-módulo que possui uma base será chamado de R-módulo livre. Mais precisamente, temos a seguinte definição.

Definição 1.2.16. *Seja L um R-módulo à esquerda. Dizemos que L é um R-módulo livre, se existir uma família $\{x_i\}_{i\in I} \subseteq L$ linearmente independente tal que $L \simeq \oplus_{i\in I} Rx_i$. Neste caso, uma tal família é dita uma R-base de L.*

Denotando por $R^{(I)}$ o R-módulo livre $\oplus_{i\in I} R_i$, onde $R_i = R$, então segue que um R-módulo à esquerda L é livre, se $L \simeq R^{(I)}$. Por simplicidade, se $I = \{i_1, i_2, ..., i_k\}$ é um conjunto finito, então escreveremos $R^{(k)}$ em lugar de $R^{(I)}$. A teoria de módulos livres se aproxima da teoria de espaços vetoriais, mas temos que ter um cuidado mesmo neste ponto, pois, por exemplo, a cardinalidade das bases de um espaço vetorial é um invariante do espaço vetorial, chamado de dimensão. No caso de módulos, é possível construir um módulo livre contendo bases com cardinalidades distintas, o que impede de generalizar o conceito de dimensão de módulos livres pela cardinalidade de uma de suas bases. Anéis para os quais todas as bases de módulos livres possuem a mesma cardinalidade são anéis que dizemos possuir a *propriedade da invariância de bases* e, para estes anéis, podemos introduzir o conceito de *dimensão* de um módulo livre pela cardinalidade de uma base qualquer. Este conceito recebe a denominação de *posto* do módulo livre. Por exemplo, anéis comutativos possuem a propriedade da invariância de bases. Uma demonstração deste resultado pode ser encontrada em [5] ou [8].

Antes de prosseguir, gostaríamos de dizer que nem todo módulo possui uma base, ou seja, existem módulos que não possuem bases. Um exemplo fácil de entender é o caso dos $\mathbb{Z}$-módulos do tipo $M = \mathbb{Z}/n\mathbb{Z}$. Para estes módulos não existe nenhuma família não vazia que seja linearmente independente sobre $\mathbb{Z}$, como é fácil verificar.

Vamos considerar agora as aplicações entre módulos que preservam esta estrutura.

Definição 1.2.17. *Sejam R um anel e M, N dois R-módulos à esquerda. Dizemos que uma função $f : M \to N$ é um homomorfismo de R-módulos (ou um R-homomorfismo), se:*

(i) $f(m_1 + m_2) = f(m_1) + f(m_2), \forall m_1, m_2 \in M$,

(ii) $f(rm) = rf(m), \forall r \in R, m \in M$.

Um R-homomorfismo $f : M \to M$ é dito um R-endomorfismo.

Decorre imediatamente da definição acima que se $\Bbbk$ é um anel de divisão, então os $\Bbbk$-homomorfismos são exatamente as transformações $\Bbbk$-lineares. Por conta disso, muitas vezes nos referimos a um R-homomorfismo como uma *aplicação R-linear*.

Exemplo 1.2.18. *Sejam R um anel e M, N dois R-módulos à esquerda. Claramente a aplicação nula $0 : M \to N$ dada por $0(m) = 0_N$ é um R-homomorfismo. Além disso, a aplicação identidade $id_M : M \to M$ também é um R-homomorfismo, como é facil verificar.*

Como no caso de anéis, se $f : M \to N$ é um homomorfismo de R-módulos à esquerda, então dizemos que f é um *monomorfismo* se f é injetor; dizemos que f é um *epimorfismo* se f é sobrejetor. Por fim, dizemos que f é um *isomorfismo* se f for bijetor. Podemos também considerar o núcleo de um R-homomorfismo $f : M \to N$ como sendo o conjunto

$$\mathcal{N}uc\, f := \{m \in M : f(m) = 0_N\}.$$

Como no caso de anéis, podemos enunciar os seguintes resultados. A demonstração será deixada como exercício ao leitor, por ser completamente análoga àquela feita antes.

Proposição 1.2.19. *Sejam R um anel, M e N dois R-módulos à esquerda e $f : M \to N$ um R-módulo. Então:*

(i) $f(0_M) = 0_N$,

(ii) $\mathcal{N}uc\, f$ *é um R-submódulo de M,*

(iii) f *é um monomorfismo se, e somente se,* $\mathcal{N}uc\, f = \{0\}$,

(iv) Se $M' \leq M$, *então* $f(M')$ *é um R-submódulo de N,*

(v) Se N' *é um R-submódulo de N, então* $f^{-1}(N')$ *é um R-submódulo de M.*

Sejam R um anel, M um R-módulo à esquerda e N um R-submódulo de M. É fácil verificar que a relação *"congruência módulo N"* define em M uma relação de equivalência, isto é, a relação definida por

$$\forall x, y \in M, x \equiv_N y \Leftrightarrow x - y \in N$$

é reflexiva, simétrica e transitiva. Vamos denotar a classe de equivalência de um elemento $m \in M$ por $\overline{m}$. Assim, $\overline{m} = m + N = \{m + x : x \in N\} \subseteq M$. Podemos então induzir, de modo natural, uma estrutura de R-módulo no conjunto quociente M/N, da seguinte forma:

$$\begin{array}{rccc} \cdot : & R \times M/N & \to & M/N \\ & (r, \overline{m}) & \mapsto & \overline{rm} \end{array}$$

Exemplo 1.2.20. *Sejam R um anel, M um R-módulo à esquerda e N um R-submódulo de M. Então a aplicação $\pi : M \to M/N$, dada por $\pi(m) = \overline{m}$ é um R-homomorfismo cujo núcleo é precisamente N. Chamamos este homomorfismo de projeção canônica em relação ao submódulo N.*

Neste contexto, podemos também enunciar um teorema de homomorfismos. Note que só foi usada a estrutura aditiva de um anel para mostrarmos o teorema dos homomorfismos para anéis. Isto permite usarmos a mesma argumentação de antes para mostrar o próximo resultado. Porém aqui vamos apresentar uma versão um pouco mais geral daquela feita antes no contexto de anéis.

Teorema 1.2.21. (Teorema dos homomorfismos) *Sejam R um anel e $f : M \to N$ um homomorfismo de R-módulos à esquerda e K um R-submódulo de M. Se $K \subseteq \mathcal{N}uc\, f$, então existe um R-homomorfismo $\overline{f} : M/K \to N$, unicamente determinado, tal que $f = \overline{f} \circ \pi$. Além disso, $\overline{f}$ é um monomorfismo se, e somente se, $K = \mathcal{N}uc\, f$.*

O seguinte corolário muitas vezes é enunciado como um segundo teorema de homomorfismos.

Corolário 1.2.22. *Sejam R um anel e M um R-módulo à esquerda. Se L e N são dois submódulos de M, então*

$$\frac{L}{L \cap N} \simeq \frac{L+N}{N}$$

Demonstração. Basta observar que a composição de homomorfismos $L \hookrightarrow L + N \twoheadrightarrow (L+N)/N$ é sobrejetor e seu núcleo é dado exatamente por $L \cap N$. O resultado então segue pelo Teorema dos Homomorfismos. □

Um fato importante neste ponto é a existência de uma correspondência biunívoca entre os submódulos de um módulo quociente M/N e os submódulos de M que contém N, dadas por

$$\{K \leq M : K \supseteq N\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{X : X \leq M/N\},$$

onde $\Phi(K) = \pi(K)$ e $\Psi(X) = \pi^{-1}(X)$, sendo $\pi : M \to M/N$ a projeção canônica.

Vamos incluir neste ponto do texto uma outra caracterização de somas diretas via sequências exatas, a qual será utilizada em uma argumentação que será feita mais adiante. Começamos com a definição de sequências de módulos e homomorfismos.

Definição 1.2.23. *Seja R um anel. Dados $\{M_i\}$ e $\{f_i : M_i \to M_{i+1}\}$, famílias de R-módulos à esquerda e R-homomorfismos, respectivamente, chamamos de uma sequência a todo diagrama do tipo*

$$\cdots \overset{f_{i-1}}{\to} M_i \overset{f_i}{\to} M_{i+1} \overset{f_{i+1}}{\to} \cdots$$

tal que $\mathcal{I}m\, f_i \subseteq \mathcal{N}uc\, f_{i+1}$*, para todo índice* i*. Uma sequência é dita exata em* M_i*, se ocorrer* $\mathcal{I}m\, f_i = \mathcal{N}uc\, f_{i+1}$*. Além disso, dizemos que uma sequência é exata, se ela é exata em todos os seus módulos. O número de* R*-homomorfismos no diagrama acima é dito o comprimento da sequência.*

Vejamos alguns exemplos claros.

Exemplo 1.2.24. *Sejam* R *um anel e* $f : N \to M$ *um homomorfismo de* R*-módulos à esquerda. Então:*

(i) A sequência $0 \to N \xrightarrow{f} M$ *é exata se, e somente se,* f *é um monomorfismo.*

(ii) A sequência $N \xrightarrow{f} M \to 0$ *é exata se, e somente se,* f *é um epimorfismo.*

(iii) A sequência $0 \to N \xrightarrow{f} M \to 0$ *é exata se, e somente se,* f *é um isomorfismo.*

No presente texto, estamos mais interessados nas chamadas sequências exatas curtas, que serão definidas a seguir.

Definição 1.2.25. *Uma sequência exata do tipo* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$*, é dita uma sequência exata curta.*

Exemplo 1.2.26. *Sejam* R *um anel,* M *um* R*-módulo à esquerda e* N *um* R*-submódulo de* M*. Então a sequência*

$$0 \to N \hookrightarrow M \xrightarrow{\pi} M/N \to 0,$$

onde π *é a projeção canônica, é claramente uma sequência exata curta.*

Num certo sentido, podemos pensar que toda sequência exata curta é desta forma. Mais precisamente, dada a sequência exata curta

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

segue que f é um monomorfismo e g é um epimorfismo. Assim, podemos pensar que A é um submódulo de B e que C é um módulo fator de B, a saber B/A, pois $\mathcal{I}m\, f = \mathcal{N}uc\, g$ e, consequentemente, temos $A \simeq \mathcal{I}m\, f \leq B$ e $C \simeq B/\mathcal{N}uc\, g = B/\mathcal{I}m\, f \simeq B/A$.

Vamos examinar agora a relação entre sequências exatas curtas e somas diretas. Começamos observando que se $M = N \oplus P$ como R-módulo à esquerda, então podemos definir as aplicações canônicas $\iota_N : N \to M$, dada por $\iota(n) = n + 0$ (inclusão canônica) e $\pi_P : M \to P$, dada por $\pi(n + p) = p$, para $n \in N$ e $p \in P$ (projeção canônica). Assim, vemos claramente que a sequência curta abaixo é exata:

$$0 \to N \xrightarrow{\iota} M \xrightarrow{\pi} P \to 0.$$

O próximo exemplo mostra que a recíproca deste fato não vale em geral.

Exemplo 1.2.27. *A sequência de $\mathbb{Z}$-módulos abaixo é exata*

$$0 \to 2\mathbb{Z} \hookrightarrow \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

mas, no entanto, $\mathbb{Z} \not\simeq 2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, como $\mathbb{Z}$-módulo.

Pode-se então questionar sob quais condições esta recíproca é verdadeira. O próximo resultado responde esta questão.

Proposição 1.2.28. *Sejam R um anel. Consideremos a sequência exata curta de R-módulos à esquerda*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0.$$

Então as seguintes afirmações são equivalentes:

(i) $M \simeq N \oplus P$*;*

(ii) Existe um R-homomorfismo $\psi : M \to N$, tal que $\psi \circ f = id_N$;

(iii) Existe um R-homomorfismo $\varphi : P \to M$, tal que $g \circ \varphi = Id_P$.

Demonstração. Vamos mostrar a equivalência $(i) \Leftrightarrow (ii)$. A equivalência $(i) \Leftrightarrow (iii)$ pode ser mostrada com uma argumentação semelhante e será deixada ao leitor.

$(i) \Rightarrow (ii)$ Como f é injetora, segue que $N \simeq \mathcal{I}m\, f$ e assim, $M \simeq N \oplus P \simeq \mathcal{I}m\, f \oplus P$. Desta forma, dado $m \in M$, temos $m = m_1 + m_2$, com $m_1 \in \mathcal{I}m\, f$ e $m_2 \in P$. Da injetividade de f segue que existe único $n \in N$ tal que $f(n) = m_1$. Definimos então $\psi : M \to N$, por $\psi(m) = n$. É fácil ver que ψ está bem definida e é um R-homomorfismo. Mais ainda, para todo $n \in N$, temos que $f(n)$ se escreve unicamente como $f(n) + 0 \in \mathcal{I}m\, f \oplus P$, de onde segue que

$$\psi \circ f(n) = \psi(f(n)) = \psi(f(n) + 0) = n = id_N(n)$$

como queríamos mostrar.

$(ii) \Rightarrow (i)$ Suponhamos que exista $\psi : M \to N$ tal que $\psi \circ f = id_N$. Afirmamos que neste caso, $M = \mathcal{I}m\, f \ \oplus \ \mathcal{N}uc\, \psi$. De fato, pois se $m \in M$, tomamos $x = f(\psi(m)) \in M$ e consideramos $y = m - x \in M$. Segue então que

$$\psi(y) = \psi(m - x) = \psi(m) - \psi(f(\psi(m))) = \psi(m) - \psi(m) = 0$$

ou seja, $y \in \mathcal{N}uc\, \psi$. Logo, $m = x + y \in \mathcal{I}m\, f + \mathcal{N}uc\, \psi$. Além disso, se $z \in \mathcal{I}m\, f \cap \mathcal{N}uc\, \psi$, segue que existe $n \in N$ tal que $f(n) = z$ e, consequentemente, $n = \psi \circ f(n) = \psi(z) = 0$, de onde decorre que $z = 0$. Portanto, $M = \mathcal{I}m\, f \oplus \mathcal{N}uc\, \psi$.

Como f é injetiva, temos que $N \simeq \mathcal{I}m\, f$. Resta mostrar agora que $P \simeq \mathcal{N}uc\, \psi$. De fato, basta observar que

$$P \simeq \frac{M}{\mathcal{N}uc\, g} = \frac{\mathcal{I}m\, f \oplus \mathcal{N}uc\, \psi}{\mathcal{I}m\, f} \simeq \mathcal{N}uc\, \psi.$$

□

Uma sequência exata curta que satisfaz (ii) (equivalentemente, que satisfaz (iii)) na Proposição acima é dita uma *sequência exata curta que cinde*. As aplicações ψ e φ acima são muitas vezes chamadas de *cisão* da sequência. Com esta nova nomenclatura, segue que $M \simeq N \oplus P$ se, e somente se, a sequência

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$$

cinde. Como uma aplicação do que fizemos acima, temos o seguinte resultado.

Um outro conceito importante na teoria de módulos, e que será usado mais adiante, é o conceito de bimódulo. Essencialmente, um bimódulo é um grupo abeliano que possui uma estrutura de módulo à esquerda sobre um anel e uma estrutura de módulo à direita sobre possivelmente outro anel, de modo que estas estruturas respeitam uma certa condição natural de compatibilidade. Mais precisamente, temos o seguinte conceito.

Definição 1.2.29. *Sejam R e S dois anéis e M um grupo abeliano. Dizemos que M é um (R, S)-bimódulo, se:*

(i) M é um R-módulo à esquerda e um S-módulo à direita.

(ii) Para todos $r \in R, s \in S$ e $m \in M$, vale que $(rm)s = r(ms)$.

Muitas vezes escrevemos ${}_RM_S$, para indicar que M é um (R, S)-bimódulo. Quando $R = S$, dizemos apenas que M é um R-bimódulo.

Exemplo 1.2.30. *Seja R um anel. A associatividade da multiplicação garante que os ideais bilaterais de R são exemplos naturais de R-bimódulos.*

Exemplo 1.2.31. *Sejam R um anel e M um R-módulo à esquerda. Consideremos $S = End_R(M)$, o anel dos R-endomorfismos de M. Afirmamos que M possui uma estrutura de (R, S)-bimódulo.*

De fato, para ver isto, basta definir uma ação de S à direita de M, por

$$m \blacktriangleleft f := (m)f$$

onde $m \in M$, $f \in S$ e o argumento de um operador R-linear está escrito à esquerda do operador, para facilitar a regra da composição de funções. Note que neste caso, se $m \in M$ e $f, g \in S$, então escrevemos $(m \blacktriangleleft f) \blacktriangleleft g = ((m)f)g = (m)f \circ g$, para indicar que aplicamos primeiro f e depois g, em analogia com o que se faz quando se escreve os argumentos à direita das funções: a primeira função a ser aplicada é aquela mais próxima do argumento.

Assim, é fácil verificar que M é de fato um S-módulo à direita. Além disso, temos

$$(r \cdot m) \blacktriangleleft f = (rm)f = r((mf)) = r \cdot (m \blacktriangleleft f)$$

e temos que M é um (R, S)-bimódulo.

Como uma aplicação dos bimódulos, podemos construir exemplos de anéis cujo reticulado de ideais à direita é completamente diferente do reticulado dos ideais à esquerda. Sejam R e S dois anéis e consideremos M um (R, S)-bimódulo. Usando operações matriciais, podemos definir um anel da forma

$$T \overset{not}{=} \begin{pmatrix} R & M \\ 0 & S \end{pmatrix} := \left\{ \begin{pmatrix} r & m \\ 0 & s \end{pmatrix} : r \in R, m \in M, s \in S \right\}$$

que é um anel com unidade $1_T = \begin{pmatrix} 1_R & 0 \\ 0 & 1_S \end{pmatrix}$. Se tomamos $I \lhd_l R$ e $J \lhd_r S$, então se verifica que

$$\begin{pmatrix} I & M \\ 0 & S \end{pmatrix} \lhd_l T \text{ e } \begin{pmatrix} R & M \\ 0 & J \end{pmatrix} \lhd_r T.$$

Além destes, é possível encontrar outros ideais tanto à esquerda como à direita de T, mas isto foge um pouco dos nossos propósitos. Portanto, a família de ideais à esquerda de T pode ter propriedades que a família de ideais à direita de T não as têm.

1.3 Produto tensorial

Num certo sentido, podemos pensar a soma direta de módulos como uma operação de soma de módulos. Queremos introduzir agora um módulo que simule uma operação de multiplicação. Isto será feito introduzindo a noção de produto tensorial de módulos. Para facilitar nosso entendimento, vamos primeiro tratar o caso de módulos sobre anéis comutativos e depois, estenderemos esta noção para o caso de anéis não comutativos. Primeiro, vamos fazer uma discussão menos formal para dar uma ideia do que estamos querendo definir e depois faremos uma definição formal do produto tensorial via uma propriedade universal. Discutiremos sua existência, unicidade e algumas de suas propriedades que

serão úteis no desenvolvimento deste texto.

Seja R um anel comutativo com unidade. Consideremos M e N dois R-módulos e sejam $\{m_i\}_{i\in I}$ e $\{n_j\}_{j\in J}$ duas famílias de geradores dos módulos M e N, respectivamente. Vamos definir o produto tensorial de M e N sobre R, como sendo o R-módulo $M \otimes_R N$ gerado por todos os símbolos $m_i \otimes n_j$, onde $i \in I, j \in J$, sujeito a algumas relações. Como estamos querendo simular uma multiplicação de módulos, ou seja, definir uma aplicação $M \times N \mapsto M \otimes_R N$ que possua as propriedades da multiplicação, precisamos exigir que valham as seguintes relações:

- $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \forall m_1, m_2 \in M, \forall n \in N,$
- $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \forall n_1, n_2 \in N, \forall m \in M,$
- $(r.m) \otimes n = r.(m \otimes n), \forall r \in R, \forall m \in M, \forall n \in N,$
- $m \otimes (r.n) = r.(m \otimes n), \forall r \in R, \forall m \in M, \forall n \in N.$

Examinemos inicialmente o caso particular de espaços vetoriais finito-dimensionais. Por simplicidade, consideremos U e V $\Bbbk$-espaços vetoriais de dimensão 2. Fixando $\{u_1, u_2\}$ e $\{v_1, v_2\}$ bases de U e V, respectivamente, obtemos que $U \otimes_\Bbbk V$ é o $\Bbbk$-espaço vetorial gerado por $\{u_1 \otimes v_1, u_1 \otimes v_2, u_2 \otimes v_1, u_2 \otimes v_2\}$. Vamos assumir que estes símbolos $u_i \otimes v_j$ são linearmente independentes sobre $\Bbbk$ (mais tarde veremos que isto sempre acontece), de modo que o conjunto $\{u_i \otimes v_j\}$ seja uma $\Bbbk$-base de $U \otimes_\Bbbk V$. Desta forma, $U \otimes_\Bbbk V$ é um $\Bbbk$-espaço vetorial de dimensão 4, cujos elementos são da forma $a_{11}u_1 \otimes v_1 + a_{12}u_1 \otimes v_2 + a_{21}u_2 \otimes v_1 + a_{22}u_2 \otimes v_2$.. Por exemplo, se $u = u_1 - u_2 \in U$ e $v = v_1 + 2v_2 \in V$, então o elemento $u \otimes v \in U \otimes_\Bbbk V$ pode ser escrito na base $\mathcal{B} := \{u_i \otimes v_j\}$ da forma

$$\begin{aligned} u \otimes v &= (u_1 - u_2) \otimes (v_1 + 2v_2) \\ &= u_1 \otimes v_1 + 2(u_1 \otimes v_2) - u_2 \otimes v_1 - 2(u_2 \otimes v_2) \end{aligned}$$

Para ver que a escolha de base não é importante aqui, suponhamos $\mathcal{B}' = \{v_1', v_2'\}$ uma base de V. Assim, $v_1' = \alpha_1 v_1 + \alpha_2 v_2$ e $v_2' = \beta_1 v_1 + \beta_2 v_2$. Portanto, a matriz

$$M = \begin{bmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{bmatrix}$$

é a matriz mudança de base, da base $\{v_1', v_2'\}$ para a base $\{v_1, v_2\}$, de onde segue que $\alpha_1\beta_2 - \beta_1\alpha_2 \neq 0$. Além disso,

$$M^{-1} = \frac{1}{\alpha_1\beta_2 - \beta_1\alpha_2} \begin{bmatrix} \beta_2 & -\beta_1 \\ -\alpha_2 & \alpha_1 \end{bmatrix}$$

é a matriz mudança de base, de base $\{v_1, v_2\}$ para a base $\{v_1', v_2'\}$.

Como as coordenadas de v na base $\{v_1', v_2'\}$ são dadas por

$$\frac{1}{\alpha_1\beta_2 - \beta_1\alpha_2}\begin{bmatrix} \beta_2 & -\beta_1 \\ -\alpha_2 & \alpha_1 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} \dfrac{\beta_2 - 2\beta_1}{det\, M} \\ \\ \dfrac{-\alpha_2 + 2\alpha_1}{\det\, M} \end{bmatrix}$$

onde $det\, M = \alpha_1\beta_2 - \beta_1\alpha_2$ é o determinante de M.

Dos cálculos acima segue que $u \otimes v$ pode ser escrito da forma

$$(u_1 - u_2) \otimes \left(\frac{\beta_2 - 2\beta_1}{det\, M}v_1' + \frac{-\alpha_2 + 2\alpha_1}{det\, M}v_1'\right)$$

ou seja,

$$\frac{\beta_2 - 2\beta_1}{\det\, M}(u_1 \otimes v_1') + \frac{-\alpha_2 + 2\alpha_1}{det\, M}(u_1 \otimes v_2') - \frac{\beta_2 - 2\beta_1}{det\, M}(u_2 \otimes v_1') - \frac{\alpha_2 + 2\alpha_1}{det\, M}(u_2 \otimes v_2')$$

Substituindo agora, nesta última expressão, v_1' e v_2' por suas escritas na base $\{v_1, v_2\}$, a saber, $v_1' = \alpha_1 v_1 + \alpha_2 v_2$ e $v_2' = \beta_1 v_1 + \beta_2 v_2$, reobtemos que

$$u \otimes v = (u_1 \otimes v_1) + 2(u_1 \otimes v_2) - (u_2 \otimes v_1) - 2(u_2 \otimes v_2)$$

mostrando que estes cálculos não dependem da escolha das bases dos espaços vetoriais.

No caso de R-módulos, não podemos fazer a definição de produto tensorial via bases, pois elas nem sempre existem. Vamos então definir o produto tensorial via uma propriedade universal. Para enunciarmos esta dita propriedade, vamos fazer uso das aplicações bilineares.

Definição 1.3.1. *Sejam R uma anel comutativo e M, N, L R-módulos. Uma aplicação $\varphi : M \times N \to L$ é dita bilinear, se φ é linear em cada variável, isto é,*

(i) $\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$ *e* $\varphi(r.m, n) = r.\varphi(m, n), \forall m, m_1, m_2 \in M, n \in N, r \in R$

(ii) $\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$ *e* $\varphi(m, r.n) = r.\varphi(m, n), \forall m \in M, n, n_1, n_2 \in N, r \in R$

Antes de prosseguir, vejamos alguns exemplos de aplicações bilineares.

Exemplo 1.3.2. (1) *A multiplicação em R, $m : R \times R \to R$ dada por $m(a, b) = ab$, é bilinear. Mais geralmente, a ação de R em um módulo M, $\cdot : R \times M \to M$ dada por $(r, m) \mapsto r \cdot m$, é bilinear.*

(2) *Se U e V são $\mathbb{R}$-espaços vetoriais, então o produto interno $<,>: U \times V \to \mathbb{R}$, dado por $(u,v) \mapsto < u, v >$ é bilinear.*

(3) *Se M, N, L e P são R-módulos, $\varphi : M \times N \to L$ é uma aplicação bilinear e $\phi : L \to P$ é uma aplicação linear (um R-homomorfismo de módulos), então a composta $\phi \circ \varphi : M \times N \to P$ é uma aplicação bilinear. Este exemplo será importante mais adiante e então vamos verificar esta afirmação. Sejam $m, m_1, m_2 \in M$, $n \in N$ e $r \in R$. Vamos mostrar que a composta $\phi \circ \varphi$ é linear na primeira variável. De fato, pois neste caso temos*

$$\begin{aligned} \phi \circ \varphi(m_1 + m_2, n) &= \phi(\varphi(m_1, n) + \varphi(m_2, n)) \\ &= \phi(\varphi(m_1, n)) + \phi(\varphi(m_2, n)) \\ &= \phi \circ \varphi(m_1, n) + \phi \circ \varphi(m_2, n) \end{aligned}$$

e

$$\begin{aligned} \phi \circ \varphi(r \cdot m, n) &= \phi(r \cdot \varphi(m, n)) \\ &= r \cdot (\phi(\varphi(m, n))) \\ &= r \cdot (\phi \circ \varphi(m, n)) \end{aligned}$$

A linearidade na segunda variável é mostrada de forma análoga.

A bilinearidade pode facilmente ser generalizada para a multilinearidade. Sejam $M_1, M_2, ..., M_k, N$ R-módulos. Dizemos que uma aplicação $\varphi : M_1 \times M_2 \times \cdots \times M_k \to N$ é multilinear, se φ é linear em cada variável. O determinante de uma matriz $n \times n$ é uma função multilinear de suas colunas, por exemplo.

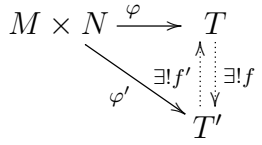
Num certo sentido, a bilinearidade traduz as propriedades que estamos procurando para definirmos nosso módulo que simularia a multiplicação de módulos. Note que o Exemplo 1.3.2(3) ensina como produzir novas aplicações bilineares a partir de uma conhecida. Vamos usar esta ideia para enunciar a propriedade universal do produto tensorial.

Propriedade Universal do Produto Tensorial. *Sejam M e N R-módulos. Definimos o produto tensorial de M e N sobre R como sendo um R-módulo T juntamente com uma aplicação bilinear $\varphi : M \times N \to T$ de modo que para toda aplicação bilinear $f : M \times N \to L$, onde L é um R-modulo qualquer, existe uma única aplicação linear $\phi : T \to L$ tal que $f = \phi \circ \varphi$.*

Vamos ver agora que esta propriedade define um R-módulo de forma única (a menos de isomorfismos). Começamos pela unicidade.

Unicidade do Produto Tensorial. Suponhamos que (T, φ) e (T', φ') são dois R-módulos munidos das respectivas aplicações bilineares satisfazendo a propriedade universal

acima, para os R-módulos M e N. Então devem existir únicas aplicações R-lineares $f : T \to T'$ e $f' : T' \to T$ tais que o diagrama abaixo comuta.



Da universalidade do par (T, φ), segue que $g \circ f = id_T$, uma vez que id_T satisfaz também a propriedade. Analogamente, da universalidade do par (T', φ') segue que $f \circ g = id_{T'}$. Portanto, devemos ter $T \simeq T'$ e, caso exista, uma solução da propriedade universal é unicamente determinada a menos de isomorfismos.

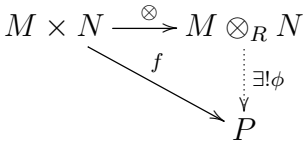
Existência do Produto Tensorial. Dados M e N dois R-módulos, vamos definir o produto tensorial de M e N sobre R como sendo o R-módulo $M \otimes_R N$ da seguinte forma: $M \otimes_R N$ é o R-módulo quociente $\dfrac{M \times N}{Q}$, onde Q é o R-submódulo de $M \times N = M \oplus N$ gerado por todos os elementos da forma $(m_1 + m_2, n) - (m_1, n) - (m_2, n), (m, n_1 + n_2) - (m, n_1) - (m, n_2), (r \cdot m, n) - r \cdot (m, n), (m, r \cdot n) - r \cdot (m, n), (r \cdot m, n) - (m, r \cdot n)$. Para facilitar a notação, vamos denotar a classe de um elemento $(m, n) \in M \times N$ no quociente $\dfrac{M \times N}{Q}$ por $m \otimes n$. Vamos mostrar agora que $(M \otimes_R N := \dfrac{M \times N}{Q}, \varphi)$, onde $\varphi : M \times N \to M \otimes N$ está definida por $\varphi(m, n) = m \otimes n$, satisfaz a propriedade universal desejada. A primeira coisa a observar neste sentido é que φ é de fato uma aplicação bilinear de $M \times N$ em $M \otimes N$ (exercício). Note que o quociente foi definido de tal forma que φ se torne uma aplicação bilinear.

Seja $f : M \times N \to P$ uma aplicação bilinear. Vamos definir $\phi : M \otimes_R N \to P$ da seguinte forma: dados $m \in M$ e $n \in N$, definimos $\phi(m \otimes n) = f(m, n)$. Para ver que ϕ está bem definida, basta verificar que $Q \subseteq \mathcal{N}uc\, f$, pelo Teorema de Homomorfismos. De fato, segue da bilinearidade de f que $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$, ou seja, $f((m_1 + m_2, n) - (m_1, n) - (m_2, n)) = 0$. Analogamente, mostramos que $f((m, n_1 + n_2) - (m, n_1) - (m, n_2)) = 0$, $f((r \cdot m, n) - r \cdot (m, n)) = 0$, $f((m, r \cdot n) - r \cdot (m, n)) = 0$ e $f((r \cdot m, n) - (m, r \cdot n)) = 0$, mostrando que $D \subseteq \mathcal{N}uc\, f$, como queríamos.

A linearidade de ϕ segue imediatamente da bilinearidade de f, pois $\phi(r \cdot (m \otimes n) + (m' \otimes n') = f(r \cdot (m, n) + (m', n')) = r \cdot f(m, n) + f(m', n') = r \cdot \phi(m \otimes n) + \phi(m' \otimes n')$, para todos $r \in R$, $m, m' \in M$ e $n, n' \in N$. Por construção, temos que $f = \phi \circ \varphi$. Falta, portanto, mostrar que ϕ está unicamente determinada.

Suponhamos que $g : M \otimes_R N \to P$ seja uma aplicação R-linear tal que $f = g \circ \varphi$. Mas então devemos ter $g(m \otimes n) = g(\varphi(m, n)) = f(m, n) = \phi(m \otimes n)$. Como g e ϕ coincidem sobre todos os geradores de $M \otimes_R N$, segue que estas aplicações coincidem em todo o R-módulo $M \otimes_R N$, ou seja, temos $g = \phi$.

Se denotarmos o conjunto de todas as aplicações R-bilineares de $M \times N$ em P por $\mathcal{B}il_R(M \times N, P)$, então o diagrama comutativo



nos diz que existe uma correspondência biunívoca entre os conjuntos $\mathcal{B}il_R(M \times N, P)$ e $Hom_R(M \otimes_R N, P)$. Num certo sentido, isto nos diz que o produto tensorial de M e N sobre R representa as aplicações bilineares de $M \times N$.

Antes de vermos alguns exemplos, vamos fazer algumas observações sobre os elementos de um produto tensorial, que podem ser deduzidos a partir da propriedade universal do produto tensorial.

- Se $x \in M \otimes_R N$, então x é uma soma finita da forma $m_1 \otimes n_1 + m_2 \otimes n_2 + \cdots \otimes m_k \otimes n_k$. De fato, pois segue da definição de produto tensorial que seus elementos são gerados por elementos da forma $r \cdot (m \otimes n)$, com $r \in R$, $m \in M$ e $n \in N$. Como $r \cdot (m \otimes n) = (r \cdot m) \otimes n$ e $r \cdot m \in M$, a fórmula acima fica clara. Os elementos da forma $m \otimes n$ são muitas vezes chamados de *tensores básicos*.

- Se M é um R-módulo gerado por $\{m_i\}_{i \in I}$ e N é um R-módulo gerado por $\{n_j\}_{j \in J}$, então o produto tensorial $M \otimes_R N$ é um R-módulo gerado por $\{m_i \otimes n_j\}_{(i,j) \in I \times J}$. De fato, pois se $m \in M$ e $n \in N$, então temos que $m \sum_{i=1}^{k} \alpha_i m_i$ e $n = \sum_{j=1}^{l} \beta_j n_j$. Assim, $m \otimes n = \left(\sum_{i=1}^{k} \alpha_i m_i\right) \otimes \left(\sum_{j=1}^{l} \beta_j n_j\right)$. Usando a bilinearidade de $\otimes$, obtemos que $m \otimes n = \sum_{i,j} \alpha_i \beta_j (m_i \otimes n_j)$. Como todo elemento de $M \otimes_R N$ é uma soma finita de tensores básicos, segue que $M \otimes_R N$ é gerado por $\{m_i \otimes n_j\}_{(i,j) \in I \times J}$.

- Em $M \otimes_R N$, temos que $m \otimes 0 = 0$ e $0 \otimes n = 0$. De fato, isto decorre do fato que para toda aplicação bilinear b definida em $M \times N$, temos $b(m, 0) = 0 = b(0, n)$.

- Um tensor básico $m \otimes n$ é nulo em $M \otimes_R N$ se, e somente se, toda aplicação bilinear definida em $M \times N$ se anula em (m, n). Assim, não é fácil mostrarmos que um elemento de um produto tensorial é nulo. Por outro lado, se queremos mostrar que um determinado elemento da forma $m \otimes n$ de $M \otimes_R N$ não é nulo, basta encontrarmos um R-módulo P e uma aplicação bilinear $b : M \times N \to P$ tal que $b(m, n) \neq 0$.

- Seguindo a ideia anterior, o produto tensorial $M \otimes_R N$ é o R-módulo nulo se, e somente se, toda aplicação bilinear de $M \times N$ em qualquer R-módulo P é nula. Veremos exemplos de uma tal situação adiante.

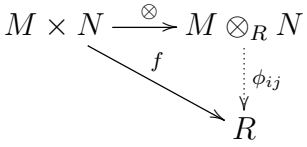
- Sejam $x, y \in M \otimes_R N$. Assim, devemos ter $x = \sum_{i=1}^{k} m_i \otimes n_i$ e $y = \sum_{j=1}^{l} m'_j \otimes n'_J$. Então, $x = y$ se, e somente se, $\sum_{i=1}^{k} b(m_i, n_i) = \sum_{j=1}^{l} b(m_j, n_j)$, para toda

a aplicação bilinear b definida em $M \times N$. Portanto, $x = 0$ se, e somente se, $\sum_{i=1}^{k} b(m,n) = 0$ para toda a aplicação bilinear definida em $M \times N$.

As observações acima nos dão uma ideia de que trabalhar com elementos de um produto tensorial é um tanto complicado. Por este motivo, as principais propriedades do produto tensorial são mostradas a partir de sua propriedade universal, como veremos adiante.

Vejamos agora alguns exemplos de produto tensorial.

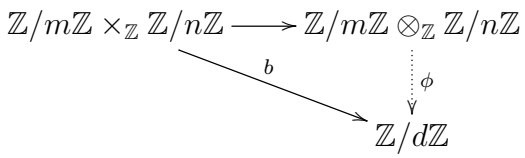
Exemplo 1.3.3. (1) *Sejam M um R-módulo livre com base $\{e_i\}_{i\in I}$ e N um R-módulo livre com base $\{f_j\}_{j\in J}$. Então o produto tensorial $M \otimes_R N$ é o R-módulo livre com base $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$. Se M ou N é o módulo nulo, então o resultado é trivial. Suponhamos então que ambos M e N são R-módulos livres não nulos. Consideremos $\{e_i\}$ uma base de M e $\{f_j\}$ uma base de N. Já sabemos que o produto tensorial é gerado pela família $\{e_i \otimes f_j\}$. Vamos mstrar agora que esta família é linearmente independente sobre R. Consideremos então uma combinação linear finita nula $\sum_{i,j} r_{ij}(e_i \otimes f_j) = 0$. Fixemos $i \in I$ e $j \in J$ tais que $r_{ij} \neq 0$ e consideremos a aplicação bilinear $b_{ij} : M \times N \to R$ definida por $b_{ij}(m,n) = \alpha_i \beta j$, onde $m = \sum_k \alpha_k e_k \in M$ e $N = \sum_l \beta_l f_l$. Da propriedade universal do produto tensorial segue que existe única aplicação linear $\phi : M \otimes_R N \to R$ dada por $\phi(m \otimes n) = b_{ij}(m,n)$, fazendo o diagrama abaixo comutar*



Assim, temos $\phi_{ij}(e_i \otimes f_j) = 1$ e $\phi_{ij}(e_k \otimes f_l) = 0$, sempre que $(k,l) \neq (i,j)$. Mas então devemos ter $0 = \phi_{ij}(\sum_{k,l} r_{kl}(e_K \otimes f_l)) = r_{ij}$, uma contradição. Esta contradição implica que a família $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$ é linearmente independente sobre R.

(2) *Sejam $m, n \in \mathbb{Z}$. Então $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$, como grupos abelianos ou, equivalentemente, como $\mathbb{Z}$-módulos, onde $d = mdc(m,n)$. De fato, pois temos que $\overline{1} \otimes \overline{1}$ gera o grupo abeliano $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$. Portanto, como $m(\overline{1} \otimes \overline{1}) = m\overline{1} \otimes \overline{1} = 0 \otimes \overline{1} = 0$ e $n(\overline{1} \otimes \overline{1}) = \overline{1} \otimes n\overline{1} = \overline{1} \otimes 0 = 0$, segue que a ordem do grupo abeliano $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ divide m e n, isto é, a ordem de $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ divide d, ou seja, $\#(\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \leq d$. Para ver a desigualdade no outro sentido, basta considerar a aplicação bilinear $b : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ dada por $b(x \pmod m, y \pmod n) = xy \pmod d$. A propriedade universal do produto tensorial vai garantir que existe única aplicação $\mathbb{Z}$-linear $\phi : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to$*

$\mathbb{Z}/d\mathbb{Z}$ *que faz o diagrama abaixo comutar*



Neste caso, temos $\phi(x \otimes y) = xy$. *Dado* $z \pmod d \in \mathbb{Z}/d\mathbb{Z}$, *segue que* $z = \phi(z \pmod m \otimes 1)$, *ou seja,* ϕ *é sobrejetora, de onde se conclui que* $\#(\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}) \geq d$. *Portanto, o grupo abeliano* $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ *é um grupo cíclico (gerado por* $\overline{1} \otimes \overline{1}$*) com ordem* d, *ou seja,* $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$, *como afirmado antes.*

(3) *Como um subexemplo do caso anterior, segue que* $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/5\mathbb{Z} = 0$, *pois* $mdc(3,5) = 1$. *Note que isto implica que não existe nenhuma aplicação* $\mathbb{Z}$*-bilinear não nula definida de* $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/5\mathbb{Z}$ *em qualquer grupo abeliano. Isto pode ser mostrado diretamente, pois se* $b : \mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/5\mathbb{Z} \to G$ *é uma aplicação bilinear, onde* G *é um grupo abeliano qualquer, então temos* $3b(x,y) = b(3x,y) = b(0,y) = 0$ *e* $5b(x,y) = b(x,5y) = b(x,0) = 0$. *Da bilinearidade de* b *segue que se* $x, y \in 3\mathbb{Z}+5\mathbb{Z} = \mathbb{Z}$ *então* $b(x \pmod 3, y \pmod 5) = 0$, *ou seja,* b *é identicamente nula. O mesmo argumento pode ser repetido no caso em que* $mdc(m,n) = 1$.

Vamos agora discutir algumas das propriedades do produto tensorial que nos serão úteis mais a frente. Todas as propriedades abaixo são obtidas como uma consequência direta da propriedade universal do produto tensorial.

Proposição 1.3.4. *Sejam* R *um anel comutativo,* M, N *e* K R*-módulos. Então:*

(i) $M \otimes_R R \simeq M$,

(ii) $M \otimes_R N \simeq N \otimes_R M$,

(iii) $(M \otimes_R N) \otimes_R K \simeq M \otimes_R (N \otimes_R K)$,

(iv) $M \otimes_R (N \oplus K) \simeq (M \otimes_R N) \oplus (M \otimes_R K)$.

Demonstração. Sabemos que a ação $f : M \times R \to M$ é uma aplicação bilinear. Portanto, a propriedade universal do produto tensorial garante que existe uma unica aplicação R-linear $\overline{f} : M \otimes_R R \to M$ dada por $\overline{f}(m \otimes r) = m \cdot r$. Se $m \otimes r \in \mathcal{N}uc\, \overline{f}$, então $m \cdot r = 0$ e segue que $0 = (m \cdot r) \otimes 1_R = m \otimes r$, e $\overline{f}$ é injetora. Claramente, $\overline{f}$ é sobrejetora, pois se $m \in M$, então $m = m \cdot 1_R = \overline{f}(m \otimes 1_R)$. Isto mostra (i).

Considere agora a aplicação $g : M \times N \to N \otimes M$ definida por $g(m,n) = n \otimes m$. É fácil verificar que g é uma aplicação R-bilinear de $M \times N$ em $N \otimes M$. A propriedade universal do produto tensorial então garante que existe uma única aplicação linear $\overline{g} : M \otimes N \to N \otimes M$,

tal que $\overline{g}(m \otimes n) = n \otimes m$. De modo análogo, se mostra que existe uma única aplicação R-linear $\overline{h} : N \otimes M \to M \otimes N$ tal que $\overline{h}(n \otimes m) = m \otimes n$. Agora basta observar que $\overline{g}$ e $\overline{h}$ assim definidas são a inversa uma da outra para obter (ii).

Para mostrar (iii), começamos definindo a aplicação $f : M \times N \times K \to M \otimes (N \otimes K)$ definida por $(m, n, k) \overset{f}{\mapsto} m \otimes (n \otimes K)$, a qual é trilinear. Assim, para cada $k \in K$, fica definida uma aplicação bilinear $f_k : M \times N \to M \otimes (N \otimes K)$ dada por $f_k(m, n) = m \otimes (n \otimes k)$. Aplicando a propriedade universal do produto tensorial para esta última aplicação, obtemos que existe uma única aplicação R-linear $\overline{f_k} : M \otimes N \to M \otimes (N \otimes K)$ dada por $\overline{f_k}(m \otimes n) = m \otimes (n \otimes k)$, para cada $k \in K$. Agora consideremos a aplicação $g : (M \otimes N) \times K \to M \otimes (N \otimes K)$, dada por $g((m \otimes n)), k) := \overline{f_k}(m \otimes n)$. Assim, g é linear na primeira variável, pois $\overline{f_k}$ o é. Vamos ver que g também é linear na segunda variável. De fato, pois se fixamos $x \in M \otimes N$, digamos $x = \sum_i m_i \otimes n_i$ (uma soma finita) e $k, k' \in K$, então temos

$$\begin{aligned} g(x, k + k') &= \overline{f_{k+k'}}(\sum_i m_i \otimes n_i) = \sum_i \overline{f_{k+k'}}(m_i \otimes n_i) \\ &= \sum_i (m_i \otimes n_i) \otimes (k + k') = \sum_i ((m_i \otimes n_i) \otimes k + (m_i \otimes n_i) \otimes k') \\ &= \sum_i \overline{f_k}(m_i \otimes n_i) + \overline{f_{k'}}(m_i \otimes n_i) = \overline{f_k}(\sum_i m_i \otimes n_i) + \overline{f_{k'}}(\sum_i m_i \otimes n_i) \\ &= g(x, k) + g(x, k') \end{aligned}$$

Além disso, se $r \in R$, então

$$\begin{aligned} g(x, r \cdot k) &= \overline{f_{r \cdot k}} \left(\sum_i m_i \otimes n_i \right) = \sum_i (m_i \otimes n_i) \otimes r \cdot k \\ &= r \cdot \left(\sum_i (m_i \otimes n_i) \otimes k \right) = r \cdot \overline{f_k}(x) \\ &= r \cdot g(x, k) \end{aligned}$$

Assim, aplicando a propriedade universal do produto tensorial, obtemos que existe uma única aplicação R-linear $\overline{g} : (M \otimes N) \otimes K \to M \otimes (N \otimes K)$ tal que $\overline{g}((m \otimes n) \otimes k) = m \otimes (n \otimes k)$. De modo completamente análogo se mostra que existe uma única aplicação R-linear $\overline{h} : M \otimes (N \otimes K) \to (M \otimes N) \otimes K$ tal que $\overline{h}(m \otimes (n \otimes k)) = (m \otimes n) \otimes k$. Portanto, para obter o resultado desejado, basta verificar que $\overline{g}$ e $\overline{h}$ assim definidas são inversas uma da outra.

Para finalizar nossa prova, falta mostrar (iv), o qual será deixado como exercício para o leitor. □

Note que na demonstração de (iii) da Proposição acima precisamos trabalhar com

várias aplicações bilineares, diferente do que ocorreu em (i) ou (ii). Este fato ocorre porque um tensor básico de $(M \otimes N) \otimes K$ não é da forma $(m \otimes n) \otimes k$, com $m \in M, n \in N$ e $k \in K$. De fato, tensores elementares de $(M \otimes N) \otimes K$ são da forma $x \otimes k$, com $x \in M \otimes N$ e $k \in K$. Agora observe que x não precisa ser da forma $x = m \otimes n$. Então, não podemos simplificar o argumento, construindo uma função linear apenas nos tensores básicos da forma $(m \otimes n) \otimes k$ e depois estender por linearidade.

O isomorfismo $\tau : M \otimes N \simeq N \otimes M$ dado por $\tau(m \otimes n) = n \otimes m$ construido em (ii) da Proposição acima será chamado de *morfismo twist* ou *morfismo flip* no decorrer do texto.

O produto tensorial também pode ser definido para morfismos, como mostra o próximo resultado.

Proposição 1.3.5. *Sejam R um anel comutativo, $f : M \to M'$, $g : N \to N'$ R-homomorfismos. Então $f \otimes g : M \otimes_R N \to M' \otimes_R N'$, definida por $f \otimes g(m \otimes n) = f(m) \otimes g(n)$, e estendida por distributividade, está bem definida e é um R-homomorfismo de módulos.*

Demonstração. De fato, basta observar que a aplicação $f \times g : M \times N \to M' \otimes_R N'$ definida por $(f \times g)(m, n) := f(m) \otimes g(n)$ é uma aplicação R-bilinear. A propriedade universal do produto tensorial vai então garantir que $f \times g$ induz uma aplicação R-linear $f \otimes g : m \otimes n \mapsto f(m) \otimes g(n)$. □

Usando aplicações multilineares em lugar de bilineares, podemos repetir nossa construção e definir o produto tensorial $\otimes_{i \in I} M_i$ de uma família de R-módulos $\{M_i\}_{i \in I}$. A ausência de parenteses na escrita $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ se dá pela associatividade do produto tensorial.

Para o caso geral, onde consideramos R um anel não necessariamente comutativo, precisamos fazer alguns ajustes necessários, pois se quisermos trabalhar com aplicações bilineares, teremos uma inconsistência com a não comutatividade de R. Mais precisamente, seja b uma aplicação bilinear definida em $M \times N$, $r, s \in R$, $m \in M$ e $n \in N$, então deveríamos ter $(rs) \cdot b(m, n) = r \cdot (s \cdot b(m, n)) = s \cdot b(r \cdot m, n) = b(r \cdot m, s \cdot n) = r \cdot (b(m, s \cdot n)) = s \cdot (r \cdot (b(m, n))) = (sr) \cdot b(m, n)$. Como tanto a forma bilinear quanto os R-módulos e os elementos neste argumento acima são tomados arbitrários, isto implicaria que $rs = sr$ em R, contrariando a não comutatividade de R. Então precisamos considerar uma forma mais fraca de bilinearidade nesta situação.

Definição 1.3.6. *Sejam R um anel, M um R-módulo à direita e N um R-módulo à esquerda. Dizemos que uma aplicação $\varphi : M \times N$ é R-balanceada, se:*

(i) $\varphi(m_1 + m_2, n) = \varphi(m_1, n) + \varphi(m_2, n)$,

(ii) $\varphi(m, n_1 + n_2) = \varphi(m, n_1) + \varphi(m, n_2)$,

(iii) $\varphi(mr, n) = \varphi(m, rn)$.

Agora, trabalhando com aplicações R-balanceadas em lugar de aplicações R-bilineares e considerando Q o subgrupo do grupo abeliano $M \times N \simeq M \oplus N$, gerado por todos os elementos da forma $(m_1 + m_2, n) - (m_1, n) - (m_2, n), (m, n_1 + n_2) - (m, n_1) - (m, n_2)$ e $(mr, n) - (m, rn)$, podemos repetir toda construção feita acima para obter o produto tensorial de M e N sobre R, onde M é um R-módulo à direita e N é um R-módulo à esquerda. Esta construção produz $M \otimes_R N := \dfrac{M \times N}{Q}$ como um grupo abeliano. Para que $M \otimes_R N$ se torne um módulo é preciso trabalhar com M ou N sendo um bimódulo. Assim, se R e S são dois anéis, M é um (S, R)-bimódulo e N é um R-módulo à esquerda, então o grupo abeliano $M \otimes_R N$ se torna um S-bimódulo à esquerda via a ação $s \cdot (m \otimes n) = (s \cdot m) \otimes n$, como é fácil verificar. De modo análogo, se N é um (R, S)-bimódulo e M é um R-módulo à direita, então o grupo abeliano $M \otimes_R N$ se torna um S-módulo à direita via a ação $(m \otimes n) \cdot s = m \otimes (n \cdot s)$.

Neste contexto mais geral também podemos mostrar um resultado análogo ao obtido na Proposição 1.3.4, cuja demonstração é praticamente a mesma de antes, tomando-se aplicações balanceadas em lugar das bilineares. Para registro e futuras referências, vamos enunciá-lo aqui.

Proposição 1.3.7. *Sejam R, S um anéis, M, N e K R-módulos ou S-módulos, de acordo com a necessidade. Então:*

(i) $M \otimes_R R \simeq M$,

(ii) $M \otimes_R N \simeq N \otimes_R M$,

(iii) $(M \otimes_R N) \otimes_S K \simeq M \otimes_R (N \otimes_S K)$,

(iv) $M \otimes_R (N \oplus K) \simeq (M \otimes_R N) \oplus (M \otimes_R K)$.

Para os propósitos deste texto, o produto tensorial será considerado quase que sempre entre espaços vetoriais. Vamos então discutir um pouco este tipo de produto tensorial.

Definição 1.3.8. *Sejam U e V espaços vetoriais sobre um corpo $\Bbbk$ e $x \in U \otimes_\Bbbk V$. Se $x = 0$, então definimos o posto de x como sendo $\text{posto}\, x = 0$. Se $x \neq 0$, então definimos o posto de x como sendo $\text{posto}\, x = r$, onde r é o menor inteiro positivo tal que $x = \sum_{i=1}^{r} u_i \otimes v_i \in U \otimes_\Bbbk V$.*

O próximo resultado nos diz como calcular o posto de um elemento em um produto tensorial.

Proposição 1.3.9. *Sejam U e V $\Bbbk$-espaços vetoriais e $0 \neq x = \sum_{i=1}^{r} u_i \otimes v_i \in U \otimes_{\Bbbk} V$. Então as seguintes afirmações são equivalentes:*

(i) $r = posto\, x$.

(ii) Os conjuntos $\{u_i\}$ *e* $\{v_i\}$ *são linearmente independentes sobre* $\Bbbk$.

Demonstração. $(i) \Rightarrow (ii)$ Seja $r = posto\, x$. Se $\{u_1, ..., u_r\}$ é linearmente dependente sobre $\Bbbk$, então $r > 1$ e existe um vetor u_j que pode ser escrito como uma combinação linear dos demais. Sem perda de generalidade, podemos assumir que $j = r$. Escrevendo $u_r = \sum_{i=1}^{r-1} \alpha_i u_i$, obtemos que

$$\begin{aligned} x &= \sum_{i=1}^{r} u_i \otimes v_i \\ &= \sum_{i=1}^{r-1} u_i \otimes v_i + \sum_{i=1}^{r-1} (\alpha_i u_i) \otimes v_r \\ &= \sum_{i=1}^{r-1} u_i \otimes (v_i + \alpha_i v_r) \end{aligned}$$

o que contraria a minimalidade de r. Portanto, $\{u_i\}$ é linearmente independente sobre $\Bbbk$. Analogamente, mostramos que $\{v_i\}$ é linearmente independente sobre $\Bbbk$.

$(ii) \Rightarrow (i)$ Suponhamos que os conjuntos $\{u_i\}$ e $\{v_i\}$ são linearmente independente sobre $\Bbbk$ e seja $r' = posto\, x$. Assim, devemos ter $x = \sum_{j=1}^{r'} u'_j \otimes v'_j \in U \otimes_{\Bbbk} V$ com $r' \leq r$. Fixamos agora $k \in \{1, 2, ..., r\}$. Da independência linear do conjunto $\{u_i\}$, segue que existe um funcional linear $f \in U^*$ tal que $f(u_k) = 1$ e $f(u_j) = 0$, se $j \neq k$. Aplicando então $f \otimes id_V$ em x, usando ambas as representações de x, obtemos

$$(f \otimes id_V)(\sum_{i=1}^{r} u_i \otimes v_i) = (f \otimes id_V)(x) = (f \otimes id_V)(\sum_{j=1}^{r'} u'_j \otimes v'_j)$$

ou seja,

$$v_k = f(u'_j)v'_j \in \mathcal{G}er\,\{v'_1, v'_2, ..., v'_{r'}\}$$

e, portanto, temos $r \leq r'$, pois $\{v_1, v_2, ..., v_r\}$ é linearmente independente por hipótese (lembre que todo subconjunto com mais de r' vetores em $W := \{\mathcal{G}er\,\{v'_1, v'_2, ..., v'_{r'}\}$ é linearmente dependente sobre $\Bbbk$). Portanto, $r = r'$ e a demonstração está finalizada. □

Este resultado tem a seguinte consequência importante.

Corolário 1.3.10. *Sejam U e V espaços vetoriais sobre um corpo $\Bbbk$. Então a aplicação $\Bbbk$-linear $\varphi : U^* \otimes_{\Bbbk} V \to Hom_{\Bbbk}(U, V)$ definida por $\varphi(f \otimes v) = f_v : u \mapsto f(u)v$, para todo $f \in U^*, v \in V$ e $u \in U$, e estendido por linearidade, é injetora.*

Demonstração. Consideremos $x \in U^* \otimes_{\Bbbk} V$ um elemento não nulo. Então podemos escrever $x = \sum_{i=1}^{r} f_i \otimes v_i$, onde $r = posto\, x$. Suponhamos por contradição que $\varphi(x) = 0 \in Hom_{\Bbbk}(U, V)$. Como o conjunto $\{v_1, ..., v_r\}$ é linearmente independente, segue que dado $u \in U$, temos

$$0 = \varphi(x) = \sum_{i=1}^{r} f_i(u) v_i$$

de onde segue que $f_i(u) = 0$, para todo $1 \leq i \leq r$. Como $u \in U$ foi tomado arbitrário, obtemos que f_i é a aplicação nula, para todo $1 \leq i \leq r$, de onde segue que $x = 0$. Esta contradição nos diz que $\mathcal{N}uc\, \varphi = \{0\}$, ou seja, φ é injetora. □

Podemos dizer mais sobre a aplicação φ dada acima. Lembremos que se $f : U \to V$ é uma aplicação $\Bbbk$-linear, então definimos o *posto de* f como sendo a dimensão da imagem de f em V, ou seja, $posto\, f = dim_{\Bbbk} \mathcal{I}m\, f$. Mantendo as hipóteses e notações da Corolário acima, podemos mostrar que se $x \in U^* \otimes_{\Bbbk} V$ é um elemento de posto r, então $posto\, \varphi(x) = r$. De fato, pois neste caso, podemos escrever $x = \sum_{i=1}^{r} f_i \otimes v_i$, onde $\{f_i\}$ e $\{v_i\}$ são conjuntos linearmente independentes. Como $\varphi(x) = \sum_{i=1}^{r} f_i(x) v_i$, segue que $\mathcal{I}m\, \varphi(x) \in \mathcal{G}er\, \{v_1, v_2, ..., v_r\} \subseteq V$. Logo, $posto\, \varphi(x) = s \leq r$. Seja $\mathcal{B}_x := \{w_1, w_2, ..., w_s\}$ uma base de $\mathcal{I}m\, \varphi(x)$. Da álgebra linear segue que existem funcionais lineares $g_1, g_2, ..., g_s \in U^*$ tais que para todo $u \in U$, temos $\varphi(x)(u) = \sum_{i=1}^{s} g_i(u) w_i$. A injetividade de φ nos diz então que $x = \sum_{i=1}^{s} g_i \otimes w_s \in U^* \otimes_{\Bbbk} V$. Como esta é uma representação de x como soma de tensores básicos de $U^* \otimes_{\Bbbk} V$, segue que $r \leq s$ e, portanto, $s = posto\, \varphi(x) = r$, como queríamos mostrar.

Denotando por $Hom_{fin}(U, V)$ o subespaço de $Hom_{\Bbbk}(U, V)$ de todas as aplicações lineares de U em V que possuem posto finito, segue que φ definida no Corolário acima induz uma aplicação $\Bbbk$ linear $\varphi' : U^* \otimes_{\Bbbk} V \to Hom_{fin}(U, V)$, pois se $g \in \mathcal{I}m\, \varphi$, então existe $x \in U^* \otimes_{\Bbbk} V$ tal que $g = \varphi(x)$. Pela argumentação acima, se $r = posto\, x$, então $r = posto\, g$ e segue que $g \in Hom_{fin}(U, V)$. Mais ainda, φ' é um isomorfismo linear. De fato, pois se $f \in Hom_{fin}(U, V)$, digamos $posto\, f = n$, tomamos $\{v_1, v_2, ..., v_n\} \subseteq V$ uma base de $\mathcal{I}m\, f$. Assim, se $\{u_j\}$ é uma base de U, então devemos ter $f(u_j) = \sum_i \alpha_{ji} v_i$. Portanto, definindo funcionais lineares em U^* por $f_i(u_j) = \alpha_{ji}$ e $f_i(u_k) = 0$, se $k \neq j$, teremos que $y = \sum_{i=1}^{n} f_i \otimes v_i \in U^* \otimes_{\Bbbk} V$ e segue que

$$\varphi'(y)(u_j) = \sum_{i=1}^{n} f_i(u_j) v_i = \sum_{i=1}^{n} \alpha_1 j i v_i = f(u_j)$$

ou seja, $f = \varphi'(y)$, pois estas duas aplicações coincidem em todos os vetores de uma base de U.

Podemos resumir o que foi discutido acima num único resultado.

Proposição 1.3.11. *Sejam U e V espaços vetoriais sobre um corpo $\Bbbk$. Consideremos a*

aplicação $\Bbbk$*-linear* $\varphi : U^* \otimes_{\Bbbk} V \to Hom_{\Bbbk}(U,V)$ *definida por* $\varphi(f \otimes v) = f_v : u \mapsto f(u)v$, *para todo* $f \in U^*, v \in V$ *e* $u \in U$. *Então:*

(i) φ *é uma aplicação injetora.*

(ii) φ *é um isomorfismo linear se, e somente se,* $dim_{\Bbbk}U < \infty$ *ou* $dim_{\Bbbk}V < \infty$.

Demonstração. Mantendo as notações da discussão acima, para mostrar (ii), basta observar que $dim_{\Bbbk}U < \infty$ ou $dim_{\Bbbk}V < \infty$ implicam que $Hom_{\Bbbk}(U,V) = Hom_{fin}(U,V)$ e, consequentemente, $\varphi = \varphi'$. A recíproca é clara. □

O produto tensorial, em teoria de categorias, representa um funtor cujo adjunto é dado pelo funtor Hom. Não queremos nos aprofundar neste assunto, mas esta relação de adjunção pode ser traduzida a nível de espaços vetoriais pela seguinte propriedade importante.

Lema 1.3.12. *Sejam* U, V *e* W *espaços vetoriais sobre um corpo* $\Bbbk$. *Então existe um isomorfismo linear entre* $Hom_{\Bbbk}(U \otimes_{\Bbbk} V, W)$ *e* $Hom_{\Bbbk}(U, Hom_{\Bbbk}(V,W))$

Demonstração. Basta considerar as aplicações lineares

$$Hom_{\Bbbk}(U \otimes_{\Bbbk} V, W) \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} Hom_{\Bbbk}(U, Hom_{\Bbbk}(V,W)),$$

onde

$$\begin{array}{rccl} \Phi: & Hom_{\Bbbk}(U \otimes_{\Bbbk} V, W) & \to & Hom_{\Bbbk}(U, Hom_{\Bbbk}(V,W)) \\ & f & \mapsto & \Phi_f: \ U \to Hom_{\Bbbk}(V,W) \\ & & & \qquad\quad u \mapsto \Phi_f(u): v \mapsto f(u \otimes v) \end{array}$$

e

$$\begin{array}{rccl} \Psi: & Hom_{\Bbbk}(U, Hom_{\Bbbk}(V,W)) & \longrightarrow & Hom_{\Bbbk}(U \otimes_{\Bbbk} V, W) \\ & g & \mapsto & \Psi_g: \ U \otimes_{\Bbbk} V \to W \\ & & & \qquad\quad u \otimes v \mapsto g(u)(v) \end{array}$$

A tarefa de verificar que estas aplicações são $\Bbbk$-lineares será deixada sob responsabilidade do leitor. Vamos apenas verificar que uma é a inversa da outra. De fato, pois se $f \in Hom_{\Bbbk}(U \otimes_{\Bbbk} V, W)$, então

$$(\Psi \circ \Phi)(f) = \Psi(\Phi_f) = \Psi_{\Phi_f} : u \otimes v \mapsto \Phi_f(u)(v) = f(u \otimes v),$$

ou seja, $(\Psi \circ \Phi)(f)(u \otimes v) = f(u \otimes v)$, o que significa que temos $(\Psi \circ \Phi)(f) = f$, para todo $f \in Hom_{\Bbbk}(U \otimes_{\Bbbk} V, W)$. Analogamente, se $g \in Hom_{\Bbbk}(U, Hom_{\Bbbk}(V,W))$, então

$$(\Phi \circ \Psi)(g) = \Phi(\Psi_g) = \Phi_{\Psi_g} : u \mapsto \Phi_{\Psi_g}(u) : v \mapsto \Psi(g)(u \otimes v) = (g(u))(v),$$

ou seja, $((\Phi \circ \Psi)(g)(u))(v) = (g(u))(v)$, o que significa que $(\Phi \circ \Psi)(g) = g$, para todo $g \in Hom_{\Bbbk}(U, Hom_{\Bbbk}(V, W))$. □

O seguinte resultado será útil adiante e segue como consequência dos anteriores. Por conta disso, resolvemos apresentá-lo aqui.

Proposição 1.3.13. *Sejam U e V espaços vetoriais sobre um corpo $\Bbbk$. Então existe um monomorfismo linear de $U^* \otimes_{\Bbbk} V^*$ em $(U \otimes_{\Bbbk} V)^*$. Este monomorfismo é um isomorfismo se, e somente se, $dim_{\Bbbk} U < \infty$ ou $dim_{\Bbbk} V < \infty$.*

Demonstração. Basta observar que podemos definir a aplicação $\Bbbk$-linear $\pi : U^* \otimes_{\Bbbk} V^* \to (U \otimes_{\Bbbk} V)^*$ como sendo a composição

$$\pi : U^* \otimes_{\Bbbk} V^* \xrightarrow{\varphi} Hom_{\Bbbk}(U, V^*) \simeq (U \otimes_{\Bbbk} V)^*$$

onde φ é dada na Proposição 1.3.11 e o isomorfismo é o mesmo do Lema 1.3.12, tomando $W = \Bbbk$. É claro que π é um isomorfismo se, e somente se, φ o é. O resultado então segue. □

É apropriado observar agora que o monomorfismo π da Proposição acima é dado por $\pi(f \otimes g)(u \otimes v) = f(u)g(v)$, para cada $f \otimes g \in U^* \otimes V^*$ e $u \otimes v \in U \otimes V$, pois na notação acima, temos $\pi(f \otimes g)(u \otimes v) = \Psi_{f_g}(u \otimes v) = (f_g(u))(v) = f(u)g(v)$.

Vamos apresentar agora um resultado que também será útil mais a frente.

Proposição 1.3.14. *Sejam $f : U \to V$ e $g : W \to T$ aplicações $\Bbbk$-lineares entre espaços vetoriais. Então $\mathcal{N}uc\,(f \otimes g) = \mathcal{N}uc\, f \otimes_{\Bbbk} W + U \otimes_{\Bbbk} \mathcal{N}uc\, g$.*

Demonstração. É claro que $\mathcal{N}uc\, f \otimes_{\Bbbk} W + U \otimes_{\Bbbk} \mathcal{N}uc\, g \subseteq \mathcal{N}uc\,(f \otimes g)$. Para ver a inclusão contrária, consideremos $\{u_i\}_{i \in I}$ uma base de $\mathcal{N}uc\, f$ e completamos este conjunto a uma base de U, digamos com $\{u_j\}_{j \in J}$. Então $\{f(u_j)\}_{j \in J}$ é um subconjunto linearmente independente de V. Analogamente, consideremos $\{w_k\}_{k \in K}$ uma base de $\mathcal{N}uc\, g$ e completamos a uma base de W, digamos com $\{w_l\}_{l \in L}$. Como antes, $\{g(w_l)\}_{l \in L}$ é um subconjunto linearmente independente em T. Para facilitar a escrita, vamos denotar $A := I \cup J$ e $B := K \cup L$.

Seja $x \in \mathcal{N}uc\, f \otimes g$. Então $x = \sum_{i \in A, k \in B} \alpha_{ij} v_i \otimes w_k \in U \otimes_{\Bbbk} W$. Assim, temos

$$0 = (f \otimes g)(x) = \sum_{i \in A, k \in B} \alpha_{ik} f(u_i) \otimes g(w_k) = \sum_{j \in J, l \in L} \alpha_{jl} f(u_j) \otimes g(w_l)$$

Da independência linear de $\{f(u_j) \otimes g(w_l)\}_{j\in J, l\in L}$ em $V \otimes_{\Bbbk} T$ segue que $\alpha_{jl} = 0$, para todos $j \in J$ e $l \in L$. Portanto, obtemos que

$$x = \sum_{i\in I, k\in B} \alpha_{ik} v_i \otimes w_k + \sum_{i\in A, k\in K} \alpha_{ik} v_i \otimes w_k \in \mathcal{N}uc\, f \otimes_{\Bbbk} W + U \otimes_{\Bbbk} \mathcal{N}uc\, g$$

□

1.4 Álgebras

Definição 1.4.1. *Sejam R um anel comutativo e A um R-módulo. Dizemos que A é uma álgebra sobre R (ou uma R-álgebra) se A possui uma estrutura de anel (não necessariamente comutativo) de modo que a multiplicação de A é compatível com a ação de R, no seguinte sentido*

$$r(ab) = (ra)b = a(rb),\ \forall r \in R; a, b \in A$$

Esta condição de compatibilidade pode ser enunciada dizendo que a multiplicação de A é uma aplicação R-bilinear. De fato, pois se A é uma R-álgebra, então a multiplicação de A, $m : A \times A \to A$ dada por $m(a, b) = ab$, satisfaz as seguintes propriedades:

- $m(a_1 + a_2, b) = (a_1 + a_2)b = a_1b + a_2b = m(a_1, b) + m(a_2, b)$,
- $m(a, b_1 + b_2) = a(b_1 + b_2) = ab_1 + ab_2 = m(a, b_1) + m(a, b_2)$,
- $m(ra, b) = (ra)b = a(rb) = m(a, rb)$,
- $m(ra, b) = (ra)b = r(ab) = r(m(a, b))$.

Assim, uma R-álgebra A é um R-módulo A que possui uma estrutura de anel cuja multiplicação é uma aplicação R-bilinear. Esta bilinearidade da multiplicação não nos permite considerar R-álgebras sobre anéis não comutativos.

Exemplo 1.4.2. (1) *Seja $L \supseteq \Bbbk$ uma extensão de corpos. Então L é um $\Bbbk$-espaço vetorial com ação dada por $r \cdot x = rx$, para todos $r \in R$ e $x \in L$. Claramente a multiplicação de L é compatível com a ação de R e, portanto, L é uma $\Bbbk$-álgebra. Assim, $\mathbb{C}$ é uma $\mathbb{R}$-álgebra, por exemplo.*

(2) *Todo anel A é uma $\mathbb{Z}$-álgebra. De fato, pois a estrutura aditiva de A define um grupo abeliano e, portanto, um $\mathbb{Z}$-módulo, como vimos antes. Segue dos axiomas da multiplicação que A é uma $\mathbb{Z}$-álgebra.*

(3) *Todo anel A é uma álgebra sobre seu centro. Aqui a ação de $\mathcal{Z}(A)$ sobre A é a própria multiplicação. A associatividade da multiplicação de A e o fato de todo elemento do centro comutar com todos os elementos de A garantem a compatibilidade exigida.*

(4) *Seja R um anel comutativo. Então o anel de polinômios $R[X]$ é uma R-álgebra. A ação de R sobre $R[X]$ é dada pela multiplicação de um elemento de R visto como um polinômio constante.*

(5) *Seja R um anel comutativo. Então $A := \mathcal{M}_n(R)$, o anel de matrizes $n \times n$ com entradas em R, é uma R-álgebra. Aqui, a ação de R sobre A é dada pela multiplicação usual de escalar por matriz.*

(6) *Generalizando o exemplo anterior, seja R um anel comutativo e M um R-módulo. Então $A := End_R(M)$ é uma R-álgebra, onde a multiplicação de A é dada pela composição de endomorfismos e a ação de R em A é dada por $r \triangleright f := m \mapsto f(rm)$. Para ver que a multiplicação de A é R-bilinear, basta observar que*

$$(r \triangleright (f \circ g))(m) = f \circ g(rm) = f(g(rm)) = f(rg(m)) = f(r \triangleright g(m)) = (f \circ (r \triangleright g))(m)$$

e

$$f(rg(m)) = (r \triangleright f)(g(m)) = ((r \triangleright f) \circ g)(m)$$

de onde segue que

$$r \triangleright (f \circ g) = (r \triangleright f) \circ g = f \circ (r \triangleright g)$$

Neste exemplo, o anel $End_R(M)$ está fazendo o papel do anel de matrizes. De fato, quando M é um R-módulo livre de posto n, então $End_R(M) \simeq \mathcal{M}_n(R)$ como anéis.

(7) *Seja G um grupo e R um anel comutativo. Definimos a álgebra de grupo de G sobre R, como sendo o R-módulo livre com base G (ou de forma equivalente, com base $\{\delta_g\}_{g \in G}$),*

$$R[G] := \oplus_{g \in G} R\delta_g$$

com multiplicação induzida pela operação de G. Assim, definimos

$$(r\delta_g)(s\delta_h) = rs\delta_{gh}$$

onde $r, s \in R$ e $g, h \in G$, e estendemos por linearidade aos elementos $x = \sum_{g \in G} r_g \delta_g \in R[G]$. Desta forma, temos

$$(\sum_{g \in G} r_g \delta_g)(\sum_{h \in G} s_h \delta_h) = \sum_{g,h \in G} r_g s_h \delta_{gh}.$$

A comutatividade de R garante a bilinearidade da multiplicação em $R[G]$.

Existe uma forma alternativa de introduzir o conceito de R-álgebra, como veremos a seguir.

Definição 1.4.3. *Seja R um anel comutativo. Um par (A, f) é dito uma R-algebra se A*

é um anel e $f : R \to A$ é um homomorfismo de anéis satisfazendo:

(i) $f(1_R) = 1_A$,

(ii) $\mathcal{I}m\, f \subseteq \mathcal{Z}(A)$.

Obviamente estas duas definições de R-álgebra são equivalentes, como mostra o próximo resultado.

Proposição 1.4.4. *As definições 1.4.1 e 1.4.3 são equivalentes, ou seja, existe uma correspondência biunívoca entre as estruturas algébricas definodas pela Definição 1.4.1 e as estruturas algébricas definidas pela Definição 1.4.3.*

Demonstração. Seja R um anel comutativo. Consideremos A uma R-álgebra via Definição 1.4.1. Vamos denotar a ação de R em A por $\triangleright : R \times A \to A$, dada por $(r, a) \mapsto r \triangleright a$. Definimos então $f : R \to A$, por $f(r) = r \triangleright 1_A$. Assim, f é um homomorfismo de anéis, pois f é claramente aditiva e

$$f(rs) = (rs) \triangleright 1_A = r \triangleright (s \triangleright 1_A) = r \triangleright (1_A(s \triangleright 1_A)) = (r \triangleright 1_A)(s \triangleright 1_A) = f(r)f(s)$$

onde na penúltima igualdade foi usada a R-bilinearidade da multiplicação de A. Além disso, temos

- $f(1_R) = 1_R \triangleright 1_A = 1_A$, pelos axiomas de R-módulo, e
- $af(r) = a(r \triangleright 1_A) = r \triangleright (a1_A) = r \triangleright (1_A a) = (r \triangleright 1_A)a = f(r)a$, mostrando que $f(R) \subseteq \mathcal{Z}(A)$. Note que a R-bilinearidade da multiplicação de A foi usada na terceira e na quinta igualdades.

O argumento acima mostra então que o par (A, f) é uma Rálgebra segundo a definição 1.4.3. Reciprocamente, suponhamos que o par (A, f) é uma Rálgebra segundo a definição 1.4.3. Para ver que neste caso A é um R-módulo de modo que a multiplicação de A é uma aplicação R-bilinear, basta definir a ação de R em A, por $r \triangleright a := f(r)a$. Como A é um anel, segue que $(A, +)$ é um grupo abeliano. Além disso, temos

- $1_R \triangleright a = f(1_R)a = 1_A a = a$,
- $(r + s) \triangleright a = f(r + s)a = (f(r) + f(s))a = f(r)a + f(s)a = (r \triangleright a) + (s \triangleright a)$,
- $r \triangleright (a + b) = f(r)(a + b) = f(r)a + f(r)b = r \triangleright a + r \triangleright b$,
- $r \triangleright (s \triangleright a) = f(r)(s \triangleright a) = f(r)(f(s)a) = (f(r)f(s))a = f(rs)a = (rs) \triangleright a$.

logo A tem uma estrutura de R-módulo. Para ver que a multiplicação de A é R-bilinear, basta observar que

$$r \triangleright (ab) = f(r)(ab) = (f(r)a)b = (r \triangleright a)b$$

e que

$$(f(r)a)b = (af(r))b = a(f(r)b) = a(r \triangleright b)$$

onde usamos o fato que $f(R) \subseteq \mathcal{Z}(A)$ na primeira igualdade acima. Assim, obtemos que

$$r \triangleright (ab) = (r \triangleright a)b = a(r \triangleright b)$$

ou seja, a multiplicação de A é R-bilinear. Portanto, A é uma R-álgebra via Definição 1.4.1.

A correspondência biunívoca então é induzida pela identidade

$$A \longleftrightarrow (A, f : r \mapsto r \triangleright 1_A).$$

□

Definição 1.4.5. *Sejam R um anel comutativo e A e B duas R-álgebras. Dizemos que uma função $f : A \to B$ é um homomorfismo de R-álgebras, se f é um homomorfismo de anéis tal que $f(1_A) = 1_B$ e f é um homomorfismo de R-módulos, ou seja, se f é uma aplicação R-linear multiplicativa e unitária (leva unidade em unidade).*

Sejam R um anel comutativo e A e B R-álgebras. Como A e B possuem estruturas de R-módulos, então podemos considerar o produto tensorial $A \otimes_R B$ o qual é um R-módulo. Desejamos definir uma multiplicação em $A \otimes_R B$ de modo a troná-lo uma R-álgebra. Isto pode ser feito de maneira natural via

$$m : (A \otimes_R B) \times (A \otimes_R B) \to A \otimes_R B,\ m(a_1 \otimes b_1, a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$$

Consideremos $m_A : A \otimes_R A \to A$ e $m_B : B \otimes_R B \to B$ as multiplicações de A e de B, respectivamente. Consideremos também o morfismo *flip* $\tau : A \otimes_R B \to B \otimes_R A$ definido anteriormente. Observemos agora que existe uma aplicação R-linear

$$\overline{m} : (A \otimes_R B) \otimes_R (A \otimes_R B) \to A \otimes_R B$$

definida por $m(a_1 \otimes b_1, a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$, a qual é dada pela composição das seguintes aplicações R-lineares:

$$A \otimes_R B \otimes_R A \otimes_R B \overset{id_A \otimes \tau \otimes id_B}{\longrightarrow} A \otimes_R A \otimes_R B \otimes_R B \overset{m_A \otimes m_B}{\to} A \otimes_R B$$

A propriedade universal do produto tensorial vai então garantir que existe uma aplicação bilinear

$$(A \otimes_R B) \times (A \otimes_R B) \to A \otimes_R B$$

como queríamos mostrar.

Sejam A uma $\Bbbk$-álgebra e M um A-módulo à esquerda. Então existe um homomorfismo de anéis $f : \Bbbk \to A$, segundo a Definição 1.4.3, de modo que M possui uma estrutura de $\Bbbk$-espaço vetorial, como visto antes. Consideremos agora V um $\Bbbk$-espaço vetorial. Queremos saber sob quais condições V se torna um A-módulo. O próximo resultado responde esta pergunta.

Proposição 1.4.6. *Sejam A uma $\Bbbk$-álgebra e V um $\Bbbk$-espaço vetorial. Então V é um A-módulo à esquerda (respectivamente, à direita) se, e somente se, existe um homomorfismo de álgebras $\varphi : A \to End_{\Bbbk}(V)$ (respectivamente, $\varphi : A^{op} \to End_{\Bbbk}(V)$).*

Demonstração. Suponhamos que V possui uma estrutura de A-módulo à esquerda, ou seja, estamos assumindo a existência de uma ação $\cdot : A \otimes M \to M$, a qual é uma aplicação $\Bbbk$-linear satisfazendo $1_A \cdot v = v$ e $a \cdot (b \cdot v) = (ab) \cdot v$, para todos $a, b \in A$ e $v \in V$. Então, basta definir $\varphi : A \to End_{\Bbbk}(V)$, por $\varphi(a) := \varphi_a : v \mapsto a \cdot v$, para obtermos o homomorfismo de álgebras desejado. De fato, pois neste caso tomando $a, b \in A$ e $v \in V$, teremos

$$\varphi(ab)(v) = \varphi_{ab}(v) = (ab) \cdot v = a \cdot (b \cdot v) = \varphi_a(\varphi_b(v)) = (\varphi_a \circ \varphi_b)(v)$$

ou seja, $\varphi(ab) = \varphi(a)\varphi(b)$. Além disso, $\varphi(1_A)(v) = 1_a \cdot v = v$, ou seja, $\varphi(1_A) = 1_{End(V)}$.

Reciprocamente, suponhamos que exista um morfismo de álgebras $\varphi : A \to End_{\Bbbk}(V)$. Neste caso, definimos a ação de A em V, por

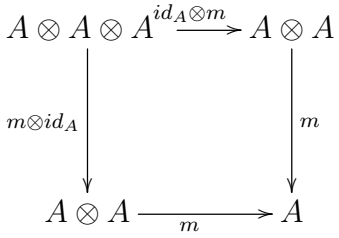
$$\begin{array}{rccc} \cdot : & A \otimes M & \longrightarrow & M \\ & a \otimes m & \mapsto & \varphi(a)(m) \end{array}$$

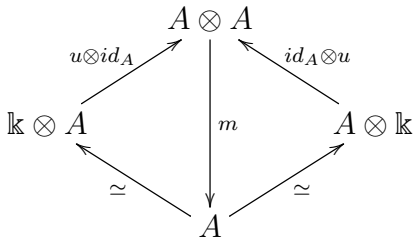
Então, para cada $a, b \in A$ e $v \in V$, teremos $a \cdot (b \cdot v) = \varphi(a)(\varphi(b)(v)) = (\varphi(a) \circ \varphi(b))(v) = \varphi(ab)(v) = (ab) \cdot v$ e $1_A \cdot v = \varphi(1_A)(v) = id_V(v) = v$. As demais propriedades a serem verificadas seguem facilmente. □

Por conta deste resultado, muitas vezes na literatura, os módulos sobre uma álgebra aparecem com a denominação de *representações* desta álgebra, pois o morfismo de álgebra nos dá uma forma de representar a álgebra A como uma subálgebra de $End_{\Bbbk}(V)$, a qual é mais simples de entender.

Para finalizar esta seção, vamos traduzir a definição de uma álgebra via diagramas, o que será importante na próximo capítulo. Uma $\Bbbk$-álgebra é um espaço vetorial A munido

de duas aplicações $\Bbbk$-lineares não nulas, a saber, a multiplicação $m : A \otimes A \to A$ e a unidade $u : \Bbbk \to A$, definidas de modo que os seguintes diagramas comutam





Assim, o primeiro diagrama retrata a associatividade da multiplicação, ou seja,

$$m \circ (id_A \otimes m) = m \circ (m \otimes id_A),$$

uma vez que se $a, b, c \in A$, então

$$(ab)c = m \circ (m \otimes id_A)(a \otimes b \otimes c) = m \circ (id_A \otimes m)(a \otimes b \otimes c) = a(bc)$$

Já o segundo diagrama retrata a unidade, sob a identificação de A com $A \otimes \Bbbk$ ou com $\Bbbk \otimes A$, pois dado $a \in A$, a igualdade

$$m \circ (id_A \otimes u) = id_A = m \circ (u \otimes id_A)$$

nos diz que

$$a = id_A(a) = m \circ (id_A \otimes u)(a \otimes 1_\Bbbk) = au(1_\Bbbk) \quad \text{e} \quad a = id_A(a) = m \circ (u \otimes Id_A)(1_\Bbbk \otimes a) = u(1_\Bbbk)a$$

de onde decorre que $1_A = u(1_\Bbbk)$.

1.5 A álgebra de grupo sobre corpos

O objetivo central destas notas é o de introduzir o leitor ao mundo das álgebras de Hopf. Podemos encarar as álgebras de Hopf como uma generalização natural das álgebras de grupo, num certo sentido. Este foi o motivo pelo qual decidimos abordar as álgebras de grupo em uma seção específica, onde veremos alguns conceitos e propriedades básicas neste contexto.

Dado um grupo G, podemos considerar a álgebra de grupo $\Bbbk G$, sobre um corpo $\Bbbk$, a qual consiste no $\Bbbk$-espaço vetorial com base G. Desta forma, os elementos de $\Bbbk G$ são da forma $\sum_{g \in G} \alpha_g g$, onde $\alpha_g \in \Bbbk$ é quase sempre nulo. A multiplicação em $\Bbbk G$ é induzida

pela multiplicação no grupo G. Assim, a multiplicação em $\Bbbk G$ é dada por

$$(\sum_{g\in G}\alpha_g g)(\sum_{g\in G}\beta_h h) = \sum_{g,h\in G}\alpha_g\beta_h gh$$

As álgebras de grupo são bastante estudadas e possuem propriedades muito interessantes. Estaremos particularmente interessados nas seguintes propriedades:

- $\Bbbk$ é um $\Bbbk G$-módulo à esquerda.

  De fato. Note que basta definir a ação de um elemento $g \in G$ em $1_\Bbbk$ para se ter uma ação de $\Bbbk G$ em $\Bbbk$. Assim, definindo-se $g \cdot 1_\Bbbk = 1_\Bbbk$, é fácil verificar que $\Bbbk$ se torna um $\Bbbk G$-módulo à esquerda via esta ação.

- $M \otimes N$ é um $\Bbbk G$-módulo à esquerda, sempre que M, N o são.

  Suponhamos que M e N são $\Bbbk G$-módulos à esquerda, as quais serão denotadas por $g \cdot m, \forall g \in G, m \in M$ e $g \cdot n, \forall g \in G, n \in N$, pois não há perigo de confusão. Definindo uma aplicação $\Bbbk$-linear $\triangleright : \Bbbk G \otimes (M \otimes N) \to M \otimes N$, por $g \triangleright (m \otimes n) = (g \cdot m) \otimes (g \cdot n)$, temos que

  $$\begin{aligned} g \triangleright (h \triangleright m \otimes n) &= g \triangleright (h \cdot m) \otimes (h \cdot n) = (g \cdot (h \cdot m)) \otimes (g \cdot (h \cdot n)) \\ &= (gh) \cdot m \otimes (gh) \cdot n = (gh) \triangleright m \otimes n \end{aligned}$$

  e

  $$1_{\Bbbk G} \triangleright m \otimes n = (1_{\Bbbk G} \cdot m) \otimes (1_{\Bbbk G} \cdot n) = m \otimes n$$

  de onde segue que $\triangleright$ define uma ação de $\Bbbk G$ em $M \otimes N$ à esquerda.

- Se M é um $\Bbbk G$-módulo à esquerda, então $M^* = Hom_\Bbbk(M, \Bbbk)$ também o é.

  Basta definir $\triangleright : \Bbbk G \otimes M^* \to M^*$ por $g \triangleright \phi : m \mapsto \phi(g^{-1} \cdot m)$, para todo $g \in G$ e $\phi \in M^*$. Desta forma, se $g, h \in G$, $\phi \in M^*$ e $m \in M$, teremos

  $$\begin{aligned} (g \triangleright (h \triangleright \phi))(m) &= (h \triangleright \phi)(g^{-1} \cdot m) = \phi(h^{-1} \cdot (g^{-1} \cdot m)) \\ &= \phi((h^{-1}g^{-1}) \cdot m) = \phi((gh)^{-1} \cdot m) \\ &= ((gh) \triangleright \phi)(m) \end{aligned}$$

  e

  $$(1_{\Bbbk G} \triangleright \phi)(m) = \phi(1_{\Bbbk G} \cdot m) = \phi(m)$$

  mostrando que $\triangleright$ define uma ação de $\Bbbk G$ em M^* à esquerda.

As ações descritas acima se fazem corresponder aos morfismos de $\Bbbk$-álgebras descritos

a seguir.

$$\begin{array}{ccc} \Bbbk G & \stackrel{\varepsilon}{\to} & End_{\Bbbk}(\Bbbk) \simeq \Bbbk \\ g & \mapsto & 1 \end{array}$$

Sejam M e N $\Bbbk$-módulos à esquerda. Então existem morfismos de $\Bbbk$-álgebras

$$\begin{array}{rccl} \varphi_M : & \Bbbk G & \to & End_{\Bbbk}(M) \\ & g & \mapsto & \varphi_M(g) : m \mapsto g \cdot m \end{array}$$

e

$$\begin{array}{rccl} \varphi_N : & \Bbbk G & \to & End_{\Bbbk}(N) \\ & g & \mapsto & \varphi_M(g) : n \mapsto g \cdot n \end{array}$$

a ação de $\Bbbk G$ se reflete na composta

$$\Bbbk G \stackrel{\Delta}{\to} \Bbbk G \otimes \Bbbk G \stackrel{\varphi_M \otimes \varphi_N}{\longrightarrow} End_{\Bbbk}(M) \otimes End_{\Bbbk}(N) \stackrel{\Psi}{\to} End(M \otimes N)$$

onde $\psi : End_{\Bbbk}(M) \otimes End_{\Bbbk}(N) \to End(M \otimes N)$ é dada por $\Psi(f \otimes g)(m \otimes n) := f(m) \otimes g(n)$, para todos elementos $f \in End_{\Bbbk}(M), g \in End_{\Bbbk}(N), m \in M, n \in N$, e $\Delta(g) := g \otimes g$.

Finalmente, a ação de $\Bbbk G$ em M^*, é representada pela composição

$$\Bbbk G \xrightarrow{S} \Bbbk G^{op} \xrightarrow{\varphi_g^*} End_{\Bbbk}(M^*)$$

onde $S(g) := g^{-1}$.

Portanto, as ações acima estão associadas a existência de morfismos de $\Bbbk$-álgebras $\varepsilon : \Bbbk G \to \Bbbk$, $\Delta : \Bbbk G \to \Bbbk G \otimes \Bbbk G$ e $S : \Bbbk G \to \Bbbk G^{op}$. Neste texto discutiremos sobre estruturas algébricas definidas em função da existência de tais morfismos.

Vamos finalizar esta seção mostrando que a existência dos respectivos morfismos é uma condição suficiente para que o corpo base, o produto tensorial e o espaço dual de módulos se torne um módulo sobre uma álgebra qualquer. O caso do corpo base é fácil e decorre imediatamente de um resultado que discutimos quando apresentamos exemplos de módulos, pois se existir um morfismo de álgebras $\varepsilon : A \to \Bbbk$, então todo espaço vetorial sobre $\Bbbk$ se torna um A-módulo, e, portanto, o próprio corpo base se torna um A-módulo à esquerda. Para os demais casos, temos o seguinte resultado.

Proposição 1.5.1. *Sejam A uma $\Bbbk$álgebra, M e N A-módulos à esquerda. Então:*

(i) $M \otimes N$ possui uma estrutura de $A \otimes A$-módulo.

(ii) $Hom_{\Bbbk}(M, N)$ possui uma estrutura de $A \otimes A^{op}$-módulo à esquerda.

Demonstração. (i) Sejam $\rightharpoonup$: $A \otimes M \to M$ e $\rightharpoondown$: $A \otimes N \to N$ as ações de A sobre M e N, respectivamente. Então, basta definir $\cdot : A \otimes A \otimes M \otimes N \to M \otimes N$, por

$(a \otimes b) \cdot (m \otimes n) := (a \rightharpoonup m) \otimes (b \rightharpoonup n) \in M \otimes N$, para se obter uma ação de $A \otimes A$ sobre $M \otimes N$.

(ii) Mantendo as notações acima, definimos $\cdot : A \otimes A^{op} \otimes Hom(M, N)$, por

$$((a \otimes b) \cdot f)(m) := a \rightharpoonup (f(b \rightharpoondown m))$$

para $a \in A, b \in A^{op}$ e $f \in Hom(M, N)$. Note que se $a \otimes b, c \otimes d \in A \otimes A^{op}$, $f \in Hom(M, N)$ e $m \in M$, então temos

$$\begin{aligned}
\big((a \otimes b) \cdot ((c \otimes d) \cdot f)\big)(m) &= a \rightharpoonup ((c \otimes d) \cdot f)(b \rightharpoondown m) \\
&= a \rightharpoonup (c \rightharpoonup f(d \rightharpoondown (b \rightharpoondown m))) \\
&= ac \rightharpoonup f((d._{op} b) \rightharpoondown m) \\
&= ac \rightharpoonup f((bd) \rightharpoondown m) \\
&= ((ac \otimes bd) \cdot f)(m)
\end{aligned}$$

ou seja, $(a \otimes b) \cdot ((c \otimes d) \cdot f) = ((a \otimes b)(c \otimes d)) \cdot f$. Além disso, é fácil verificar que $(1_A \otimes 1_{A^{op}}) \cdot f = f$. Logo, $Hom(M, N)$ possui uma estrutura de $A \otimes A^{op}$–módulo à esquerda. □

Considere agora uma $\Bbbk$-álgebra para a qual está definido um morfismo de álgebras $\varepsilon : A \to \Bbbk$. Neste caso, $\Bbbk$ é um A-módulo à esquerda e, fazendo $N = \Bbbk$ na parte (ii) da Proposição acima, obtemos que $M^* = Hom(M, \Bbbk)$ é um $A \otimes A^{op}$-módulo à esquerda. Portanto, se supomos adicionalmente que existem morfismos de álgebras $\Delta : A \to A \otimes A$ e $S : A \to A^{op}$, então, pelo mesmo raciocínio feito antes da última Proposição, obteremos que se M e N são A-módulos à esquerda, então $M \otimes N$ e M^* são A-módulos à esquerda. No caso da álgebra de grupo, nós exibimos tais morfismos. No que segue, vamos procurar estruturas adicionais em uma álgebra para que tais morfismos existam.

Capítulo 2

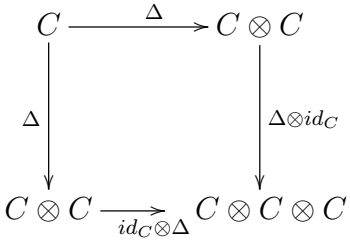
Biálgebras

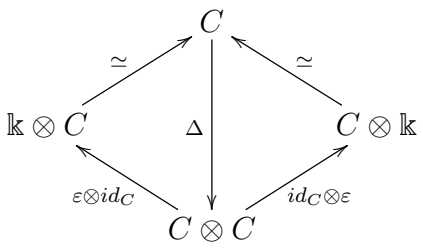
A partir deste ponto, $\Bbbk$ será um corpo e todos os espaços vetoriais e álgebras serão tomadas sobre $\Bbbk$, a menos que algo seja dito em contrário. Além disso, os símbolos $\otimes$, Hom e End, significam $\otimes_{\Bbbk}$, $Hom_{\Bbbk}$ e $End_{\Bbbk}$, respectivamente. Vamos discutir neste capítulo, as estruturas algébricas que denominamos biálgerbas sobre corpos. Como veremos mais adiante, uma biálgebra é um espaço vetorial que possui uma estrutura de álgebra e uma estrutura de coálgebra, as quais são compatíveis entre si. Começaremos o capítulo estudando as coálgebras.

2.1 Coálgebras

Dualizando a definição de álgebra obtemos o conceito de coálgebra. Esta dualização é uma noção categórica, e é obtida revertendo as flechas nos diagramas que definem uma álgebra, e que vimos no final da Seção 1.4. Mais precisamente, temos a seguinte definição.

Definição 2.1.1. *Sejam $\Bbbk$ um corpo. Uma coálgebra sobre $\Bbbk$ (ou uma $\Bbbk$-coálgebra) é uma terna $\mathcal{C} = (C, \Delta, \varepsilon)$, onde C é um $\Bbbk$-espaço vetorial, $\Delta : C \to C \otimes C$ e $\varepsilon : C \to \Bbbk$ são aplicações $\Bbbk$-lineares de modo que os diagramas abaixo são comutativos.*





O primeiro diagrama é chamado de *diagrama da coassociatividade* da coálgebra C, bem como o segundo é chamado de *diagrama da counidade* de C. Ou seja, as coálgebras

que vamos considerar neste texto são apenas as coálgebras coassociativas e counitárias, dualizando as álgebras associativas e unitárias.

Dado uma álgebra A com multiplicação $m : A \otimes A \to A$, $m(a \otimes b) := ab$, podemos considerar a álgebra oposta A^{op}, cuja multiplicação é dada por $m^{op} : A \otimes A \to A$, por $m^{op}(a \otimes b) = ba = m(b \otimes a)$, ou seja, $m^{op} = m \circ \tau$, onde $\tau = \tau_{A,A}$ é a aplicação $flip$ $\tau : a \otimes b \mapsto b \otimes a$. Além disso, vimos que A é comutativa se, e somente se, $A = A^{op}$ ou, equivalentemente, se $m^{op} = m$. Da mesma forma, podemos introduzir o conceito de coálgebra cooposta e de cocomutatividade de uma coálgebra.

Definição 2.1.2. *Seja (C, Δ, ε) uma coálgebra sobre $\Bbbk$. Chamamos de coálgebra cooposta de C a coálgebra $(C, \Delta^{cop}, \varepsilon)$, onde $\Delta^{cop} = \tau_{C,C} \circ \Delta$. Dizemos que uma coálgebra é cocomutativa, se $\Delta^{cop} = \Delta$.*

Frequentemente, vamos denotar uma coálgebra apenas por C, em lugar de (C, Δ, ε). Nesta mesma linha, denotaremos via de regra a coálgebra cooposta por C^{cop}. Vamos chamar a aplicação Δ de *comultiplicação* e ε de *counidade*.

Antes de prosseguir, vamos gastar um tempo discutindo uma nova notação para as explosões originárias da aplicação sucessiva da comultiplicação. Sejam C uma $\Bbbk$-coálgebra e $c \in C$. Então $\Delta(c) \in C \otimes C$, ou seja, devemos ter $\Delta(c) = \sum_{i=1}^{n} c_{i1} \otimes c_{i2}$. Aplicando agora $id_C \otimes \Delta$ e $\Delta \otimes id_C$ neste elemento, teremos por um lado

$$(id_C \otimes \Delta)(\Delta(c)) = (id_C \otimes \Delta)(\sum_{i=1}^{n} c_{i1} \otimes c_{i2}) = \sum_{i=1}^{n} c_{i1} \otimes (\sum_{j=1}^{m} c_{i2_{j1}} \otimes c_{i2_{j2}})$$

e por outro,

$$(\Delta \otimes id_C)(\Delta(c)) = (\Delta \otimes id_C)(\sum_{i=1}^{n} c_{i1} \otimes c_{i2}) = \sum_{i=1}^{n} (\sum_{j=1}^{k} c_{i1_{j1}} \otimes c_{i1_{j2}}) \otimes c_{i2})$$

a coassociatividade de Δ agora garante que $(id_C \otimes \Delta) \circ \Delta = (\Delta \otimes id_C) \circ \Delta$. Assim, devemos ter

$$\sum_{i=1}^{n} c_{i1} \otimes (\sum_{j=1}^{m} c_{i2_{j1}} \otimes c_{i2_{j2}}) = \sum_{i=1}^{n} (\sum_{j=1}^{k} c_{i1_{j1}} \otimes c_{i1_{j2}}) \otimes c_{i2})$$

por este motivo, vamos simplificar nossas notações escrevendo

$$\Delta(c) = \sum_{(c)} c_1 \otimes c_2$$

onde c_1 e c_2 são símbolos e não elementos, de modo que c_1 representa todas as primeiras entradas dos tensores básicos que aparecem numa determinada escrita de $\Delta(c) \in C \otimes C$ e, analogamente, c_2 representa todas as segundas entradas dos tensores básicos que aparecem

numa determinada escrita de $\Delta(c)$. A igualdade acima nos diz então que

$$(id_C \otimes \Delta)\Delta(c) = \sum_{(c),(c_2)} c_1 \otimes c_{2_1} \otimes c_{2_2} = \sum_{(c),(c_1)} c_{1_1} \otimes c_{1_2} \otimes c_2 = (\Delta \otimes id_C)\Delta(c)$$

e, portanto, vamos denotar esta igualdade apenas por

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

Esta notação é chamada de *notação de Sweedler*, e depois de o leitor se acostumar com ela, verá que a mesma trás inúmeras facilidades.

Ainda, vamos denotar por $\Delta^{\otimes n}$ o operador obtido por aplicarmos Δ n vezes, em qualquer ordem, pois a coassociatividade dispensa uso de parenteses para identificar qual membro de um tensor foi "explodido"pela aplicação de Δ. Assim,

- $\Delta^{\otimes 2} = (id_C \otimes \Delta)\Delta = (\Delta \otimes id_C)\Delta$,
- $\Delta^{\otimes 3} = (\Delta \otimes id_C \otimes id_C) \circ \Delta^{\otimes 2} = (id_C \otimes \Delta \otimes id_C) \circ \Delta^{\otimes 2} = (id_C \otimes id_C \otimes \Delta) \circ \Delta^{\otimes 2}$
- $\Delta^{\otimes n} = \Delta^{\otimes n-1} \circ \Delta, \forall n \geq 2$.

de modo que se $c \in C$, então escreveremos $\Delta^{\otimes n}(c) = c_1 \otimes c_2 \otimes \cdots \otimes c_{n+1}$.

O axioma da counidade nos diz que $(\varepsilon \otimes id_C) \circ \Delta = id_C = (id_C \otimes \varepsilon) \circ \Delta$. Usando a notação de Sweedler, esta relação pode ser traduzida da seguinte forma

$$\sum_{(c)} c_1\varepsilon(c_2) = c = \sum_{(c)} \varepsilon(c_1)c_2, \ \forall c \in C$$

Note que o axioma da counidade também garante que a aplicação Δ é injetora, pois se assim não fosse, jamais poderíamos ter $(\varepsilon \otimes id_C) \circ \Delta$ uma aplicação injetora tal como é id_C. Vamos apresentar agora alguns exemplos básicos de coálgebras.

Exemplo 2.1.3. (**1**). *Todo corpo* $\Bbbk$ *tem uma estrutura de coálgebra, a saber,* $\Delta(1) = 1 \otimes 1$ *e* $\varepsilon(1) = 1$.

(**2**). *Generalizando o exemplo anterior, podemos considerar um conjunto* S *qualquer e considerar* C *o* $\Bbbk$*-espaço vetorial com base* S*. Então* $C = \Bbbk S$ *tem uma estrutura de coálgebra dada por* $\Delta : \Bbbk S \to \Bbbk S \otimes \Bbbk S$, $\Delta : s \mapsto s \otimes s$, *e* $\varepsilon : \Bbbk S \to \Bbbk$, $\varepsilon : s \mapsto 1$. *Note que basta definir* Δ *e* ε *nos elementos da base e estender por linearidade.*

(**3**). *Um subexemplo do caso anterior, o qual será bastante interessante para nosso estudo, é dado pelos anéis de grupo. Seja* G *um grupo e* $C = \Bbbk G$ *o anel de grupo sobre*

$\Bbbk$ *correspondente. Definindo* $\Delta : \Bbbk G \to \Bbbk G \otimes \Bbbk G$ *por* $\Delta(g) = g \otimes g$ *e* $\varepsilon : \Bbbk G \to \Bbbk$, *por* $\varepsilon(g) = 1$, *obtemos uma estrutura de coálgebra no anel de grupo* $\Bbbk G$.

(**4**). *Um outro subexemplo do caso de* (3) *é dado pelos anéis de polinômios sobre corpos. Seja* $C = \Bbbk[X]$ *o anel de polinômios sobre* $\Bbbk$. *Então* C *é um* $\Bbbk$*-espaço vetorial com base infinita* $\{1, X, X^2, \ldots, X^n, \ldots\}$. *Então, se definimos* $\Delta(1) = 1 \otimes 1$ *e* $\Delta(X^n) = X^n \otimes X^n$, $\varepsilon(1) = 1$ *e* $\varepsilon(X^n) = 1$, *obtemos que* $C = \Bbbk[X]$ *é uma coálgebra.*

(**5**).. *Muitas vezes podemos introduzir mais de uma estrutura de coálgebra em um* $\Bbbk$*-espaço vetorial. Vejamos um tal exemplo para o anel de polinômios* $C = \Bbbk[X]$. *Basta definirmos* $\Delta(1) = 1 \otimes 1$, $\Delta(X) = X \otimes 1 + 1 \otimes X$, $\varepsilon(1) = 1$ *e* $\varepsilon(X) = 0$, *estendendo* Δ *e* ε *multiplicativamente sobre a base, ou seja,* $\Delta(X) = \sum_{k=0}^{n} \binom{n}{k} X^k \otimes X^{n-k}$ *e* $\varepsilon(X^n) = \delta_{n,0}$, *também obtemos uma nova estrutura de coálgebra em* $C = \Bbbk[X]$.

(**6**). *Na mesma linha dos exemplos anteriores, considere um conjunto* S *e seja* $C = \Bbbk[S \times S]$ *o* $\Bbbk$*-espaço vetorial com base* $S \times S$. *Então* C *possui uma estrutura de coálgebra dada por*

$$\Delta(s,t) = \sum_{u \in S} (s,u) \otimes (u,t) \;\; e \;\; \varepsilon(s,t) = \delta_{s,t}, \; \forall (s,t) \in S \times S$$

onde $\delta_{s,t} = 1$, *se* $s = t$ *e* $\delta_{s,t} = 0$, *se* $s \neq t$ *(delta de Kronecker).*

(**7**) *Sejam* $C = (C, \Delta_C, \varepsilon_C)$ *e* $D = (D, \Delta_D, \varepsilon_D)$ *duas coálgebras. Então o espaço vetorial* $C \otimes D$ *possui uma estrutura de coálgebra definida por* $(C \otimes D, \Delta_{C\otimes D}, \varepsilon_{C\otimes D})$, *onde* $\Delta_{C\otimes D} = (id_C \otimes \tau \otimes id_D) \circ (\Delta_C \otimes \Delta_D)$ *e* $\varepsilon_{C\otimes D} = \varepsilon_C \otimes \varepsilon_D$. *Desta forma, se* $c \in C; d \in D$, *então*

$$(\Delta_C \otimes \Delta_D)(c \otimes d) = \sum_{(c),(d)} c_1 \otimes d_1 \otimes c_2 \otimes d_2 \quad e \quad \varepsilon_{C\otimes D}(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d)$$

Vamos discutir um pouco sobre alguns fatos relativos aos exemplos acima, aproveitando o momento para introduzir alguns conceitos usuais na teoria de coálgebras. Seja C uma coálgebra. Um elemento $c \in C$ é dito *elemento group-like*, se $\Delta(c) = c \otimes c$ e $\varepsilon(c) = 1$. O conjunto de todos os elementos group-like de uma coálgebra C será denotado por $G(C)$. A condição $\varepsilon(c) = 1$ da definição de elemento group-like pode ser substituida exigindo-se que um elemento group-like seja não nulo, por conta do seguinte resultado.

Proposição 2.1.4. *Seja* C *uma* $\Bbbk$*-coálgebra. Então o conjunto* $G(C)$ *é linearmente independente sobre* $\Bbbk$.

Demonstração. Suponhamos por contradição que $G(C)$ não é linearmente independente sobre $\Bbbk$. Então existe uma combinação linear finita não trivial $\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_k s_k = 0$,

onde $\alpha_i \in \Bbbk$, $1 \leq i \leq k$. Podemos supor que esta é uma menor tal combinação linear, de modo que podemos assumir que $\alpha_i \neq 0$, para todo i, e $s_i \neq s_j$, se $i \neq j$. Como $0 \notin G(C)$, pois $\varepsilon(0) = 0 \neq 1$, segue que $k \geq 1$. Portanto, $\{s_1, ..., s_{k-1}\}$ deve ser linearmente independente sobre $\Bbbk$, de modo que podemos escrever $s_k = \beta_1 s_1 + \cdots + \beta_{k-1} s_{k-1}$. Mas então temos, por um lado, que $\Delta(s_r) = s_r \otimes s_r$ e, por outro, $\Delta(s_r) = \sum_{i=1}^{k-1} \beta_i s_i \otimes s_i$.Portanto, o posto de s_r é dado por $1 = k - 1$, e segue que $k = 2$. Mas então, $s_2 = \beta_1 s_1$. Aplicando ε nesta igualdade, obtemos que $1 = \varepsilon(s_2) = \beta_1 \varepsilon(s_1) = \beta_1$, ou seja $s_2 = s_1$. Mas isto contradiz o fato de que os elementos $s_i's$ eram todos distintos. Esta contradição produz o resultado desejado. □

Segue do resultado acima que no caso da coálgebra $\Bbbk S$ do Exemplo 2.1.3(2), devemos ter $G(\Bbbk S) = S$. Reciprocamente, se C é uma coálgebra gerada como espaço vetorial por seus elementos group-like, então $C = \Bbbk G(C)$. Por conta destes fatos, a coálgebra $\Bbbk S$ acima é chamada de *coálgebra group-like*.

Sejam $g, h \in C$ dois elementos group-like. Dizemos que $x \in C$ é um elemento *skew primitivo*, ou g, h*-primitivo* (quando necessitamos, por exemplo, explicitar os elementos group-like considerados), se $\Delta(x) = g \otimes x + x \otimes h$. Se $g = 1 = h$, então dizemos que um elemento $x \in C$ tal que $\Delta(x) = 1 \otimes x + x \otimes 1$ é *primitivo*. Assim, no Exemplo 2.1.3(4) o anel de polinômios foi apresentado com uma estrutura de coálgebra gerado por um elemento primitivo. Gostaríamos de observar aqui que se $x \in C$ é um elemento skew primitivo, então $\varepsilon(x) = 0$. De fato, pois $x = (id_C \otimes \varepsilon)\Delta(x) = (id_C \otimes \varepsilon)(g \otimes x + x \otimes h) = g\varepsilon(x) + x\varepsilon(h) = g\varepsilon(x) + x$, de onde segue que $0 = g\varepsilon(x)$. Como $\varepsilon(x) \in \Bbbk$ e $\{g\}$ é linearmente independente sobre $\Bbbk$, segue que $\varepsilon(x) = 0$, como afirmado.

Se g e h são elementos group-like de uma coálgebra C, então denotamos por $P_{g,h}(C) := \{x \in C : \Delta(x) = g \otimes x + x \otimes h\}$. Se $g = 1 = h$, então escrevemos $P(C)$ para denotar o conjunto $P_{1,1}(C)$ dos elementos primitivos de C. A linearidade de Δ e as propriedades do produto tensorial garantem que $P_{g,h}(C)$ é um subespaço vetorial de C.

Vamos denotar por $C_S(\Bbbk)$ a coálgebra do Exemplo 2.1.3(6). Escrevendo e_{ij} para denotar o elemento $(i, j) \in S \times S$, teremos que

$$\Delta(e_{ij}) = \sum_{k \in S} e_{ik} \otimes e_{kj} \qquad \text{e} \qquad \varepsilon(e_{ij}) = \delta_{i,j}.$$

Como a fórmula de Δ lembra o produto matricial, quando S for um conjunto finito, esta coálgebra será chamada de *coálgbra de comatrizes sobre* $\Bbbk$. Vamos definir $C_\emptyset(\Bbbk) := 0$ e se $S = \{1, 2, ..., n\}$, então escreveremos $C_n(\Bbbk)$, em lugar de $C_S(\Bbbk)$. Além disso, dizemos que uma família de elementos $\{c_{ij}\}$ de $C_S(\Bbbk)$ satisfaz as identidades de comatrizes, se valer

$$\Delta(c_{ij}) = \sum_{k \in S} c_{ik} \otimes c_{kj} \qquad \text{e} \qquad \varepsilon(c_{ij}) = \delta_{i,j} \tag{2.1}$$

Quando estudamos álgebras, estamos sempre interessados nas subestruturas subálgebras, ideais à direita e à esquerda e nos ideais. Vamos ver que existem, na teoria de coálgebras, os correspondentes conceitos destas subestruturas. Se $A = (A, m, u)$ é uma $\Bbbk$-álgebra, então uma subálgebra é um subespaço V de A para o qual a restrição da multiplicação está bem definida e $(V, m_{|_{V \otimes V}}, u)$ é uma $\Bbbk$-álgebra. Um ideal à esquerda é um $\Bbbk$-subespaço de A tal que $m(A \otimes V) \subseteq V$. Assim, dualizando estes conceitos, podemos introduzir a noção de subcoálgebra e de coideias unilaterais.

Definição 2.1.5. *Sejam $C = (C, \Delta, \varepsilon)$ uma coálgebra e V um $\Bbbk$-subespaço de C. Então dizemos que:*

(i) V é uma subcoálgebra de C, se $\Delta(V) \subseteq V \otimes V$,

(ii) V é um coideal à esquerda de C, se $\Delta(C) \subseteq C \otimes V$,

(iii) V é um coideal à direita de C, se $\Delta(V) \subseteq V \otimes C$.

Note que se V é ambos, um coideal à direita e um coideal à esquerda, então devemos ter $\Delta(V) \subseteq C \otimes V$ e $\Delta(V) \subseteq V \otimes C$, de onde segue que $\Delta(V) \subseteq V \otimes V$, ou seja, V é uma subcoálgebra de C. Então, uma noção de coideal (o correspondente a um ideal de uma álgebra) não pode ser definido como sendo um coideal "bilateral", pois esta noção coincide com subcoalgebra. Um ideal (bilateral) de uma álgebra é caracterizado como sendo o núcleo de um homomorfismo de álgebras. Vamos então introduzir o conceito de morfismo de coálgebras antes de considerar o que seriam os coideais.

Definição 2.1.6. *Sejam $C = (C, \Delta_C, \varepsilon_C)$ e $D = (D, \Delta_D, \varepsilon_D)$ coálgebras sobre um corpo $\Bbbk$ e $f : C \to D$ uma aplicação $\Bbbk$-linear. Dizemos que f é um homomorfismo de coálgebras, se:*

(i) $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$,

(ii) $\varepsilon_D \circ f = \varepsilon_C$.

Um isomorfismo de coálgebra é um homomorfismo de coálgebra que é um isomorfismo linear.

As condições da definição acima dizem que os diagramas abaixo comutam

Em termos da notação de Sweedler, as condições acima nos dizem que, para todo $c \in C$, temos

$$(f(c))_1 \otimes (f(c))_2 = \Delta_D(f(c)) = (f \otimes f)(\sum_{(c)} c_1 \otimes c_2) = \sum_{(c)} f(c_1) \otimes f(c_2)$$

e

$$\varepsilon_D(f(c)) = \varepsilon_C(c)$$

Seja $f : C \to D$ um homomorfismo de coálgebras. A condição $\varepsilon_D \circ f = \varepsilon_C$ nos diz que $\mathcal{N}uc\, f \subseteq \mathcal{N}uc\, \varepsilon_C$, ou seja, $\varepsilon_C(\mathcal{N}uc\, f) = 0$. Já a condição $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$ nos diz que $\Delta_C(\mathcal{N}uc\, f) \subseteq \mathcal{N}uc\, (f \otimes f)$, pois se $x \in \mathcal{N}uc\, f$, segue que $0 = \Delta_D(f(x)) = (f \otimes f)(\Delta_C(x))$. Como $\mathcal{N}uc\, (f \otimes f) = \mathcal{N}uc\, f \otimes C + C \otimes \mathcal{N}uc\, f$, segue que

$$\Delta_C(\mathcal{N}uc\, f) \subseteq \mathcal{N}uc\, f \otimes C + C \otimes \mathcal{N}uc\, f.$$

Assim, as propriedades do núcleo de um homomorfismo de coálgebras discutidas acima induzem o seguinte conceito.

Definição 2.1.7. *Sejam C uma $\Bbbk$-coálgebra e $I \subseteq C$ um $\Bbbk$-subespaço de C. Dizemos que I é um coideal de C, se*

(i) $\varepsilon(I) = 0$,

(ii) $\Delta(I) \subseteq I \otimes C + C \otimes I$.

Dado C uma coálgebra, segue que $\varepsilon : C \to \Bbbk$ é um homomorfismo de coálgebras. De fato, pois se $c \in C$, então $(\varepsilon \otimes \varepsilon)\Delta(c) = \sum_{(c)} \varepsilon(c_1) \otimes \varepsilon(c_2) = (\sum_{(c)} \varepsilon(c_1)\varepsilon(c_2))(1 \otimes 1) = \varepsilon(\sum_{(c)} c_1\varepsilon(c_2))(1 \otimes 1) = \varepsilon(c)(1 \otimes 1) = \Delta_{\Bbbk}(\varepsilon(c))$ e $\varepsilon_{\Bbbk} \circ \varepsilon = id \circ \varepsilon = \varepsilon$. Portanto, $\mathcal{N}uc\, \varepsilon$ é um coideal de C, o qual será denotado por C^+.

Tal como no caso de álgebras, estruturas quocientes também estão definidas no contexto de coálgebras, como mostra o próximo resultado.

Proposição 2.1.8. *Sejam C, D $\Bbbk$-coálgebras, $f : C \to D$ um morfismo de coálgebras e I um coideal de C. Então:*

(i) O $\Bbbk$-espaço vetorial quociente C/I possui uma única estrutura de coálgebra de modo que a projeção canônica linear $\pi : C \to C/I$ se torna um morfismo de coálgebras.

(ii) **(Teorema dos homomorfismos para coálgebras)** *$\mathcal{N}uc\, f$ é um coideal de C e se $I \subseteq \mathcal{N}uc\, f$, então existe um único morfismo de coálgebra $\overline{f} : C/I \to D$ tal que $\overline{f} \circ \pi = f$. Além disso, $\overline{f}$ é injetiva se, e somente se, $I = \mathcal{N}uc\, f$.*

Demonstração. (i) Como I é um coideal de C, temos que $\Delta(I) \subseteq I \otimes C + C \otimes I$ e $\varepsilon(I) = 0$. Assim, temos $(\pi \otimes \pi)\Delta(I) \subseteq \pi(I) \otimes \pi(C) + \pi(C) \otimes \pi(I) = 0 \otimes I + I \otimes 0 = 0$. Segue então do Teorema de Homomorfismos para espaços vetoriais que existem únicas aplicações lineares $\overline{\Delta} : C/I \to C/I \otimes C/I$ e $\overline{\varepsilon} : C/I \to \Bbbk$ tais que os diagramas abaixo comutam (onde os morfismos são considerados apenas como aplicações $\Bbbk$-lineres)

$$\begin{array}{ccc} C & \xrightarrow{\pi} & C/I \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\overline{\Delta}} \\ C \otimes C & \xrightarrow[\pi\otimes\pi]{} & C/I \otimes C/I \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{\pi} & C/I \\ & {\scriptstyle\varepsilon}\searrow \quad \swarrow{\scriptstyle\overline{\varepsilon}} & \\ & \Bbbk & \end{array}$$

onde as aplicações $\overline{\Delta}$ e $\overline{\varepsilon}$ estão definidas por $\overline{\Delta}(\overline{c}) = \sum_{(c)} \overline{c_1} \otimes \overline{c_2}$ e $\overline{\varepsilon}(\overline{c}) = \varepsilon(c)$. Portanto, devemos ter

$$(\overline{\Delta} \otimes id_{C/I})\overline{\Delta}(\overline{c}) = \sum_{(c)} \overline{c_1} \otimes \overline{c_2} \otimes \overline{c_3} = (id_{C/I} \otimes \overline{\Delta})\overline{\Delta}(\overline{c})$$

e

$$\overline{c} = \pi(c) = \pi(\sum_{(c)} \varepsilon(c_1)c_2) = \sum_{(c)} \varepsilon(c_1)\pi(c_2) = \sum_{(c)} \overline{\varepsilon}(\overline{c_1})\overline{c_2}$$

ou seja, $(C/I, \overline{\Delta}, \overline{\varepsilon})$ é uma $\Bbbk$-coálgebra. Para finalizar a demonstração de (i), basta observar que a unicidade da estrutura de coálgebra de C/I é dada pela unicidade das aplicações $\Bbbk$-lineares $\overline{\Delta}$ e $\overline{\varepsilon}$.

(ii) A demonstração deste item segue a mesma ideia da anterior, ou seja, primeiro usamos o Teorema dos Homomorfismos para espaços vetoriais para garantir a existência de uma aplicação $\Bbbk$-linear $\overline{f} : C/I \to D$ tal que $\overline{f} \circ \pi = f$, e depois mostramos que esta aplicação é coassociativa e counitária. Os detalhes serão deixados à cargo do leitor. □

Vamos encerrar esta seção discutindo sobre uma propriedade das coálgebras que não tem contrapartida no caso das álgebras, a saber, vamos mostrar que coálgebras são estruturas localmente finitas, ou seja, todo elemento de uma coálgebra está contido numa subcoálgebra de dimensão finita. Para esta finalidade, começamos com uma observação que segue das propriedades da counidade e da coassociatividade de uma coálgebra.

Seja C uma coálgebra. Note que $c = (\varepsilon \otimes id_C \otimes \varepsilon)\Delta^{\otimes 2}(c)$, para todo $c \in C$, pois

$$\begin{aligned}(\varepsilon \otimes id_C \otimes \varepsilon)\Delta^{\otimes 2} &= (\varepsilon \otimes id_C \otimes \varepsilon)(id_C \otimes \Delta)\Delta \\ &= ((\varepsilon \circ id_C) \otimes (id_C \otimes \varepsilon)\Delta)\Delta \\ &= (\varepsilon \otimes id_C)\Delta \\ &= id_C\end{aligned}$$

Podemos então enunciar nosso resultado.

Teorema 2.1.9. (Teorema Fundamental das Coálgebras). *seja C uma coálgebra. Todo elemento $c \in C$ está contido numa subcoálgebra finito-dimensional de C.*

Demonstração. Seja $c \in C$. Vamos denotar o elemento $\Delta^{\otimes 2}(c)$, por $\Delta^{\otimes 2}(c) := \sum_{i,j} c_i \otimes e_{ij} \otimes d_j$, onde as famílias finitas $\{c_i\}$ e $\{d_j\}$ são tomadas linearmente independentes sobre $\Bbbk$. Consideremos o $\Bbbk$-espaço vetorial $V = \mathcal{G}er\,\{e_{ij}\}$ gerado pelos elementos e_{ij}, o qual tem dimensão finita. Pela observação anterior, como $c = (\varepsilon \otimes id_C \otimes \varepsilon)\Delta^{\otimes 2}(c) = \sum_{i,j} \varepsilon(c_i)\varepsilon(d_j)e_{ij}$, segue que $c \in V$. Agora, usando a coassociatividade de Δ, obtemos que

$$\sum_{i,j} \Delta(c_i) \otimes e_{ij} \otimes d_j = (\Delta \otimes id_C \otimes id_C)\Delta^{\otimes 2}(c) = (id_C \otimes \Delta \otimes id_C)\Delta^{\otimes 2}(c) = \sum_{i,j} c_i \otimes \Delta(e_{ij}) \otimes d_j$$

e segue da independência linear da família $\{d_j\}$ que

$$\sum_i \Delta(c_i) \otimes e_{ij} = \sum_i c_i \otimes \Delta(e_{ij}) \in C \otimes C \otimes V$$

e usando agora a independência linear da família $\{c_i\}$, segue que $\Delta(e_{ij}) \in C \otimes V$. De modo análogo, usando a igualdade $(id_C \otimes id_C \otimes \Delta)\Delta^{\otimes 2}(c) = (id_C \otimes \Delta \otimes id_C)\Delta^{\otimes 2}$ obtemos que $\Delta(e_{ij}) \in V \otimes C$. Portanto, devemos ter $\Delta(V) \subseteq (C \otimes V) \cap (V \otimes C) = V \otimes V$ e, consequentemente, V é uma subcoálgebra finito-dimensional de C. Isto finaliza a demonstração. □

2.2 O dual de uma coálgebra

Nesta seção veremos que o espaço vetorial dos funcionais lineares definidos sobre uma coálgebra possui uma estrutura de álgebra, bem como estudaremos as relações entre a estrutura da coálgrba considerada e de sua álgebra dual.

Sejam $C = (C, \Delta, \varepsilon)$ uma coálgebra sobre um corpo $\Bbbk$ e $C^* = Hom_{\Bbbk}(C, \Bbbk)$ o espaço vetorial dual de C. Vamos considerar as aplicações transpostas $\Delta^* : (C \otimes C)^* \to C^*$ e $\varepsilon^* : \Bbbk \to C^*$. Da álgebra linear, sabemos que estas aplicações são dadas por $\Delta^*(f) = f \circ \Delta$,

para todo $f \in (C \otimes C)^*$, e $\varepsilon^*(1) = \Phi \circ \varepsilon$, onde $\Phi : \Bbbk \simeq \Bbbk^*$. Como $C^* \otimes C^*$ é um subespaço vetorial de $(C \otimes C)^*$, podemos considerar a restrição de Δ^* ao subespaço $C^* \otimes C^*$, que denotaremos por $\Delta^*_{|_{C^* \otimes C^*}} : C^* \otimes C^* \to C^*$. Com estas notações, temos o seguinte resultado.

Proposição 2.2.1. *Mantendo as notações acima, temos que (C^*, m, u) é uma álgebra, onde $m = \Delta^*_{|_{C^* \otimes C^*}}$ e $u = \varepsilon^* \circ \Phi$.*

Demonstração. Começamos observando que se $f, g \in C^*$ e $c \in C$, então

$$\Delta^*_{|_{C^* \otimes C^*}}(f \otimes g) : c \mapsto (f \otimes g)\Delta(c) = \sum_{(c)} f(c_1) \otimes g(c_2) = \sum_{(c)} f(c_1)g(c_2).$$

Por este motivo, vamos denotar a multiplicação de $C^* \otimes C^*$, por $m = (f \otimes g)\Delta := f * g$. Para ver que esta multiplicação é associativa, basta observar que se $f, g, h \in C^*$ e $c \in C$, então

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

Para ver que C^* com a multiplicação $m = f * g$ é uma álgebra unitária, primeiro note que Φ nada mais é do que a multiplicação por um escalar. Assim, $u(1) = \varepsilon$. Agora, se $f \in C^*$ e $c \in C$, então segue que $(\varepsilon * f)(c) \sum_{(c)} \varepsilon(c_1)f(c_2) = \sum_{(c)} f(\varepsilon(c_1)c_2) = f(\sum_{(c)} \varepsilon(c_1)c_2) = f(c)$. Analogamente, $(f * \varepsilon)(c) = f(c)$, de onde se conclui que $u(1) = \varepsilon = 1_{C^*}$. Isto finaliza nossa demonstração. □

Definição 2.2.2. *A álgebra definida na Proposição acima é chamada de álgebra dual de C.*

Seja $f : C \to D$ um morfismo de coálgebras. Como f é uma aplicação $\Bbbk$-linear, podemos considerar a sua transposta $f^* : D^* \to C^*$ que é uma aplicação $\Bbbk$-linear, a princípio, entre duas $\Bbbk$-álgebras. Então é completamente natural neste momento nos perguntarmos se f^* é um morfismo de álgebras. O próximo resultado nos dá uma resposta positiva para esta questão.

Proposição 2.2.3. *Seja $f : C \to D$ um morfismo de coálgebras. Então $f^* : D^* \to C^*$ é um morfismo de álgebras.*

Demonstração. Sejam $\alpha, \beta \in D^* = Hom_{\Bbbk}(D, \Bbbk)$ e $c \in C$. Então $(f^*(\alpha \otimes \beta))(c) = (\alpha \otimes \beta)f(c) = \sum_{(f(c))} \alpha(f(c)_1)\beta(f(c)_2) = \sum_{(c)} \alpha(f(c_1))\beta(f(c_2)) = \sum_{(c)}(f^*(\alpha))(c_1)(f^*(\beta))(c_2) = (f^*(\alpha) * f^*(\beta))(c)$, ou seja, $f^*(\alpha * \beta) = f^*(\alpha) * f^*(\beta)$, onde na terceira igualdade foi usado que f é um morfismo de coálgebras. Assim, f^* é uma aplicação multiplicativa. Para ver que f^* é unitária, basta observar que $f^* \circ \varepsilon_D = \varepsilon_D \circ f = \varepsilon_C$, pois f é um morfismo de coálgebras. Portanto, $f^*(1_{D^*}) = 1_{C^*}$. Isto completa a demonstração. □

Podemos estar interessados em saber qual a relação existente, se é que uma tal relação existe, entre a estrutura de uma coálgebra e de sual álgebra dual. Veremos isto no próximo resultado. Lembremos antes alguns fatos básicos de álgebra linear. Seja V um espaço vetorial e $S \subseteq V$ um subconjunto qualquer. Então definimos o subespaço $S^{\perp}$ de $V^* = Hom_{\Bbbk}(V, \Bbbk)$, por

$$S^{\perp} := \{f \in V^* : f(s) = 0, \forall s \in S\} \subseteq V^*$$

tal subespaço é chamado de anulador de S em V^*. De modo análogo, se $T \subseteq V^*$ é um subconjunto qualquer, então definimos o anulador de T em V, por

$$T^{\perp} := \{v \in V : f(v) = 0, \forall f \in T\} \subseteq V$$

é um exercício relativamente fácil mostrar que de fato $S^{\perp}$ e $T^{\perp}$ são subespaços vetoriais de V^* e de V, respectivamente.

Antes de prosseguir, gostaríamos de fazer dois comentários neste momento. Existe um teorema de representação de funcionais lineares por produtos internos, de modo que é completamente natural escrevermos $< f, v >$, para denotar o elemento $f(v) \in \Bbbk$, para $f \in V^*$ e $v \in V$. Assim, usando esta notação, se $S \subseteq V$, então $S^{\perp} = \{f \in V^* :< f, S >= 0\}$, induzindo o uso do símbolo de ortogonalidade, usado em álgebra linear, para denotar o anulador de S.

Outra coisa que queremos chamar atenção é o fato termos $(S^{\perp})^{\perp} = S$, sempre que S é um subespaço de V. De fato, pois a inclusão $S \subseteq (S^{\perp})^{\perp}$ é clara. Para ver a outra inclusão, observamos que se $x \in (S^{\perp})^{\perp} \setminus S$, então $\Bbbk x \cap S = 0$, pois S é um subespaço de V e, assim, deve existir um funcional linear $f \in V^*$ tal que $f(x) = 1$ e $f(S) = 0$. Mas então, $f \in S^{\perp}$ e segue que $f(x) = 0$, pois $x \in (S^{\perp})^{\perp}$. Esta contradição produz o resultado desejado.

Proposição 2.2.4. *Sejam C uma coálgebra sobre um corpo $\Bbbk$ e D um subespaço de C. Então, D é uma subcoálgebra de C se, e somente se, o espaço $D^{\perp}$ é um ideal (bilateral) da álgebra dual C^*.*

Demonstração. Suponhamos que D é uma subcoálgebra de C. Para mostrar que $D^{\perp}$ é

um ideal de C^*, basta mostrar que $D^\perp$ é o núcleo de algum morfismo de álgebras definido em C^*. Para tanto, basta observar que a inclusão de espaços vetoriais $\iota : D \to C$ é um morfismo de coálgebras, visto que D é uma subcoálgebra de C. Mas então, a transposta deste morfismo, a saber, $\iota^* : C^* \to D^*$ é um morfismo de álgebras, pela Proposição 2.2.3. Agora é só observar que $\mathcal{N}uc\,\iota^* = D^\perp$.

Reciprocamente, suponhamos que $D^\perp$ é um ideal de $C^* := Hom_{\Bbbk}(C, \Bbbk)$ a qual é uma álgebra com o produto $f * g(c) = \sum_{(c)} f(c_1)g(c_2)$, para todos $f, g \in C^*$. Pela observação feita antes, temos que $(D^\perp)^\perp = D$, pois D é um subespaço de C. Seja $d \in D = (D^\perp)^\perp$ e escrevemos $\Delta(d) = \sum_{i=1}^n x_i \otimes y_i \in C \otimes C$ de modo que os conjuntos $\{x_i\}$ e $\{y_i\}$ sejam linearmente independentes em C. Queremos mostrar que $\Delta(d) \in D \otimes D = (C \otimes D) \cap (D \otimes C)$. Note que se $\Delta(d) \notin D \otimes C$, então podemos supor que $x_1 \neq D$. Assim, existe $f \in D^\perp \subseteq C^*$ tal que $f(x_1) \neq 0$. A independência liner dos elementos $y_j's$ nos diz que existe $g \in C^*$ tal que $g(y_j) = \delta_{1,j}$. Como $D^\perp$ é um ideal de C^*, por hipótese, segue que $f * g \in D^\perp$. Mas então, devemos ter

$$0 = (f * g)(d) = \sum_{i=1}^{n} f(x_i)g(y_i) = f(x_1)g(y_1) = f(x_1) \neq 0$$

Esta contradição nos diz então que $\Delta(d) \in D \otimes C$. De modo análogo se mostra que $\Delta(d) \in C \otimes D$, de onde segue que $\Delta(D) \subseteq D \otimes D$. Portanto, D é uma subcoálgebra de C. □

Outras relações serão apresentadas no final da próxima seção.

2.3 O dual finito de uma álgebra

seja $A = (A, m, u)$ uma $\Bbbk$-álgebra. Como antes, podemos considerar o espaço dual $A^* = Hom_{\Bbbk}(A, \Bbbk)$ e nos perguntar se é possível introduzir uma estrutura de coálgebra neste espaço. O problema agora é mais delicado. Note que toda coálgebra é localmente finita e se $dim_{\Bbbk} A = \infty$, então não vamos poder garantir esta propriedade para o espaço dual A^*. Para contornar este problema, trabalharemos com o maior subespaço localmente finito contido em A^*, o qual será chamado de dual finito de A, como veremos adiante.

Para procurar este subespaço de A^* que seria o maior subespaço localmente finito, vamos começar observando que A^* tem uma estrutura de A-bimódulo dada pelas seguintes ações:

$$\begin{array}{rccc} \rightharpoonup\colon & A \otimes A^* & \longrightarrow & A^* \\ & a \otimes f & \mapsto & a \rightharpoonup f : \begin{array}{ccc} A & \to & \Bbbk \\ x & \mapsto & f(xa) \end{array} \end{array}$$

e

$$\begin{array}{rccc} \leftharpoonup\colon & A^* \otimes A & \longrightarrow & A^* \\ & f \otimes a & \mapsto & f \leftharpoonup a : \begin{array}{ccc} A & \to & \Bbbk \\ x & \mapsto & f(ax) \end{array} \end{array}$$

De fato, pois se $a, b, x \in A$ e $f \in A^*$, então temos

$$(b \rightharpoonup (a \rightharpoonup f))(x) = (a \rightharpoonup f)(xb) = f((xb)a) = f(x(ba)) = (ba \rightharpoonup f)(x)$$

e

$$(1_A \rightharpoonup f)(x) = f(x1_A) = f(x)$$

e obtemos que $b \rightharpoonup (a \rightharpoonup f) = ba \rightharpoonup f$ e $1_A \rightharpoonup f = f$, de modo que $\rightharpoonup$ define em A^* uma estrutura de A-módulo à esquerda. Analogamente se mostra que $(f \leftharpoonup a) \leftharpoonup b = f \leftharpoonup ab$ e $f \leftharpoonup 1_A = f$, de modo que $\leftharpoonup$ define em A^* uma estrutura de A-módulo à direita. Além disso, temos

$$\begin{aligned} ((a \rightharpoonup f) \leftharpoonup b)(x) &= (a \rightharpoonup f)(bx) \\ &= f((bx)a) = f(b(xa)) \\ &= (f \leftharpoonup b)(xa) \\ &= (a \rightharpoonup (f \leftharpoonup b))(x) \end{aligned}$$

ou seja,

$$((a \rightharpoonup f) \leftharpoonup b) = (a \rightharpoonup (f \leftharpoonup b))$$

e A^* se torna um A-bimódulo via estas ações.

Vamos considerar então o subespaço de A^* definido por

$$A^\circ := \{f \in A^* : dim_{\Bbbk}(A \rightharpoonup f \leftharpoonup A) < \infty\}$$

Este subespaço possui a propriedade de que todo elemento está contido em um subespaço finito-dimensional, a qual é uma condição necessária para que possua uma estrutura de coálgebra. Antes de mostrarmos isto, vamos examinar uma forma equivalente de definirmos A° que se torna mais útil no desenvolvimento de nossa teoria.

Proposição 2.3.1. *Sejam A uma álgebra sobre um corpo $\Bbbk$ e $f \in A^*$ um funcional linear. As seguintes afirmações são equivalentes:*

(i) $dim_{\Bbbk}(A \rightharpoonup f \leftharpoonup A) < \infty$,

(ii) Existe um ideal I *de* A *tal que* $f(I) = 0$ *e* $dim_{\Bbbk} A/I < \infty$.

Demonstração. Vamos assumir que $dim_{\Bbbk}(A \rightharpoonup f \leftharpoonup A) < \infty$. Então, como

$$A \rightharpoonup f = A \rightharpoonup f \leftharpoonup 1_A \subseteq A \rightharpoonup f \leftharpoonup A,$$

segue que $dim_{\Bbbk}(A \rightharpoonup f) < \infty$. Consideremos agora a aplicação linear

$$\begin{array}{rccc} \psi: & A & \longrightarrow & End_{\Bbbk}(A \rightharpoonup f) \\ & a & \mapsto & \psi_a: \begin{array}{ccc} (A \rightharpoonup f) & \to & (A \rightharpoonup f) \\ g & \mapsto & a \rightharpoonup g \end{array} \end{array}$$

e vejamos que esta aplicação é um homomorfismo de álgebras. De fato, pois se $a, b \in A$ e $g \in A \rightharpoonup f$, então temos

$$\psi(ab)(g) = \psi_{ab}(g) = ab \rightharpoonup g = a \rightharpoonup (b \rightharpoonup g) = \psi_a \circ \psi_b(g)$$

e

$$\psi(1_A)(g) = 1_A \rightharpoonup g = g$$

de onde segue que $\psi(ab) = \psi(a)\psi(b)$ e $\psi(1_A) = 1_{End(A \rightharpoonup f)}$, como queríamos mostrar.

Como temos $dim_{\Bbbk}(A \rightharpoonup f) < \infty$, segue que $End_{\Bbbk}(A \rightharpoonup f)$ é isomorfo a um anel de matrizes e, portanto, um espaço vetorial finito-dimensional sobre $\Bbbk$. Desta forma, tomando $I = \mathcal{N}uc\,\psi$, obtemos que I é um ideal de A e, como $A/I \simeq \mathcal{I}m\,\psi \subseteq End_{\Bbbk}(A \rightharpoonup f)$, segue que $dim_{\Bbbk} A/I < \infty$. Observamos agora que se $a \in I = \mathcal{N}uc\,\psi$, então

$$f(a) = f(1_A a) = (a \rightharpoonup f)(1_A) = \psi_a(1_A) = 0,$$

pois $\psi_a = \psi(a)$. Assim, f anula um ideal I de A tal que $dim_{\Bbbk} A/I < \infty$.

Reciprocamente, suponhamos que existe um ideal I de A tal que $dim_{\Bbbk} A/I < \infty$ e $f(I) = 0$. Então, para todos $a, b \in A$, devemos ter $(a \rightharpoonup f \leftharpoonup b)(I) = f(bIa) \subseteq f(I) = 0$, de onde segue que $A \rightharpoonup f \leftharpoonup A \in \{g \in A^* : g(I) = 0\}$. Como $dim_{\Bbbk}(A/I) < \infty$, segue que existe uma família finita de elementos $\{a_i\}_{i=1}^n \subseteq A$ que completa uma $\Bbbk$-base de I a uma $\Bbbk$-base de A.

Para cada $i \in \{1, 2, ..., n\}$, consideremos o funcional linear $\varphi_i \in A^*$ definido por $\varphi_i(I) = 0$ e $\varphi_i(a_j) = \delta_{i,j}$. Logo, $\{g \in A^* : g(I) = 0\} = \mathcal{G}er_{\Bbbk}\{\varphi_1, \varphi_2, ..., \varphi_n\}$, de onde se obtém que $dim_{\Bbbk}\{g \in A^* : g(I) = 0\} < \infty$ e, consequentemente, $dim_{\Bbbk}(A \rightharpoonup f \leftharpoonup A) < \infty$, como queríamos mostrar. □

Antes de prosseguir, gostaríamos de lembrar que se W é um subespaço vetorial de V tal que $dimV/W < \infty$, então dizemos que W é um subespaço de *codimensão* finita. O resultado acima nos diz então que o maior subespaço localmente finito de A^* é o subespaço formado pelos funcionais lineares que anulam algum ideal de codimensão finita de A. No que segue, vamos utilizar a igualdade

$$A^\circ = \{f \in A^* : \exists I \lhd A, dim_{\Bbbk} A/I < \infty \text{ e } f(I) = 0\}$$

Nosso objetivo agora é introduzir uma comultiplicação em A°. Algum trabalho para tanto será necessário ainda. Começamos com o próximo resultado que é simples, mas tem consequências úteis.

Lema 2.3.2. *Sejam $f : A \to B$ um homomorfismo de álgebras e J um ideal de codimensão finita de B. Então $I := f^{-1}(J)$ é um ideal de codimensão finita de A.*

Demonstração. Já sabemos que $I = f^{-1}(J)$ é um ideal de A. Para ver que I tem codimensão finita, basta considerar a composição de homomorfismos de anéis

$$A \xrightarrow{f} B \xrightarrow{\pi} B/J$$

onde $\pi : B \to B/J$ é a projeção canônica. Assim, $I = f^{-1}(J) = \mathcal{N}uc\, \pi \circ f$ e, portanto, $A/(f^{-1}(J)) \simeq \mathcal{I}m\, (\pi \circ f) \subseteq B/J$, de onde se obtém que $dim_{\Bbbk} A/(f^{-1}(J)) < \infty$. □

Para o próximo resultado, lembramos que se $h : U \to V$ é uma aplicação $\Bbbk$-linear, então a transposta de h é definida como sendo $h^* : V^* \to U^*$, $h^* : \alpha \mapsto \alpha \circ h$, para todo $\alpha \in V^*$.

Corolário 2.3.3. *Seja $f : A \to B$ um homomorfismo de álgebras. Então $f^*(B^\circ) \subseteq A^\circ$.*

Demonstração. Seja $g \in B^\circ$. Então existe um ideal J de B com codimensão finita tal que $g(J) = 0$. Segue do Lema anterior que $I := f^{-1}(J)$ é um ideal de A com codimensão finita. Além disso, $f^{-1}(J) \subseteq \mathcal{N}uc\, (g \circ f) = \mathcal{N}uc\, f^*(g)$, ou seja, $f^*(g) \in A^\circ$, como queríamos mostrar. □

Para o próximo resultado, vamos precisar lembrar o monomorfismo canônico

$$\psi : A^* \otimes B^* \to (A \otimes B)^*,$$

definido por $\psi(f \otimes g)(a \otimes b) = f(a)g(b)$, para todos $f \otimes g \in A^* \otimes B^*$ e $a \otimes b \in A \otimes B$, o qual foi introduzido na Proposição 1.3.13.

Lema 2.3.4. *Mantendo as notações acima, temos $\psi(A^\circ \otimes B^\circ) = (A \otimes B)^\circ$.*

Demonstração. Sejam $\alpha \in A^\circ$ e $\beta \in B^\circ$. Consideremos $I \lhd A$ e $J \lhd B$ ideais de codimensão finita tais que $\alpha(I) = 0 = \beta(J)$. Netse caso, temos $A \otimes J + I \otimes B \subseteq \mathcal{N}uc\,(\alpha \otimes \beta)$. Como $A \otimes J + I \otimes B \lhd A \otimes B$ e $\dfrac{A \otimes B}{A \otimes J + I \otimes B} \simeq A/I \otimes B/J$, segue que $\psi(\alpha \otimes \beta) \in (A \otimes B)^\circ$. Portanto, $\psi(A^\circ \otimes B^\circ) \subseteq (A \otimes B)^\circ$.

Para ver a inclusão contrária, tomamos $\gamma \in (A \otimes B)^\circ$. Então existe um ideal K de $A \otimes B$ de codimensão finita tal que $\gamma(K) = 0$. Vamos definir

$$I := \{a \in A : a \otimes 1_B \in K\} \quad \text{e} \quad J := \{b \in B : 1_A \otimes b \in K\}$$

e consideremos as aplicações canônicas $i_A : A \to A \otimes B$ dada por $i_A(a) = a \otimes 1_B$, e $i_B : A \to A \otimes B$ dada por $i_B(b) = 1_A \otimes b$. É fácil verificar que estas são homomorfismos de álgebras injetores, de modo que podemos considerar $A \subseteq A \otimes B$ e $B \subseteq A \otimes B$. Assim, por construção, temos que $I = i_A^{-1}(K)$ e $J = i_B^{-1}(K)$. Segue então do Lema 2.3.2 que $dim_{\Bbbk} A/I, dim_{\Bbbk} B/J < \infty$.

Observamos agora que $A \otimes J + I \otimes B$ é um ideal de $A \otimes B$ tal que $\gamma(A \otimes J + I \otimes B) = 0$ e $\dfrac{A \otimes B}{A \otimes J + I \otimes B} \simeq A/I \otimes B/J$. Segue então do Teorema dos Homomorfismos que deve existir $\overline{\gamma} : A/I \otimes B/J \to \Bbbk$ de modo que o diagrama abaixo comuta

$$\begin{array}{ccc} A \otimes B & \xrightarrow{\pi_I \otimes \pi_J} & A/I \otimes B/J \\ & {\scriptstyle \gamma} \searrow \quad \swarrow {\scriptstyle \overline{\gamma}} & \\ & \Bbbk & \end{array}$$

Como $dim_{\Bbbk}(A/I)^* = dim_{\Bbbk}(A/I) < \infty$ e $dim_{\Bbbk}(B/J)^* = dim_{\Bbbk}(B/J) < \infty$, segue que o monomorfismo canônico $\Theta : (A/I)^* \otimes (B/J)^* \to (A/I \otimes B/J)^*$ é um isomorfismo, de onde obtemos que existem conjuntos finitos $\{\alpha_i\} \subseteq (A/I)^*$ e $\{\beta_j\} \subseteq (B/J)^*$ tais que $\overline{\gamma} = \theta(\sum_{i,j} \alpha_i \otimes \beta_i)$. Portanto, se $a \in A$ e $b \in B$, temos

$$\begin{aligned} \gamma(a \otimes b) &= \overline{\gamma}(\pi_I(a) \otimes \pi_J(b)) \\ &= \sum_{i,j} (\alpha_i \otimes \beta_j)(\pi_I(a) \otimes \pi_J(b)) \\ &= (\sum_{i,j} (\alpha_i \circ \pi_I)(a)(\beta_j \circ \pi_J)(b) \\ &= \theta(\sum_{i,j} (\alpha_i \circ \pi_i) \otimes (\beta \circ \pi_j))(a \otimes b) \end{aligned}$$

ou seja, $\gamma = \theta(\sum_{i,j} (\alpha_i \circ \pi_i) \otimes (\beta \circ \pi_j))$, com $\alpha_i \circ \pi_I \in A^*$ e $\beta \circ \pi_J \in B^*$. Mas como $I \subseteq \mathcal{N}uc\,(\alpha_{ik} \circ \pi_I)$ e $J \subseteq \mathcal{N}uc\,(\beta \circ \pi_J)$, segue que $\alpha \circ \pi_I \in A^\circ$ e $\beta \circ \pi_J \in B^\circ$. Portanto, $h \in \theta(A^\circ \otimes B^\circ)$, e segue que $\psi(A^\circ \otimes B^\circ) = (A \otimes B)^\circ$, o que finaliza nossa demonstração. $\square$

Para definir uma comultiplicação em A°, que tem sido nosso objetivo até o momento,

precisamos de mais um resultado auxiliar.

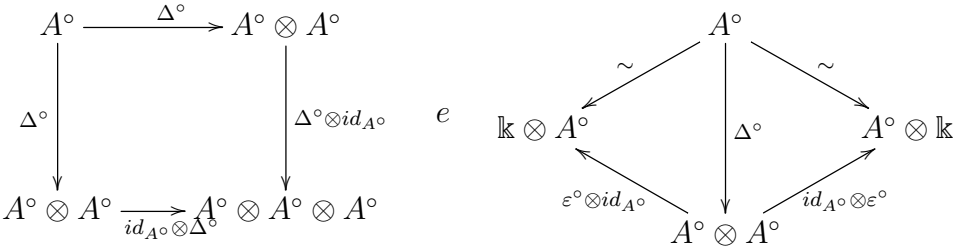
Lema 2.3.5. *Seja A uma $\Bbbk$-álgebra com multiplicação $m : A \otimes A \to A$. Então $m^* : A^* \to (A \otimes A)^*$ é tal que $m^*(A^\circ) \subseteq (A \otimes A)^\circ$.*

Demonstração. Seja $f \in A^\circ$. Então existe um ideal I de A de codimensão finita tal que $f(I) = 0$. Assim, $A \otimes I + I \otimes A$ é um ideal de $A \otimes A$ satisfazendo $dim_{\Bbbk}\left(\frac{A \otimes A}{A \otimes I + I \otimes A}\right) = dim_{\Bbbk}(A/I \otimes A/I) < \infty$ e tal que $m^*(f)(A \otimes I + I \otimes A) = f \circ m(A \otimes I + I \otimes A) \subseteq f(I) = 0$. Portanto, $m^*(A^\circ) \subseteq (A \otimes A)^\circ$, como queríamos mostrar. □

Segue dos resultados acima que se A é uma álgebra com multiplicação $m : A \otimes A \to A$, então $m^*(A^\circ) \subseteq (A \otimes A)^\circ = \psi(A^\circ \otimes A^\circ)$. Notemos agora que a restrição do monomorfismo canônico $\psi : A^* \otimes A^* \to (A \otimes A)^*$ ao espaço finito-dimensional $A^\circ \otimes A^\circ$ é um isomorfismo $\Psi := \psi_{|A^\circ \otimes A^\circ} : A^\circ \otimes A^\circ \to (A \otimes A)^\circ$. Portanto, mostramos até aqui que $\Psi^{-1} \circ m^* : A^\circ \to A^\circ \otimes A^\circ$ é uma aplicação $\Bbbk$-linear que se apresenta então como uma candidata natural a ser nossa comultiplicação. De fato é isto o que acontece e será mostrado no próximo resultado. Antes porém, vamos fixar uma notação que será útil. Se V é um $\Bbbk$-espaço vetorial, então mostramos que $V^* \otimes V^*$ é um subespaço de $(V \otimes V)^*$, em geral. O mesmo argumento pode mostrar este fenômeno para mais parcelas de V, ou seja, $V^* \otimes V^* \otimes \cdots \otimes V^*$ é um subespaço de $(V \otimes V \otimes \cdots \otimes V)^*$, usando indução no argumento que utilizamos. No próximo resultado vamos precisar utilizar que $A^* \otimes A^* \otimes A^*$ é um subespaço de $(A \otimes A \otimes A)^*$, quando A é uma álgebra. Se $f, g, h \in A^*$ e $a, b, c \in A$, então vamos denotar o elemento $(f \otimes g \otimes h)(a \otimes b \otimes c)$, por $f(a)g(b)h(c) \in \Bbbk$.

Teorema 2.3.6. *Seja $A = (A, m, u)$ uma álgebra sobre um corpo $\Bbbk$. Então $(A^\circ, \Delta^\circ, \varepsilon^\circ)$ é uma coálgebra, onde $\Delta^\circ = \Psi^{-1} \circ m^*$ e $\varepsilon^\circ = u^*$.*

Demonstração. Já sabemos que $\Delta^\circ(A^\circ) \subseteq A^\circ \otimes A^\circ$ e $\varepsilon^\circ(A^\circ) \subseteq \Bbbk$ são aplicações $\Bbbk$-lineares. Então, para obter o resultado desejado, precisamos ver que estas aplicações cumprem as condições de coassociatividade e counidade, ou seja, precisamos verificar que os seguintes diagramas comutam



Observamos que $\Delta^\circ : A^\circ \to A^\circ \otimes A^\circ$. Assim, se $\Delta^\circ(f) = \sum_{(f)} f_1 \otimes f_2 \in A^\circ \otimes A^\circ$, para $f \in A^\circ$, como $\Delta^\circ = \Psi^{-1} \circ m^*$, segue se $a, b \in A$, então $\Delta^\circ(f)(a \otimes b) = (\Psi \circ m^*(f))(a \otimes b)$

se, e somente se,

$$\Big(\sum_{(f)} f_1 \otimes f_2\Big)(a \otimes b) = \Psi \circ \Delta^\circ(f)(a \otimes b) = m^*(f)(a \otimes b) = f(ab)$$

Denotando por $\theta : A^\circ \otimes A^\circ \otimes A^\circ \to (A \otimes A \otimes A)^*$ o monomorfismo canônico, tomando $f, g \in A^\circ$ e $a, b, c \in A$, temos

$$\begin{aligned}
\theta(\Delta^\circ \otimes id_{A^\circ})(f \otimes g)(a \otimes b \otimes c) &= \theta(\sum_{(f)} f_1 \otimes f_2 \otimes g)(a \otimes b \otimes c) \\
&= \sum_{(f)} f_1(a) f_2(b) g(c) \\
&= f(ab)g(c) \\
&= (\psi(f \otimes g))(ab \otimes c) \\
&= (\psi(f \otimes g)(m \otimes id_A)(a \otimes b \otimes c) \\
&= (m \otimes id_A)^{*|}(\psi(f \otimes g)(a \otimes b \otimes c)
\end{aligned}$$

ou seja, $\theta(\Delta^\circ \otimes id_{A^\circ}) = (m \otimes id_A)^* \circ \psi$. Analogamente, mostramos que $\theta(id_{A^\circ} \otimes \Delta^\circ) = (id_A \otimes m)^* \circ \psi$. Usando estas igualdades, obtemos

$$\begin{aligned}
\theta((\Delta^\circ \otimes id_{A^\circ})\Delta^\circ) &= (m \otimes id_A)^* \psi \circ \Delta^\circ \\
&= (m \otimes id_A)^* \circ m^* \\
&= (id_A \otimes m)^* \circ m^* \\
&= (id_A \otimes m)^* \circ \psi \circ \Delta^\circ \\
&= \theta(id_{A^\circ} \otimes \Delta^\circ) \circ \Delta^\circ
\end{aligned}$$

ou seja, $\theta((\Delta^\circ \otimes id_{A^\circ})\Delta^\circ) = \theta((id_{A^\circ} \otimes \Delta^\circ) \circ \Delta^\circ)$. Como θ é injetora, segue que

$$(\Delta^\circ \otimes id_{A^\circ})\Delta^\circ = (id_{A^\circ} \otimes \Delta^\circ) \circ \Delta^\circ$$

o que mostra a comutatividade do primeiro diagrama. Para verificarmos a comutatividade do segundo diagrama, basta observar que se $f \in A^\circ$, $\Delta^\circ(f) = \sum_{(f)} f_1 \otimes f_2 \in A^\circ \otimes A^\circ$ e $a \in A$, então temos

$$\Big(\sum_{(f)} \varepsilon^\circ(f_1) f_2\Big)(a) = \sum_{(f)} f_1(1_A) f_2(a) = f(1_A a) = f(a)$$

e, de modo análogo, se mostra que

$$f(a) = \Big(\sum_{(f)} f_1 \varepsilon^\circ(f_2)\Big)(a)$$

o que finaliza nossa demonstração. □

Definição 2.3.7. *Seja $A = (A, m, u)$ uma álgebra. A coálgebra definida acima é chamada de coálgebra dual de A.*

Note que se $f : A \to B$ é um morfismo de álgebras, então sabemos que $f^\circ(B^\circ) \subseteq A^\circ$. Como, tanto A° como B° são coálgebras, é natural se perguntar se a trnsposta de f restrita ao dual finito de A é um morfismo de coálgebras. Uma resposta afirmativa a esta questão é dada no próximo resultado.

Proposição 2.3.8. *Seja $f : A \to B$ um morfismo de álgebras. Então $f^\circ : B^\circ \to A^\circ$ é um morfismo de coálgebras.*

Demonstração. Precisamos ver que os diagramas abaixo comutam

$$\begin{array}{ccc} B^\circ & \xrightarrow{f^\circ} & A^\circ \\ {\scriptstyle \Delta_A B^\circ}\downarrow & & \downarrow{\scriptstyle \Delta_A A^\circ} \\ B^\circ \otimes B^\circ & \xrightarrow[f^\circ \otimes f^\circ]{} & A^\circ \otimes A^\circ \end{array} \qquad \begin{array}{ccc} B^\circ & \xrightarrow{f^\circ} & A^\circ \\ & {\scriptstyle \varepsilon_{B^\circ}} \searrow \quad \swarrow {\scriptstyle \varepsilon_{A^\circ}} & \\ & \Bbbk & \end{array}$$

Seja $\beta \in B^\circ$. Então

$$\varepsilon_{A^\circ} \circ f^\circ(\beta) = (f^\circ(\beta))(1_A) = \beta(f(1_A)) = \beta(1_B) = \varepsilon_{B^\circ}(\beta)$$

e segue que o segundo diagrama comuta. Para ver a comutatividade do primeiro, vamos denotar por $\psi : A^\circ \otimes A^\circ \to (A \otimes A)^*$ o monomorfismo canônico. Dado $\beta \in B^\circ$, usando a notação de Sweedler, vamos escrever $\Delta_{B^\circ}(\beta) = \sum_{(\beta)} \beta_1 \otimes \beta_2 \in B^\circ \otimes B^\circ$. Com estas notações, se $x, y \in A$, então temos, por um lado

$$\begin{aligned} ((\psi(f^\circ \otimes f^\circ)\Delta_{B^\circ})(\beta))(x \otimes y) &= \sum_{(\beta)} (f^\circ(\beta_1))(x)(f^\circ(\beta_2))(y) \\ &= \sum_{(\beta)} \beta_1(f(x))\beta_2(f(y)) \\ &= \beta(f(x)f(y)) \\ &= (\beta \circ f)(xy) \end{aligned}$$

e, por outro,

$$\begin{aligned} ((\psi(\Delta_{A^\circ} f^\circ))(\beta))(x \otimes y) &= (\psi\Delta_{A^\circ})(\beta \circ f)(x \otimes y) \\ &= (m_A^*(\beta \circ f))(x \otimes y) \\ &= (\beta \circ f)m(x \otimes y) \\ &= (\beta \circ f)(xy) \end{aligned}$$

Agora, usando o fato que ψ é um monomorfismo, segue que $(f^\circ \otimes f^\circ)\Delta_{B^\circ} = \Delta_{A^\circ} f^\circ$ e o primeiro diagrama comuta. Isto finaliza nossa demonstração. □

Finalizaremos esta seção discutindo relações entre a estrutura de uma álgebra e de sua coálgebra dual.

Proposição 2.3.9. *Seja A uma álgebra sobre um corpo $\Bbbk$. Então:*

(i) Se B é uma subálgebra de A, então $B^\perp \cap A^\circ$ é um coideal da coálgebra dual A°.

(ii) Se I é um coideal da coálgebra dual A°, então $I^\perp$ é uma subálgebra de A.

Demonstração. (i) Seja $\iota : B \to A$ a inclusão de espaços vetoriais. Como B é uma subálgebra de A, segue que ι é um morfismo de álgebras. Assim, obtemos da Proposição 2.3.8 que $\iota^\circ A^\circ \to B^\circ$ é um morfismo de coálgebras. Note agora que

$$\begin{aligned} \mathcal{N}uc\,\iota^\circ &= \{f \in A^\circ : \iota^\circ(f) \\ &= 0\} = \{f \in A^\circ : f \circ \iota = 0\} \\ &= \{f \in A^\circ : f(B) = 0\} \\ &= A^\circ \cap B^\perp \end{aligned}$$

e segue que $A^\circ \cap B^\perp$ é um ideal de A, por ser o núcleo de um morfismo de álgebras.

(ii) Sejam $f \in I \subseteq A^\circ$ e $a, b \in I^\perp \subseteq A$. Como I é um coideal de A°, segue que $\Delta(f) = \sum_{(f(c))} f_1 \otimes f_2 \in A^\circ \otimes I + I \otimes A^\circ$. Mas então, $f(ab) = \sum f_1(a) f_2(b) = 0$, de modo que $ab \in I^\perp$. Além disso, como I é um coideal de A° segue que $0 = \varepsilon_{A^\circ}(f) = f(1)$, para todo $f \in I$, de modo que $1 \in I^\perp$. Portanto, $I^\perp$ é uma subálgebra de A. □

Com uma argumentação semelhante, podemos mostrar mais alguns resultados sobre a relação das estruturas de álgebras e coálgebras duais. Por este motivo apenas enunciaremos tais resultados aqui. Para uma demonstração com detalhes, citamos [4]

Proposição 2.3.10. *Mantendo as notações acima, temos:*

(1) *Seja C uma coálgebra e C^* sua álgebra dual. Então:*

(i) Se I é um ideal à esquerda (respectivamente, á direita) de C^*, então $I^\perp$ é um coideal à esquerda (resp., à direita) de C.

(ii) Se D é um coideal à esquerda (respectivamente, à direita) de C, então $D^\perp$ é um ideal è esquerda (resp., à direita) de C^*.

(2) *Seja A uma álgebra e A° sua coálgebra dual. Então:*

(i) Se I é um ideal à esquerda (resp., à direita) de A, então $I^{\perp} \cap A^{\circ}$ é um coideal à esquerda (resp., à direita) de A°.

(ii) Se D é um coideal à esquerda (resp., à direita) de A°, então $D^{\perp}$ é um ideal à esquerda (resp., à direita) de A.

2.4 Biálgebras

Estudamos espaços vetoriais que possuem uma estrutura de álgebra e de coálgebra. Queremos agora investigar espaços vetoriais que possuem ambas as estruturas de álgebra e de coálgebra, de modo que exista entre elas alguma espécie de compatibilidade a fim de conferir uma nova estrutura a estes espaços vetoriais, as quais serão chamadas de biálgebras. Esta compatibilidade se dará através de morfismos como veremos adiante. Discutiremos algumas propriedades destas estruturas.

Proposição 2.4.1. *Seja H um $\Bbbk$-espaço vetorial munido de uma estrutura de álgebra, dada por (H, m, u), e de uma estrutura de coálgebra, dada por (H, Δ, ε). As seguintes afirmações são equivalentes:*

(i) Δ e ε são morfismos de álgebras.

(ii) m e u são morfismos de coálgebras.

Demonstração. Lembramos que nas hipóteses da Proposição, $H \otimes H$ possui estruturas de álgebra e de coálgebra. Suponhamos que $\Delta : H \to H \otimes H$ e $\varepsilon : H \to \Bbbk$ são morfismos de álgebras. Então, se $h, g \in H$, temos que $\Delta(hg) = \Delta(h)\Delta(g) = \sum_{(h)(g)} h_1 g_1 \otimes h_2 g_2$ e $\varepsilon(hg) = \varepsilon(h)\varepsilon(g)$. Consideremos agora $m : H \otimes H \to H$ e $u : \Bbbk \to H$ os morfismos multiplicação e unidade, respectivamente. Portanto, se $g, h \in H$, temos

$$\begin{aligned}
((m \otimes m) \circ \Delta_{H\otimes H})(h \otimes g) &= (m \otimes m)(\sum_{(h)(g)} h_1 g_1 \otimes h_2 g_2) \\
&= \sum_{(h)(g)} h_1 g_1 h_2 g_2 \\
&= \sum_{(h)(g)} (hg)_1 \otimes (hg)_2 \\
&= \Delta(hg) \\
&= \Delta(m(h \otimes g)) \\
&= \Delta \circ m(h \otimes g)
\end{aligned}$$

e

$$\varepsilon_{H\otimes H}(h \otimes g) = \varepsilon(h)\varepsilon(g) = \varepsilon(hg) = \varepsilon(m(h \otimes g)) = \varepsilon \circ m(h \otimes g)$$

e segue que m é um morfismo de coálgebras. Analogamente,

$$\Delta \circ u(1_{\Bbbk}) = \Delta(1_H) = 1_H \otimes 1_H = u(1_{\Bbbk}) \otimes u(1_{\Bbbk}) = (u \otimes u)(1_{\Bbbk} \otimes 1_{\Bbbk}) = (u \otimes u) \circ \Delta_A \Bbbk(1_{\Bbbk})$$

e

$$\varepsilon_{\Bbbk}(1_{\Bbbk}) = 1_{\Bbbk} = \varepsilon(1_H) = \varepsilon(u(1_{\Bbbk})) = \varepsilon \circ u(1_{\Bbbk})$$

e obtemos que u é um morfismo de coálgebras. Isto mostra $(i) \Rightarrow (ii)$.

A recíproca é mostrada de forma análoga e será deixada ao leitor. □

O resultado acima induz a seguinte definição.

Definição 2.4.2. *Seja $H = (H, m, u, \Delta, \varepsilon)$ um espaço vetorial sobre um corpo $\Bbbk$ munido de estrutura de álgebra (H, m, u) e de uma estrutura de coálgebra (H, Δ, ε). Dizemos que H é uma biálgebra se Δ e ε são morfismos de álgebras (ou, equivalentemente, se m e u são morfismos de coálgebras).*

Exemplo 2.4.3. (**1**). *A álgebra de grupo $\Bbbk G$, com estrutura usual de álgebra e com estrutura de coálgebra dada por $\Delta : \Bbbk G \to \Bbbk \otimes \Bbbk G$, induzida por $\Delta(g) = g \otimes g$, e $\varepsilon : \Bbbk G \to \Bbbk$, induzida por $\varepsilon(g) = 1$ é uma biálgebra, como é fácil verificar.*

(**2**). *O anel de polinômios $\Bbbk[X]$, com estrutura usual de álgebra e com a estrutura de coálgebra dada por*

$$\Delta(X) = X \otimes X \quad e \quad \varepsilon(X) = 1$$

é uma biálgebra.

(**3**). *O anel de polinômios $\Bbbk[X]$, com estrutura usual de álgebra e com a estrutura de coálgebra dada por*

$$\Delta(X) = X \otimes 1 + 1 \otimes X \quad e \quad \varepsilon(X) = 0$$

é uma biálgebra.

Uma questão interessante é a seguinte: Seja H um $\Bbbk$-espaço vetorial munido de uma estrutura de álgebra. Será que sempre podemos introduzir uma estrutura de coálgebra em H de modo que H se torne uma biálgebra? A resposta para esta pergunta é negativa, pois se uma álgebra H possuir uma estrutura de biálgebra, então o morfismo counidade $\varepsilon : H \to \Bbbk$ será um morfismo de álgebra e, consequentemente, seu núcleo será um ideal (bilateral) de H. Se H for tomada uma álgebra simples, então não haverá em H ideais diferentes de 0 e H, impossibilitando a existência de uma tal aplicação ε. Este é o caso das álgebras de matrizes sobre corpos, por exemplo.

Observe que todo espaço vetorial tem uma estrutura de coálgebra. O que estamos afirmando acima é que, em certos casos, nenhuma estrutura de coálgebra pode ser compatível

com qualquer estrutura de álgebra que possa existir no espaço vetorial considerado.

Seja $H = (H, m, u, \Delta, \varepsilon)$ uma biálgebra. Combinando a estrutura oposta da álgebra H e a estrutura cooposta da coálgebra H, podemos associar as seguintes biálgebras à biálgebra H:

$$H^{op} := (H, m^{op}, u, \Delta, \varepsilon), \quad H^{cop} := (H, m, u, \Delta^{cop}, \varepsilon) \quad \text{e} \quad H^{op\,cop} := (H, m^{op}, u, \Delta^{cop}, \varepsilon)$$

Definição 2.4.4. *Com as notações acima, chamaremos de biálgebra oposta de H a biálgebra $H^{op\,cop}$.*

Ao estudarmos a estrutura de uma biálgebra, podemos considerar apenas a estrututra de álgebra ou de coálgebra, mas também podemos olhar para aquelas estruturas derivadas simultaneamente destas duas estruturas contidas na biálgebra. Neste sentido, temos

Definição 2.4.5. *Sejam H uma biálgebra e A um subespaço vetorial de H. Dizemos que A é uma subbiálgebra de H, se A for simultaneamente uma subálgebra e uma subcoálgebra de H.*

Seja H uma biálgebra. Como a interseção de uma família de subálgebras é uma subálgebra e a interseção d uma família de subcoálgebras é novamente uma coálgebra, podemos definir a subbiálgebra gerada por um subconjunto de H, como sendo a menor subbiálgebra contendo este conjunto.

Definição 2.4.6. *Sejam H e H' biálgebras e $f : H \to H'$ uma aplicação $\Bbbk$-linear. Dizemos que f é um homomorfismo de biálgebras se f for um homomorfismo de álgebras e, simultaneamente, um homomorfismo de coálgebras. Além disso, f é dito um isomorfismo, se f for bijetora.*

Segue da definição acima que o núcleo de um homomorfismo de biálgebras é, simultaneamente, um ideal e um coideal de H. Isto induz a seguinte definição.

Definição 2.4.7. *Um biideal de uma biálgebra é um subespaço vetorial que possui uma estrutura de ideal e de coideal simultaneamente.*

Aproveitando o que se fez para álgebras e coálgebras, podemos enunciar um teorema de homomorfismo no contexto de biálgebras, o qual será apresentado aqui sem demonstração. Observamos que se I é um biideal de uma biálgebra H, então o quociente H/I possui estrutura tanto de álgebra como de coálgebra de modo que estas estruturas são compatíveis e, portanto, H/I é uma biálgebra. Mais precisamente, temos o seguinte resultado.

Proposição 2.4.8. *Sejam H uma biálgebra e I um biideal de H. Então:*

(i) Existe uma única estrutura de biálgebra em H/I de modo que a projeção canônica (linear) $\pi : H \to H/I$ seja um homomorfismo de biálgebras.

(ii) Se $f : H \to H'$ é um homomorfismo de biálgebras tal que $I \subseteq \mathcal{N}uc\, f$, então existe um único morfismo de biálgebras $\overline{f} : H/I \to H'$ tal que $\overline{f} \circ \pi = f$. Além disso, $\overline{f}$ é injetora se, e somente se, $\mathcal{N}uc\, f = I$.

Considerando agora o espaço dual de uma biálgebra H. Para evitar problemas com a finitude local, vamos nos restringir ao contexto de biálgebras de dimensão finita. Porém, o mesmo resultado vale se consideramos o dual finito, no caso de H ter dimensão infinita.

Proposição 2.4.9. *Seja H uma biálgebra de dimensão finita. Então o espaço dual H^* tem uma estrutura de biálgebra induzida pelas estruturas de álgebra e coálgebra duais.*

Demonstração. Seja $H = (H, m, u, \Delta, \varepsilon)$ uma biálgebra finito-dimensional. Então sabemos que (H^*, m^*, u^*) é uma coálgebra e $(H^*, \Delta^*, \varepsilon^*)$ é uma álgebra. O fato de H ser uma biálgebra nos diz que Δ e ε são morfismos de álgebras e que m e u são morfismos de coálgebras. Segue então de resultados vistos antes que m^* e u^* são morfismos de coálgebras e que Δ^* e ε^* são morfismos de álgebras. Portanto, H^* é uma biálgebra. □

Vamos analisar as representações de uma biálgebra. Em geral, se A é uma álgebra, então não podemos garantir que o produto tensorial de A-módulos seja um A-módulo. Este problema deixa de existir quando trabalhamos com uma biálgebra em lugar de uma álgebra, como veremos a seguir. Sejam H uma biálgebra e M e N dois H-módulos à esquerda. Então o produto tensorial $M \otimes_{\Bbbk} N$ também possui uma estrutura de H-módulo, via $\cdot : H \otimes (M \otimes N) \to (M \otimes N)$, dada por $h \cdot (m \otimes n) = \sum_{(h)} h_{(1)} \cdot m \otimes h_{(2)} \cdot n$. De fato, pois se $h, g \in H, m \in M$ e $n \in N$, temos

$$\begin{aligned} h \cdot (g \cdot (m \otimes n)) &= h \cdot (\sum_{(g)} g_1 \cdot m \otimes g_2 \cdot n) \\ &= \sum_{(h),(g)} (h_1 \cdot (g_1 \cdot m)) \otimes (h_2 \cdot (g_2 \cdot n)) \\ &= \sum_{(h),(g)} (h_1 g_1) \cdot m \otimes (h_2 g_2) \cdot n \\ &= \sum_{(h),(g)} (hg)_1 \cdot m \otimes (hg)_2 \cdot n \\ &= (hg) \cdot (m \otimes n) \end{aligned}$$

e

$$1_H \cdot (m \otimes n) = (1_H \cdot m) \otimes (1_H \cdot n) = m \otimes n$$

Note também que todo $\Bbbk$-espaço vetorial V possui uma estrutura de H-módulo via $\cdot : H \otimes V \to V$, dada por $h \cdot v = \varepsilon(h)v$, como é fácil verificar. Uma tal ação de H em V é dita *ação trivial* de H em V. Assim, se $V = \Bbbk$, temos que $\Bbbk$ é um H-módulo à esquerda. Como $\Bbbk$ é um corpo (então, comutativo), segue que H age via ε em V tanto à esquerda como à direita.

De fato é possível mostrar que a condição necessária para que $\Bbbk$ e o produto tensorial de módulos seja ainda um módulo sobre uma álgebra é justamente a existência de uma estrutura de biálgebra nesta álgebra. Isto será discutido na próxima seção.

2.5 Quando o produto tensorial de H-módulos é ainda um H-módulo?

Como dito no final da seção anterior, vamos procurar condições para que o corpo base e o produto tensorial de módulos sobre uma álgebra sejam módulos sobre esta mesma álgebra. Este problema tem uma importância no contexto da teoria de categorias, e quer dizer que procuramos condições sobre uma álgebra para que sua categoria de representações seja o que chamamos de uma *categoria monoidal*. No que segue, vamos ver que a exigência que devemos fazer é que exista uma estrutura de biálgebra nesta álgebra considerada.

Consideremos então uma $\Bbbk$-álgebra H e vamos supor que $\Bbbk$ é um H-módulo à esquerda e, além disso, se M e N são H-módulos à esquerda, então $M \otimes N$ também o é. Além disso, vamos supor que valem as propriedades $(M \otimes N) \otimes K \simeq M \otimes (N \otimes K)$ e $M \otimes \Bbbk \simeq M \simeq \Bbbk \otimes M$, para todos H-módulos à esquerda M, N e K, e que estes isomorfismos sejam os mesmos como transformações lineares de $\Bbbk$-espaços vetoriais, ou seja, estamos supondo que os isomorfismos acima sejam de fato igualdades. Discutiremos a seguir quais propriedades adicionais esta álgebra H deve possuir. Para tanto, consideremos $a : (M \otimes N) \otimes K \to M \otimes (N \otimes K)$ dado por $a((m \otimes n) \otimes k) = m \otimes (n \otimes k)$, $l : \Bbbk \otimes M \to M$ dado por $l(\alpha \otimes m) = \alpha m$ e $r : M \otimes \Bbbk \to M$ dado por $r(m \otimes \alpha) = m\alpha$ os isomorfismos acima.

Como H é um H-módulo via multiplicação, segue que $H \otimes H$ também é um H-módulo. Assim, podemos considerar a aplicação H-linear $\Delta : H \to H \otimes H$ dada por $\Delta(h) = h \cdot (1_H \otimes 1_H)$. Como $\Delta(h) \in H \otimes H$, podemos escrever o elemento $\Delta(h)$ como uma soma finita da forma $\Delta(h) = \sum_{i=1}^{n} h_{i_1} \otimes h_{i_2}$, onde $h_{i_1}, h_{i_2} \in H$. Para não carregar muito nossa notação, tal como fizemos antes com a notação de Sweedler, vamos escrever $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$.

Sejam M e N dois H-módulos. Vamos ver agora como está definida a ação de H sobre

$M \otimes N$ a partir da definição de Δ. Assim, dados $h \in H$, $m \in M$ e $n \in N$, queremos definir o elemento $h \cdot (m \otimes n) \in M \otimes N$. Para tal, consideremos as aplicações H-lineares $f_m : H \to M$ e $f_n : H \to N$ dadas por $f_m(h) = h \cdot m$ e $f_n(h) = h \cdot n$, respectivamente. Assim, a aplicação $f_m \otimes f_n : H \otimes H \to M \otimes N$ é também uma aplicação H-linear. Portanto, devemos ter

$$\begin{aligned} h \cdot (m \otimes n) &= h \cdot ((f_m \otimes f_n)(1_H \otimes 1_H)) \\ &= (f_m \otimes f_n)(h \cdot (1_H \otimes 1_H)) \\ &= (f_m \otimes f_n)(\Delta(h)) \\ &= (f_m \otimes f_n)(\sum_{(h)} h_{(1)} \otimes h_{(2)}) \\ &= \sum_{(h)} h_{(1)} \cdot m \otimes h_{(2)} \cdot n \end{aligned}$$

ou seja, a ação de H em $M \otimes N$ deve ser dada por

$$h \cdot (m \otimes n) = \sum_{(h)} h_{(1)} \cdot m \otimes h_{(2)} \cdot n.$$

Observemos agora que se $h \in H$, então $h \cdot (1_H \otimes (1_H \otimes 1_H)) = \sum_{(h)} h_{(1)} \cdot 1_H \otimes h_{(2)} \cdot (1_H \otimes 1_H) = \sum_{(h)} h_{(1)} \otimes \Delta(h_{(2)})$, pois $H \otimes (H \otimes H)$ é um H-módulo, uma vez que H e $H \otimes H$ o são. Por outro lado, usando o isomorfismo de associatividadde, também obtemos que

$$\begin{aligned} h \cdot (1_H \otimes (1_H \otimes 1_H)) &= h \cdot (a((1_H \otimes 1_H) \otimes 1_H)) \\ &= a(h \cdot ((1_H \otimes 1_H) \otimes 1_H)) = a(\sum_{(h)} h_{(1)} \cdot (1_H \otimes 1_H) \otimes h_{(2)} \cdot 1_H) \\ &= a(\Delta(h_{(1)}) \otimes h_{(2)}) \\ &= \Delta(h_{(1)}) \otimes h_{(2)} \end{aligned}$$

ou seja, devemos ter

$$\sum_{(h)} \Delta(h_{(1)}) \otimes h_{(2)} = \sum_{(h)} h_{(1)} \otimes \Delta(h_{(2)}), \forall h \in H$$

o que, dito de outra maneira, é equivalente a

$$(\Delta \otimes id_H) \circ \Delta = (id_H \otimes \Delta) \circ \Delta$$

Consideremos agora a aplicação H-linear $\varepsilon : H \to \Bbbk$, dada por $\varepsilon(h) = h \cdot 1_{\Bbbk}$, a qual está bem definida pois $\Bbbk$ é um H-módulo. Considerando agora a aplicação H-linear

$l_H : \Bbbk \otimes H \to H$ dada por $l_H(\alpha \otimes h) = \alpha h$, obtemos

$$\begin{aligned} h &= h1_h \\ &= hl_H(1_\Bbbk \otimes 1_H) \\ &= l_H(h \cdot (1_\Bbbk \otimes 1_H)) \\ &= l_H(\sum_{(h)} h_{(1)} \cdot 1_\Bbbk \otimes h_{(2)}1_H) \\ &= l_H\left(\sum_{(h)} \varepsilon(h_{(1)}) \otimes h_{(2)}\right) \\ &= \sum_{(h)} \varepsilon(h_{(1)})h_{(2)} \end{aligned}$$

De modo análogo, usando $r_H : H \otimes \Bbbk \to H$ definida por $r_H(h \otimes \alpha) = h\alpha$ em lugar de l_H, obtemos $h = \sum_{(h)} h_{(1)}\varepsilon(h_{(2)})$. Portanto, devemos ter

$$\sum_{(h)} \varepsilon(h_{(1)})h_{(2)} = h = \sum_{(h)} h_{(1)}\varepsilon(h_{(2)})$$

ou seja,

$$(\varepsilon \otimes id_H) \circ \Delta = id_H = (id_H \otimes \varepsilon) \circ \Delta$$

Visto que $H \otimes H$ é uma $\Bbbk$-álgebra via multiplicação dada por $(h \otimes g)(h' \otimes g') = hh' \otimes gg'$, segue que as aplicações Δ e ε acima consideradas são morfismos de álgebras. De fato, pois se $h, g \in H$, então temos

$$\begin{aligned} \Delta(hg) &= hg \cdot (1_H \otimes 1_H) \\ &= h \cdot (g \cdot (1_H \otimes 1_H)) \\ &= \sum_{(g)} h \cdot (g_{(1)} \otimes g_{(2)}) \\ &= \sum_{(g)(h)} h_{(1)}g_{(1)} \otimes h_{(2)}g_{(2)} \end{aligned}$$

e

$$\begin{aligned} \varepsilon(hg) &= hg \cdot 1_\Bbbk \\ &= h \cdot (g \cdot 1_\Bbbk) \\ &= h \cdot \varepsilon(g)1_\Bbbk \\ &= \varepsilon(h)\varepsilon(g) \end{aligned}$$

além do que, temos também $\Delta(1_H) = 1_H \cdot (1_H \otimes 1_H) = 1_H \otimes 1_H$ e $\varepsilon(1_H) = 1_H \cdot 1_\Bbbk = 1_\Bbbk$

como é fácil ver. Portanto, Δ e ε são morfismos de álgebras como afirmado.

Assim, são condições necessárias para que uma álgebra H admita o corpo $\Bbbk$ e o produto tensorial de seus módulos como H-módulos, a existência de dois morfismos de álgebra, a saber, $\Delta : H \to H \otimes H$ e $\varepsilon : H \to \Bbbk$ satisfazendo as seguintes condições:

$$(\Delta \otimes id_H) \circ \Delta = (id_H \otimes \Delta) \circ \Delta \qquad \text{e} \qquad (\varepsilon \otimes id_H) \circ \Delta = id_H = (id_H \otimes \varepsilon) \circ \Delta$$

Portanto, a argumentação acima produz o seguinte resultado.

Teorema 2.5.1. *Seja H uma $\Bbbk$-álgebra. As seguintes afirmações são equivalentes:*

(i) $\Bbbk$ e o produto tensorial $M \otimes_{\Bbbk} N$ são H-módulos à esquerda, para todos M, N H-módulos à esquerda.

(ii) H é uma biálgebra.

Capítulo 3

A Álgebra de convolução

Para introduzir o conceito de álgebra de Hopf, que será feito no p´roximo capítulo, vamos necessitar da estrutura de álgebra de convolução definida no espaço vetorial $Hom_{\Bbbk}(C, A)$, onde C é uma coálgebra e A é uma álgebra. Vamos introduzir este conceito no que segue e discutir algumas de suas propriedades básicas que nos serão úteis mais a frente. Tomando $A = \Bbbk$, temos que $Hom_{\Bbbk}(C, A) = Hom_{\Bbbk}(C, \Bbbk) = C^*$ e assim, o que vamos discutir aqui é uma generalização da álgebra dual da coálgebra C, num certo sentido.

3.1 O produto convolução

Sejam $A = (A, m, u)$ uma $\Bbbk$-álgebra e $C = (C, \Delta, \varepsilon)$ uma $\Bbbk$-coálgebra. Podemos então dotar o espaço vetorial $Hom_{\Bbbk}(C, A)$ de uma estrutura de álgebra, definindo a multiplicação da seguinte forma

$$f * g = m \circ (f \otimes g) \circ \Delta, \, \forall f, g \in Hom_{\Bbbk}(C, A)$$

Note que se $c \in C$ e $f, g \in Hom_{\Bbbk}(C, A)$, então

$$c \longrightarrow^{\Delta} \sum_{(c)} c_1 \otimes c_2 \xrightarrow{f \otimes g} \sum_{(c)} f(c_1) \otimes g(c_2) \xrightarrow{m} \sum_{(c)} f(c_1) g(c_2)$$

ou seja, $(f * g)(c) = \sum_{(c)} f(c_1) g(c_2)$.

É fácil verificar que a coassociatividade de Δ implica na associatividade da multiplicação acima definida. Além disso, $u \circ \varepsilon$ é o elemento unidade desta multiplicação. De

fato, pois se $f \in Hom_{\Bbbk}(C, A)$, $c \in C$, então

$$\begin{aligned}((u \circ \varepsilon) * f)(c) &= \sum_{(c)} u \circ \varepsilon(c_{(1)}) f(c_{(2)}) \\ &= \sum_{(c)} \varepsilon(c_{(1)}) f(c_{(2)}) \\ &= f\left(\sum_{(c)} \varepsilon(c_{(1)}) c_{(2)}\right) \\ &= f(c)\end{aligned}$$

ou seja, $(u \circ \varepsilon) * f = f$. De modo análogo se mostra que $f = f * (u \circ \varepsilon)$. Assim, temos a seguinte definição.

Definição 3.1.1. *A álgebra $(Hom_{\Bbbk}(C, A), *, u \circ \varepsilon)$ definida acima é chamada de álgebra de convolução de C e A. A multiplicação $*$ desta álgebra é chamado de produto convolução.*

Note que se $A = \Bbbk$, então a álgebra de convolução $Hom_{\Bbbk}(C, \Bbbk)$ nada mais é do que a álgerba dual C^* da coálgebra C. Além disso, se $C = \Bbbk$, então a álgebra de convolução $Hom_{\Bbbk}(\Bbbk, A) \simeq A$.

Exemplo 3.1.2. *Seja $C = \Bbbk[S]$ a coálgebra grouplike e A uma álgebra qualquer. Então a álgebra de convolução $Hom_{\Bbbk}(C, A)$ é isomorfa a álgebra das funções de S em A com operações pontuais.*

Exemplo 3.1.3. *Seja $C = C_n(\Bbbk)$ a coálgebra de matrizes. Então a a álgebra de convolução $Hom_{\Bbbk}(C, A)$ é isomorfa a álgebra de matrizes sobre A.*

3.2 Inversas convolutivas

Nesta seção vamos discutir algumas propriedades das inversas convolutivas que nos serão úteis no decorrer do texto.

Consideremos agora A, B álgebras e C, D coálgebras. Vamos definir as seguintes aplicações

$$\begin{array}{rccc} \pi^* : & Hom_{\Bbbk}(D, A) & \to & Hom_{\Bbbk}(C, A) \\ & f & \mapsto & f \circ \pi \end{array}$$

e

$$\begin{array}{rccc} \iota_* : & Hom_{\Bbbk}(C, A) & \to & Hom_{\Bbbk}(C, B) \\ & f & \mapsto & \iota \circ f \end{array}$$

Afirmamos que estas aplicações são morfismos de álgebras. De fato, pois se $f, g \in$

$Hom_{\Bbbk}(D, A)$ e $c \in C$, então

$$(\pi^*(f*g))(c) = f*g(\pi(c)) = \sum_{(c)}(f\circ\pi(c_{(1)}))(g\circ\pi(c_{(2)})) = \sum_{(c)}(\pi^*(f))(C_{(1)})(\pi^*(g)(c_{(2)})) = (\pi^*(f))*(\pi^*($$

e

$$\pi^*(\nu_A \circ \varepsilon_D) = (\nu_A \circ \varepsilon_D) \circ \pi = \nu_A \circ (\varepsilon_D \circ \pi) = \nu_A \circ \varepsilon_C$$

ou seja, $\pi^*(f * g) = (\pi^*(f)) * (\pi^*(g))$ e $\pi^*(1_{Hom_{\Bbbk}(D,A)}) = (1_{Hom_{\Bbbk}(C,A)})$. De modo análogo se mostra que $\iota_*(f * g) = (\iota_*(f)) * (\iota_*(g))$ e $\iota_*(1_{Hom_{\Bbbk}(C,A)}) = (1_{Hom_{\Bbbk}(C,B)})$. Com estas notações, podemos mostrar os seguintes resultados que serão úteis mais a frente.

Lema 3.2.1. *Sejam C uma biálgebra e A uma álgebra. Suponhamos que $f \in Hom_{\Bbbk}(C, A)$ possui uma inversa convolutiva f^{-1} em $Hom_{\Bbbk}(C, A)$. Então:*

(i) Se $f : C \to A$ é um morfismo de álgebras, então $f^{-1} : C \to A^{op}$ é um morfismo de álgebras;

(ii) Se $f : C \to A^{op}$ é um morfismo de álgebras, então $f^{-1} : C \to A$ é um morfismo de álgebras.

Demonstração. Observemos inicialmente que $(i) \Leftrightarrow (ii)$. Assim, basta mostrarmos o item (i). Seja $D = C \otimes C$ a coálgebra produto tensorial, cuja estrutura é dada por $\Delta_D(x \otimes y) = \sum_{(x),(y)}(x_{(1)} \otimes y_{(1)}) \otimes (x_{(2)} \otimes y_{(2)})$ e $\varepsilon_D(x \otimes y) = \varepsilon_C(x)\varepsilon_C(y)$, onde $\Delta_C(x) = \sum_{(x),(y)} x_{(1)} \otimes x_{(2)}$ e $\Delta_C(y) = \sum_{(y)} y_{(1)} \otimes y_{(2)}$. Como C é uma biálgebra, segue que a multiplicção $\mu_C : C \otimes C \to C$ é um morfismo de coálgebras, de onde segue que μ_C^* é um morfismo de álgebras, pela observação feita acima. Assim, $\mu^*(f)$ possui uma inversa convolutiva em $Hom_{\Bbbk}(D, A)$, a saber, $\mu^*(f^{-1})$.

Consideremos agora a aplicação $h : C \otimes C \to A$ dada por $h(x \otimes y) = f^{-1}(y)f^{-1}(x)$. Vamos mostrar que h também é uma inversa convolutiva de $\mu^*(f)$ em $Hom_{\Bbbk}(D, A)$, para obtermos que $h = \mu^*(f^{-1})$. De fato, pois se $x \otimes y \in D$, ntão temos

$$\begin{aligned}
(h * \mu^*(f))(x \otimes y) &= \sum h(x_1 \otimes y_1)f(\mu(x_2 \otimes y_2)) \\
&= \sum h(x_1 \otimes y_1)f(x_2y_2) \\
&= \sum f^{-1}(y_1)f^{-1}(x_1)f(x_2)f(y_2) \\
&= \sum f^{-1}(y_1)\varepsilon(x)f(y_2) \\
&= \varepsilon(x)\varepsilon(y) \\
&= \varepsilon_D(x \otimes y)
\end{aligned}$$

Analogamente, mostramos que $\mu^*(f) * h = \varepsilon_D$. Logo, h e $\mu^*(f^{-1})$ são inversas convo-

lutivas de $\mu^*(f)$. Portanto,

$$f^{-1} \circ \mu_C = \mu_C^*(f^{-1}) = h$$

de onde obtemos que se $x, y \in C$, então

$$f^{-1}(xy) = (f^{-1} \circ \mu_C)(x \otimes y) = h(x \otimes y) = f^{-1}(y)f^{-1}(x) = f^{-1}(x).{}_{op}f^{-1}(y)$$

ou seja, $f^{-1} : C \to A^{op}$ é um morfismo de álgebras. □

Proposição 3.2.2. *Sejam A uma biálgebra e C uma coálgebra. Suponha que $f \in Hom_{\Bbbk}(C, A)$ possui uma inversa convolutiva f^{-1}. Então:*

(i) Se $f : C \to A$ é um morfismo de coálgebras, então $f^{-1} : C \to A^{cop}$ é um morfismo de coálgebras.

(ii) $f : C \to A^{cop}$ é um morfismo de coálgebras de C em A^{op}, então $f^{-1} : C \to A$ é um morfismo de coálgebras.

Demonstração. Segue de uma argumentação análoga, usando que $\Delta_A : A \to A \otimes A$ é um morfismo de álgebras. □

Gostaríamos de observar neste momento que se A e B são álgebras e $f : A \to B^{op}$ é um morfismo de álgebra, então dizemos que $f : A \to B$ é um *anti-morfismo* de álgebras. O mesmo se diz de *anti-morfismos* de coálgebras.

Capítulo 4

Álgebras de Hopf

Chegamos ao momento em que podemos introduzir o conceito de álgebras de Hopf. Veremos adiante que uma álgebra de Hopf é uma biálgebra com uma estrutura adicional dada por um antimorfismo de álgebras que faz o papel da inversa na álgebra de grupo. Este antimorfismo é chamado de antípoda. Começaremos este capítulo introduzindo a noção de antípoda para então definirmos o que seria uma álgebra de Hopf. Na sequência, estudaremos algumas propriedades básicas da antípoda.

4.1 Biálgebras com antípodas

Lembramos que uma biálgebra possui uma estrutura tanto de álgebra como de coálgebra. Assim, se H é uma biálgebra, então o espaço $End_{\Bbbk}(H)$ possui uma estrutura de álgebra de convolução. Para introduzir o conceito de antípoda em H, vamos precisar da estrutura convolutiva de $End_{\Bbbk}(H)$.

Definição 4.1.1. *Seja $H = (H, \mu, \nu, \Delta, \varepsilon)$ uma biálgebra sobre um corpo $\Bbbk$. Uma aplicação $\Bbbk$-linear $S : H \to H$ é dita uma antípoda de H, se $\mu\circ(id_H \otimes S)\circ\Delta = \nu\circ\varepsilon = \mu(S\otimes id_H)\circ\Delta$, ou seja, S é uma inversa convolutiva de id_H na álgebra de convolução $End_{\Bbbk}(H)$.*

Note que a condição $\mu \circ (id_H \otimes S) \circ \Delta = \nu \circ \varepsilon = \mu(S \otimes id_H) \circ \Delta$, quando escrita em notação de Sweedler, significa que $\sum_{(h)} h_1 S(h_2) = \varepsilon(h) = \sum_{(h)} S(h_1)h_2$, para todo $h \in H$.

Segue imediatamente da definição que uma antípoda, quando existe, está unicamente determinada, por se tratar de um inverso de um elemento em uma determinada álgebra. Além disso, segue dos resultados já vistos anteriormente que se $S \in End_{\Bbbk}(H)$ é a antípoda de H, então S é um antimorfismo de álgebra e um antimorfismo de coálgebras. assim, se $g, h \in H$, então:

- $S(gh) = S(h)S(g)$,

- $\Delta(S(h)) = \sum_{(h)} S(h_2) \otimes S(h_1)$.

Exemplo 4.1.2. *(1) Seja G um grupo. Então $H = \Bbbk G$ é uma biálgebra com antípoda $SH \to H$ definida por $S(g) = g^{-1}$ e estendido ppor linearidade.*

(2) Considere o anel de polinômios $H = \Bbbk[X]$ com estrututra de biálgebra dada por $\Delta(X) = 1 \otimes X + X \otimes 1$ e $\varepsilon(X) = 0$. Então se $S : H \to H$ é uma antípoda de H, devemos ter $0 = \varepsilon(X) = (id)_H \otimes S)\Delta(X) = (id_H \otimes S)(1 \otimes X + X \otimes 1) = S(X) + XS(1)$. Como $S(1) = 1$, segue que devemos ter $S(X) = -X$. Então a aplicação linear $S : H \to H$ definida por $S(1) = 1$ e $S(X) = -X$ é a antípoda de H.

(3) Antípoda para a álgebra de Sweedler. Fazer as contas de que esta é uma biálgebra nas seções correspondentes anteriores e tomar este como um exemplo construido aos poucos.

Nem toda biálgebra possui uma antípoda, como mostra o próximo exemplo.

Exemplo 4.1.3. *Seja $H = \Bbbk[X]$ o anel de polinômios com estrutura usual de álgebra e com estrutura de coálgebra dada por $\Delta(X) = X \otimes X$ e $\varepsilon(X) = 1$. Sabemos que H é uma biálgebra. Afirmamos que esta biálgebra não possui nenhuma antípoda. De fato, pois se $S : H \to H$ é uma tal antípoda, então deveríamos ter $1 = \varepsilon(X) = (id_H \otimes S)\Delta(X) = XS(X)$, o que é impossível, pois o elemento X não possui inverso no anel de polinômios.*

Definição 4.1.4. *Uma álgebra de Hopf é uma biálgebra munida de uma antípoda.*

Já vimos antes alguns exemplos de álgebras de Hopf (biálgebras com antípoda) e que nem todo biálgebra é uma álgebra de Hopf.

Exemplo 4.1.5. *Dar alguns exemplos mais de álgebras de Hopf. Por exemplo, a Taft, alguma envolvente de álgebras de Lie (?).*

Como toda álgebra de Hopf é uma biálgebra, então sabemos que tanto $\Bbbk$ como o produto tensorial $M \otimes_{\Bbbk} N$ de H-módulos são também H-módulos. O que difere uma álgebra de Hopf de uma biálgebra é a existência da antípoda, e esta aplicação é responsável pelo fato de o dual linear de um H-módulo ser também um H-módulo, como mostra o próximo resultado.

Proposição 4.1.6. *Sejam H uma álgebra de Hopf com antípoda $S : H \to H$, M um H-módulo à esquerda e $M^* := Hom_{\Bbbk}(M, \Bbbk)$ seu dual linear. Então M^* é um H-módulo à esquerda via a ação $h \triangleright \varphi := \varphi(S(h) \triangleright \_)$, para $h \in H$, $\varphi \in M^*$.*

Demonstração. Consideremos a aplicação $\Bbbk$-linear $\triangleright : H \times M^* \to M^*$, definida por $h \triangleright \varphi := \varphi(S(h) \triangleright \_)$, para todos $h \in H$ e $\varphi \in M^*$. Afirmamos que esta aplicação define uma ação

de H em M^* à esquerda. De fato, pois se $h, g \in H$, $\varphi \in M^*$ e $m \in M$, então temos

$$\begin{aligned}(h \cdot (g \cdot \varphi))(m) &= (g \cdot \varphi)(S(h) \cdot m) \\ &= \varphi(S(g) \cdot (S(h) \cdot m)) \\ &= \varphi(S(g)S(h) \cdot m) \\ &= \varphi(S(hg) \cdot m) \\ &= (hg \cdot \varphi)(m)\end{aligned}$$

de onde segue que $h \cdot (g \cdot \varphi) = hg \cdot \varphi$. Claramente se Vê que $1_H \triangleright \varphi = \varphi$, para todo $\varphi \in M^*$, pois $S(1_H) = 1_H$. Isto finaliza nossa demonstração. □

Uma consequência do fato de a antípoda S ser um anti-morfismo de coálgebras é o seguinte.

Proposição 4.1.7. *Seja H uma álgebra de Hopf com antípoda S. Então $\varepsilon \circ S = \varepsilon$.*

Demonstração. Basta observar que se $h \in H$ então

$$\begin{aligned}\varepsilon(h) = \varepsilon(h)1_{\Bbbk} = \varepsilon(h)\varepsilon(1_H) &= \varepsilon(\sum_{(h)} h_1 S(h_2)) && (4.1)\\ &= \sum_{(h)} \varepsilon(h_1)\varepsilon(S(h_2)) && (4.2)\\ &= \sum_{(h)} \varepsilon \circ S(\varepsilon(h_1)h_2) && (4.3)\\ &= \varepsilon \circ S(\sum_{(h)} \varepsilon(h_1)h_2) && (4.4)\\ &= \varepsilon \circ S(h) && (4.5)\end{aligned}$$

□

O resultado acima pode ser generalizado da seguinte forma.

Proposição 4.1.8. *Seja H uma álgebra de Hopf com antípod S.*

(i) Se A é uma álgebra e $f \in Hom_{\Bbbk}(H, A)$ é um morfismo de álgebras, então f possui uma inversa convolutiva dada por $f \circ S$.

(ii) Se C é uma coálgebra e $f \in Hom_{\Bbbk}(C, H)$ é um morfismo de coálgebras, então f possui uma inversa convolutiva dada por $S \circ f$.

(iii) Se H' é uma álgebra de Hopf com antípoda $S' e f \in Hom_{\Bbbk}(H, H')$ é um morfismo de biálgebras, então devemos ter $f \circ S = S' \circ f$.

Demonstração. (i) Como id_H é a inversa convolutiva de S em $End_{\Bbbk}(H)$ e $f : H \to A$ é um morfismo de álgebras, considerando $f_* : Hom(H, H) \to Hom(H, A)$. E segue então que $f_*(id_H)$ e $f_*(S)$ são inversas convolutivas uma da outra em $Hom(H, A)$, ou seja, f e $f \circ S$ são inversas convolutivas uma da outra em $Hom(H, A)$, como queríamos mostrar.

(ii) Considerando agora $f^* : End(H) \to Hom(C, H)$, obtemos que $f^*(id_H)$ e $f^*(S)$ são inversas convolutivas uma da outra em $Hom(C, H)$. Portanto, f e $S \circ f$ são inversas convolutivas uma da outra em $Hom(C, A)$.

(iii) Da parte (i), concluimos que $f \circ S$ é uma inversa convolutiva de f em $Hom(H, H')$, e da parte (ii), concluimos que $S' \circ f$ é uma inversa convolutiva de f em $Hom(H, H')$. Portanto, devemos ter $f \circ S = S' \circ f$. □

O resultado acima induz a seguinte definição.

Definição 4.1.9. *Sejam H e H' álgebras de Hopf com antípodas S e S', respectivamente. Uma aplicação $\Bbbk$-linear $f : H \to H'$ é dita um homomorfismo de álgebras de Hopf, se f é um homomorfismo de biálgebras tal que $f \circ S = S' \circ f$.*

Assim, segue que todo morfismo de biálgebras entre duas álgebras de Hopf é um morfismo de álgebras de Hopf, ou seja, todo morfismo de biálgebras entre álgebras de Hopf respeita as antípodas.

Definição 4.1.10. *Sejam H uma álgebra de Hopf com antípoda S e A uma subbiálgebra de H. Dizemos que A é uma subálgebra de Hopf de H, se $S(A) \subseteq A$.*

Esta definição tem as seguintes consequências imediatas.

- Se $f : H \to H'$ é um morfismo de álgebras de Hopf e A é uma subálgebra de Hopf de H, então $f(A)$ é uma subalgebra de Hopf de H', pois segue dos resultados anteriores que $S'(f(A)) = S(f(A)) \subseteq f(A)$.

- Como a interseção de biálgebras é uma biálgebra, a interseção de subálgebras de Hopf de H também é uma subálgebra de Hopf de H. Podemos assim definir, como usualmente fazemos, a subálgebra de Hopf de H gerada por um $\Bbbk$-subespaço V de H, como sendo a interseção de todas as subálgebras de Hopf de H que contém V.

Definição 4.1.11. *Sejam H uma álgebra de Hopf com antípoda H e I um biideal de H. Dizemos que I é um ideal de Hopf se $S(I) \subseteq I$.*

Note que se $f : H \to H'$ é um morfismo de álgebras de Hopf, então $\mathcal{N}uc\, f$ é um ideal de Hopf, pois se $x \in \mathcal{N}uc\, f$, então

$$0 = S' \circ f(x) = f \circ S(x)$$

de onde segue que $S(x) \in \mathcal{N}uc\, f$, ou seja, $S(\mathcal{N}uc\, f) \subseteq \mathcal{N}uc\, f$. Além disso, repetindo-se uma argumentação feita antes, pode-se mostrar que se I é um ideal de Hopf de H, então existe uma única estrutura de álgebra de Hopf em H/I tal que a projeção canônica $\pi : H \to H/I$ é um morfismo de álgebras de Hopf e vale um teorema de homomorfismos para álgebras de Hopf. Deixamos para o leitor a tarefa de enunciar um tal teorema e demonstrá-lo.

4.2 Algumas propriedades da antípoda

Vamos discutir agora algumas propriedades da antípoda. Começamos por considerar H uma álgebra de Hopf com antípoda S. Afirmamos que o conjunto $G(H) = \{g \in H : g \text{ é elemento group-like }\}$ é um subgrupo do grupo multiplicativo $(H, \cdot)$. De fato, pois $1 \in G(H)$, visto que $\Delta(1) = 1 \otimes 1$ pois Δ é um morfismo de álgebras e dado $g \in G(H)$, devemos ter $\Delta(g) = g \otimes g$, de onde segue que $gS(g) = \varepsilon(g) = 1$, ou seja, $S(g) = g^{-1}$ e temos que todo elemento group-like é invertível em H. Portanto, $G(H)$ é um subgrupo multiplicativo de H.

Dados $g, h \in G(H)$, consideremos um elemento (g, h)-primitivo. Então $\Delta(x) = g \otimes x + x \otimes h$, de onde concluímos que $\Delta(S(x)) = \sum_{(S(x))} S(x)_1 \otimes S(x)_2 = \sum_{(x)} S(x_2) \otimes S(x_1) = S(x) \otimes S(g) + S(h) \otimes S(x) = h^{-1} \otimes S(x) + S(x) \otimes g^{-1}$ e segue que $S(x)$ é um elemento (h^{-1}, g^{-1})-primitivo. Logo, S leva elementos skew primitivos em elementos skew primitivos. Mais precisamente, como $\varepsilon(x) = 0$, para todo elemento skew primitivo, segue da propriedade da counidade que $0 = \varepsilon(x) = (\varepsilon \otimes id_H)\Delta(S(x)) = gS(x) + xh^{-1}$, ou seja, devemos ter $S(x) = -g^{-1}xh^{-1}$. Assim, denotando o conjunto dos elementos (g, h)-primitivos por $P_{g,h}(H)$, é fácil ver que $P_{g,h}(H)$ é um subespaço vetorial de H e temos que a restrição de S a este subespaço é dada por $S(\_) := -g^{-1}\_h^{-1}$, de onde segue que $S_{|P_{g,h}} : P_{g,h}(H) \to P_{h^{-1},g^{-1}}(H)$ é uma aplicação linear bijetiva com inversa dada por $S_{|P_{g^{-1},h^{-1}}} : P_{g^{-1},h^{-1}}(H) \to P_{g,h}(H)$, uma vez que g, h foram tomados arbitrários na argumentação acima.

Como S é um anti-morfismo de álgebras e um antimorfismo de coálgebras, segue que $S : H \to H^{op}$ é um morfismo de álgebras e $S : H \to H^{cop}$ é um morfismo de coálgebras. Assim, $H^{op\,cop}$ também é uma álgebra de Hopf com antípoda S. De fato, pois se $h \in H = H^{op\,cop}$, temos

$$\begin{aligned}
\varepsilon(h) &= \sum_{(h)} S(h_1)h_2 \\
&= m^{op}(h_2 \otimes S(h_1)) \\
&= m^{op}(id_H \otimes S)(h_2 \otimes h_1) \\
&= m^{op}(id_H \otimes S)\Delta^{cop}(h)
\end{aligned}$$

de modo análogo se mostra que $m^{op}(S \otimes id_H)\Delta^{cop}(h) = \varepsilon(h)1_H$, ou seja, $m^{op}(id_H \otimes S)\Delta^{cop} = u \circ \varepsilon = m^{op}(S \otimes id_H)\Delta^{cop}$ e S é a inversa convolutiva de id_H na álgebra de convolução $End_{\Bbbk}(H^{op\,cop})$. Porém, note que tanto H^{op} como H^{cop} poderiam não ser álgebras de Hopf. O próximo resultado nos diz que examinando a antípoda de H sabemos dizer quando estas álgebras são de fato álgebras de Hopf.

Proposição 4.2.1. *Seja H uma álgebra de Hopf com antípoda S. Então as seguintes afirmações são equivalentes:*

(i) H^{op} é uma álgebra de Hopf.

(ii) H^{cop} é uma álgebra de Hopf.

(iii) S é bijetiva.

Além disso, se S é bijetiva, então S^{-1} é a antípoda de ambas as álgebras de Hopf H^{op} e H^{cop}.

Demonstração. Primeiro observamos que $H^{op} = (H^{cop})^{op\,cop}$ e $H^{cop} = (H^{op})^{op\,cop}$. A observação acima então nos diz que (i) e (ii) são equivalentes. Assim, vamos mostrar $(i) \Leftrightarrow (iii)$.

$(i) \Rightarrow (iii)$ Suponhamos que H^{op} é uma álgebra de Hopf com antípoda T. Neste caso, temos $\varepsilon(h)1_H = m^{op}(id_H \otimes T)\Delta(h) = \sum_{(h)} h_2T(h_1)$, ou seja, $\varepsilon(h) = \sum_{(h)} h_2T(h_1)$ em H. Aplicando agora S em ambos os lados desta igualdade, chegamos a $S(\varepsilon(h)) = \sum_{(h)} S(h_2T(h_1)) = \sum_{(h)}(S \circ T)(h_1)S(h_2)$, pois S é um antimorfismo de álgebras. Como $S \circ \varepsilon = \varepsilon$, segue que $S * S \circ T = u \circ \varepsilon$ em $End_{\Bbbk}(H)$. Analogamente se mostra que $(S \circ T) * S = u \circ \varepsilon$, de onde segue que $S \circ T$ é a inversa convolutiva de S em $End_{\Bbbk}(H)$, isto é, $S \circ T = id_H$. Repetindo agora o mesmo argumento acima com $S(h)$ em lugar de h, obtemos que $T \circ S$ é uma inversa convolutiva de S em $End_{\Bbbk}(H)$. Portanto, $T \circ S = id_H = S \circ T$, e segue que $T = S^{-1}$.

$(iii) \Rightarrow (i)$ Suponhamos que $S : H \to H$ é invertível e denotemos por S^{-1} a inversa linear de S. Queremos mostrar que S^{-1} é a antípoda de H^{op}. Note que o fato de S ser um antimorfismo de álgebras de H, segue que S^{-1} também o é. De fato, pois se $a, b \in H$ então $a = S(a')$ e $b = S(b')$, para certos $a', b' \in H$. Dai, $S^{-1}(ab) = S^{-1}(S(a'S(b'))) = S^{-1}(S(b'a')) = b'a' = s^{-1}(b)S^{-1}(a)$. Assim, dado $h \in H$, temos

$$\sum_{(h)} S(h_1)h_2 = \varepsilon(h)1_H = \sum_{(h)} h_1S(h_2)$$

Aplicando S^{-1} nos termos desta igualdade e usando que S^{-1} é um antimorfismo de

álgebras em H, obtemos

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

ou seja,

$$m^{op}(id_H \otimes S^{-1})\Delta(h) = \varepsilon(h)1_H = m^{op}(S^{-1} \otimes id_H)\Delta(h)$$

e, portanto, S^{-1} é a antípoda de H^{op}, como queríamos mostrar. □

Uma consequência imediata deste resultado é o seguinte.

Corolário 4.2.2. *Se H é uma álgebra de Hopf com antípoda S. Se H é comutativa ou cocomutativa, então S é bijetiva. Mais ainda, em qualquer destes casos, temos $S^2 = id_H$.*

Demonstração. No caso em que H é comutiva, temos $H = H^{op}$ e no caso em que H é cocomutativa, então temos $H = H^{cop}$. Assim, a bijetividade de S segue imediatamente. Mas em qualquer dos casos, temos que $S = S^{-1}$, de onde segue que $S^2 = id$. □

Quando ocorre que a antípoda S de uma álgebra de Hopf H é tal que $S^2 = id_H$, então S define uma involução em H. Lembramos que uma involução em uma álgebra A é justamente uma aplicação de A em A que é aditiva, antimultiplicativa e quando composta com ela mesma resulta na identidade. Exemplos usuais de involução são dados pela transposição de matrizes ou pelo conjugado complexo. A próxima definição é induzida por estes fatos.

Definição 4.2.3. *Seja H uma álgebra de Hopf com antípoda S. Dizemos que H é uma álgebra de Hopf involutiva, se $S^2 = id_H$.*

Sabemos que a álegebra de grupo é sempre cocomutativa. Se G é um grupo abeliano, então a álgebra de grupo correspondente é comutativa. Estes são exemplos de álgebras de Hopf involutivas.

Procurando condições que assegurem a bijetividade da antípoda de uma álgebra de Hopf, temos o seguinte resultado.

Proposição 4.2.4. *Seja H uma álgebra de Hopf com antípoda S. Se $S_{|S(H)} : S(H) \to S(H)$ é bijetiva, então $S : H \to H$ é bijetiva.*

Demonstração. Como S é um morfismo de álgebras de Hopf, segue que $S(H)$ é uma subálgebra de Hopf de H. Considerando a sequência exata curta $0 \to \mathcal{N}uc\, S \xrightarrow{S} S(H) \to 0$, obtemos que a mesma cinde, pois $S_{|S(H)} : S(H) \to S(H)$ é bijetiva por hipótese. Assim, $H = \mathcal{N}uc\, S \oplus S(H)$. Consideremos a projeção $\Bbbk$-linear $\pi : H \to S(H)$ relativa a $\mathcal{N}uc\, S$ (isto é, estamos considerando π apenas como aplicação linear entre espaços vetoriais).

Como $\mathcal{N}uc\,S$ é um ideal de Hopf, obtemos que $\varepsilon(\mathcal{N}uc\,S) = 0$ ($\mathcal{N}uc\,S$ é um ideal de H) e $\Delta(\mathcal{N}uc\,S) \subseteq \mathcal{N}uc\,S \otimes H + H \otimes \mathcal{N}uc\,S = \pi \otimes H + H \otimes \mathcal{N}uc\,S$ ($\mathcal{N}uc\,S$ é um coideal de H). Portanto, se $x \in \mathcal{N}uc\,S$, temos

$$0 = \varepsilon(x) = \varepsilon(x)1_H = (\pi * S)(x)$$

de modo análogo se mostra que $(S*\pi)(x) = 0 = \varepsilon(x)$ e segue que π é a inversa convolutiva de S em $End_{\Bbbk}(H)$, de onde se conclui que $\pi = id_H$, ou seja, $S(H) = \pi(H) = id_H(H) = H$ e obtemos que S é bijetiva em H, como queríamos mostrar. □

Note que $S^n(H)$ é uma subálgebra de Hopf de H, para todo $n \geq 0$, onde S^n significa compor S com ela mesma n vezes e $S^0 = id_H$, como usual. Assim, o seguinte corolário nos dá algumas condições suficientes para termos uma antípoda bijetiva.

Corolário 4.2.5. *Seja H uma álgebra de Hopf com antípoda S. Então:*

(i) S é bijetiva se, e somente se, $S_{|S^n} : S^n(H) \to S^n(H)$ é bijetiva, para algum $n \geq 0$.

(ii) Se $dim_{\Bbbk}(H) < \infty$, então S é bijetiva.

(iii) Se $S^n(H) = S^{n+1}(H)$ e $\mathcal{N}uc\,S^n = \mathcal{N}uc^n(S)$, para algum $n \geq 0$, então S é bijetiva.

Demonstração. (i) Uma das implicações é óbvia. Suponhamos que existe n tal que $S_{|S^n} : S^n(H) \to S^n(H)$ é bijetiva. Argumentando por indução, podemos supor que $n = 1$. Mas então a Proposição anterior garante que S é bijetiva.

(ii) Como H tem dimensão finita, segue que deve existir algum inteiro n tal que $S^n(H) = S^{n+1}(H)$ e, neste caso, devemos ter $S_{|S^{n+1}(H)} : S^{n+1}(H) \to S^{n+1}(H)$ bijetiva. Segue então da Proposição anterior que S é bijetiva.

(iii) As hipóteses de (iii) garantem que $S_{|S^n} : S^n(H) \to S^n(H)$ é bijetiva. De fato, pois $S^n(H) = S^{n+1}(H) = S(S^n(H))$, o que implica que $S_{|S^n}$ é sobrejetora. Seja $x \in S^n(H)$, tal que $S(x) = 0$. Então existe $y \in H$ tal que $x = S^n(y)$ e como $0 = S(x) = S^{n+1}(y)$, obtemos que $y \in \mathcal{N}uc\,S^{n+1} = \mathcal{N}uc\,S^n$ e assim $x = S^n(y) = 0$, de onde segue que $S_{|S^n}$ é injetora. Portanto a conclusão de (iii) segue diretamente da parte (i). □

Capítulo 5

Representações de álgebras de Hopf

Como dito antes, representações de uma álgebra nada mais são de que seus módulos. Como uma álgebra de Hopf H possui duas estruturas compatíveis, de álgebra e de coálgebra, então podemos esperar que um *módulo de Hopf* sobre uma álgebra de Hopf deve ser um espaço vetorial que possui uma estrutura de módulo sobre a álgebra H e uma estrutura de *módulo* sobre a coálgebra H, de modo que haja uma compatibilidade entre estas estruturas. Vamos começar estudando o que seriam estes "módulos"sobre uma coálgebra, cujo conceito ainda não surgiu neste texto. Então estamos num bom lugar para introduzi-lo e faremos isto, como poderia se esperar, via dualização do conceito de módulo sobre uma álgebra.

5.1 Comódulos

Vamos começar interpretando a definição de um módulo sobre uma álgebra via diagramas, para podermos dualizar este conceito. Sejam A uma $\Bbbk$-álgebra e M um $\Bbbk$-espaço vetorial. Dizemos que M é um A-módulo à esquerda, se existir uma aplicação $\Bbbk$-linear $\triangleright : A \otimes M \to M$, dada por $\triangleright(a, m) := a \triangleright m$, chamada ação à esquerda de A em M, satisfazendo as seguintes condições:

(i) $a \triangleright (b \triangleright m) = ab \triangleright m, \forall a, b \in A; \forall m \in M$

(ii) $1_A \triangleright m = m, \forall m \in M$

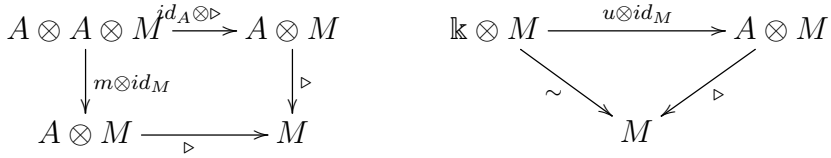
Note que as demais propriedades que aparecem na definição de um módulo são cumpridas pela linearidade da ação. De modo análogo podemos definir *ação à direita de A em M*, usando uma aplicação $\Bbbk$-linear $\triangleleft : M \otimes A \to M$, $\triangleleft : m \otimes a \mapsto m \triangleleft a$, e fazendo as devidas adaptações nas condições acima.

Estas propriedades acima podem ser escritas, respectivamente, como:

(i') $\triangleright \circ (id_A \otimes \triangleright) = \triangleright \circ (m \otimes id_M)$

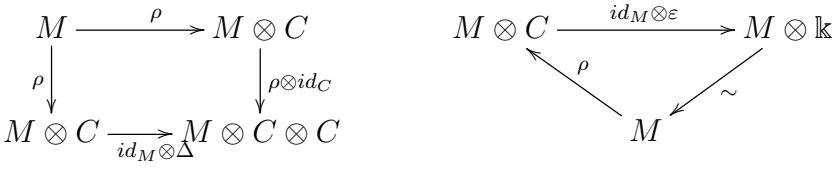
(ii') $\triangleright \circ (u \otimes id_M) = id_M$

as quais, por sua vez, podem ser interpretadas sob forma de diagramas da seguinte maneira: Um A-módulo à esquerda é um $\Bbbk$-espaço vetorial munido de uma aplicação $\Bbbk$-linear $(M, \triangleright)$, definida de tal modo que os diagramas abaixo comutam



Dualizando os diagramas acima, obtemos a noção de um comódulo sobre uma coálgebra.

Definição 5.1.1. *Sejam $C = (C, \Delta, \varepsilon)$ uma coálgebra sobre um corpo $\Bbbk$ e M um $\Bbbk$-espaço vetorial. Dizemos que M é um comódulo à direita sobre C, se existir uma aplicação $\Bbbk$-linear $\rho : M \to M \otimes C$, definida de modo que os seguintes diagramas comutem*



A interpretação destes diagramas nos dão as seguintes condições

(i) $(\rho \otimes id_C) \circ \rho = (id_M \otimes \Delta) \circ \rho$.

(ii) $(id_M \otimes \varepsilon) \circ \rho = id_M$

Vamos agora interpretar as condições acima em termos da notação de Sweedler que terá que ser adaptada para o contexto de comódulos. Sejam C uma coálgebra e M um C-comódulo à direita via a coação $\rho : M \to M \otimes C$. Então denotaremos o elemento $\rho(m) \in M \otimes C$ por $\rho(m) = \sum_{[m]} m_0 \otimes m_1$, de modo que os símbolos m_0 (respectivamente m_1) indicam os elementos de M (respectivamente, de C) que aparecem na primeira entrada (respectivamente, na segunda entrada) dos tensores básicos de uma representação de $\rho(m)$ como elemento de $M \otimes C$. Assim, a condição (i) acima nos diz que

$$\sum_{[m],[m_0]} m_{0_0} \otimes m_{0_1} \otimes m_1 = ((\rho \otimes id_C) \circ \rho)(m) = ((id_M \otimes \Delta) \circ \rho)(m) = \sum_{[m],(m_1)} m_0 \otimes m_{1_1} \otimes m_{1_2}$$

e por consequência, vamos escrever $\sum_{[m]} m_0 \otimes m_1 \otimes m_2 \in M \otimes C \otimes C$ para representar este elemento.

A notação de Sweedler nos permite representar a imagem de um elemento quando aplicamos sucessivas vezes a coação, usando a propriedade (i) acima, teremos, para todo $n \geq 2$:

$$\begin{aligned}\sum_{[m]} m_0 \otimes m_1 \otimes \cdots \otimes m_n &= \sum_{[m]} \rho(m_0) \otimes m_1 \otimes \cdots \otimes m_{n-1} \\ &= \sum_{[m]} m_0 \otimes m_1 \otimes \cdots \otimes m_{i-1} \otimes \Delta(m_{i+1}) \otimes \cdots \otimes m_{n-1}\end{aligned}$$

de modo que o símbolo com índice 0 sempre representará um elemento de M, enquanto que os síbolos com índices positivos representarão elementos de C.

Se estamos trabalhando com comódulos à esquerda, se escrevemos a coação da forma $\delta : M \to C \otimes M$, então representaremos a imagem de um elemento $\delta(m) \in C \otimes M$, por $\delta(m) = \sum_{[m]} m_{-1} \otimes m_0$ de modo que os símbolos com índice zero são sempre elementos de M, como antes, mas agora os símbolos com índices negativos representam elementos de C, de modo que ao aplicarmos a coação diversas vezes, a posição de índice zero permanece sempre mais à direita e as novas entradas vão ocorrendo mais para a esquerda, cujos índices serão negativos. Assim, para $n \geq 2$, temos

$$\sum_{[m]} m_{-n} \otimes \cdots \otimes m_{-1} \otimes m_0 = \sum_{[m]} m_{-n+1} \otimes \cdots \otimes m_1 \otimes \delta(m_0) = \sum_{[m]} m_{-n+1} \otimes \cdots \otimes \Delta(m_i) \otimes \cdots \otimes m_0$$

Antes de prosseguir, gostríamos de observar que a condição $(id_M \otimes \varepsilon) \circ \rho = id_M$ para comódulos à direita, nos diz que a aplicação linear ρ que define a coação de C em M é injetora. A injetividade de ρ permite mostrar que se (M, ρ) é um C-comódulo à direita se, e somente se, (M, ρ^{cop}) é um C^{cop}-comódulo à esquerda, onde $\rho^{cop} : M \to C \otimes M$ é definida por $\rho^{cop}(m) = \sum_{[m]} m_{[1]} \otimes m_{[0]}$, ou seja, $\rho^{cop} = \tau \circ \rho$, onde $\tau : M \otimes C \to M \otimes C$ é a aplicação twiste $\tau(m \otimes c) = c \otimes m$. Assim, a teoria para C-comódulos à direita é exatamente a mesma para C-comódulos à esquerda. Portanto, podemos fixar coações à direita ou coações à esquerda para estudar comódulos.

Veremos alguns exemplos de comódulos.

Exemplo 5.1.2. (1) *Uma coálgebra C é um C-comódulo tanto à esuqerda quanto à direita, via a comultiplicação.*

(2) *Se C é uma coálgebra e V é um $\Bbbk$-espaço vetorial qualquer, então $V \otimes C$ é um C-comódulo à direita com estrutura dada pela coação $\rho : V \otimes C \to V \otimes C \otimes C$, onde $\rho = id_V \otimes \Delta$, como é fácil verificar.*

(3) *Sejam $S \neq \emptyset$ e $C = \Bbbk S$ a coálgebra group-like definida antes (i. é, $\Delta(s) = s \otimes s$ e $\varepsilon(s) = 1, \forall s \in S$). Se $\{M_s\}_{s \in S}$ é uma família de $\Bbbk$-espaços vetoriais e $M := \oplus_{s \in S} M_s$,*

então M é um C-comódulo à direita, via a coação definida por $\rho : M \to M \otimes C$, $\rho(m_s) = m_s \otimes s \otimes s$, para todos $s \in S$, $m_s \in M$, e estendido por linearidade. De fato, pois se $m = \sum_{s\in S} m_s \in M$ (soma finita), então:

$$((\rho \otimes id_C)\rho)(m) = \sum_{s\in S}(\rho \otimes id_C)(m_s \otimes s) = \sum_{s\in S} m_s \otimes s \otimes s$$

e

$$((id_M \otimes \Delta)\rho)(m) = \sum_{s\in S}(id_M \otimes \Delta)(m_s \otimes s) = \sum_{s\in S} m_s \otimes s \otimes s$$

de onde segue que

$$(\rho \otimes id_C)\rho = (id_M \otimes \Delta)\rho$$

Além disso, temos ainda

$$((id_M \otimes \varepsilon)\rho)(m) = id_M\otimes)(\sum m_s \otimes s) = \sum m_s = m$$

ou seja, $(id_M \otimes \varepsilon)\rho = id_M$. Portanto, M é um C-comódulo à direita.

(4) *Sejam $M = (M, \rho_M)$ e $N = (N, \rho_N)$ dois H comódulos à direita. Então o produto tensorial $M\otimes N$ possui uma estrutura de H-comódulo à direita dada por $\rho_{M\otimes N} : M\otimes N \to (M \otimes N) \otimes H$, definida por $\rho_{M\otimes N}(m \otimes n) = \sum_{[m],[n]} m_{[0]} \otimes n_{[0]} \otimes m_{[1]}n_{[1]}$. Note que $m_{[1]}, n_{[1]} \in H$ e, portanto, $m_{[1]}n_{[1]} \in H$. Basta observar que*

$$\begin{aligned}
((id_{M\otimes N} \otimes \varepsilon_H) \circ \rho_{M\otimes N})(m \otimes n) &= (id_{M\otimes N} \otimes \varepsilon_H)(\sum_{[m],[n]} m_{[0]} \otimes n_{[0]} \otimes m_{(1)}n_{(1)}) \\
&= \sum_{[m],[n]} m_{[0]} \otimes n_{[0]} \otimes \varepsilon(m_{(1)}n_{(1)}) \\
&= \sum_{[m],[n]} m_{[0]} \otimes n_{[0]} \otimes \varepsilon(m_{(1)})\varepsilon(n_{(1)}) \\
&= \sum_{[m],[n]} m_{[0]}\varepsilon(m_{(1)}) \otimes n_{[0]}\varepsilon(n_{(1)}) \\
&= m \otimes n
\end{aligned}$$

e

$$\begin{aligned}
((\rho_{M\otimes N} \otimes id_H) \circ \rho_{M\otimes N})(m \otimes n) &= (\rho_{M\otimes N} \otimes id_H)(\sum_{[m],[n]} m_{[0]} \otimes n_{[0]} \otimes m_{(1)}n_{(1)}) \\
&= \sum m_{[0]_{[0]}} \otimes n_{0]_{[0]}} \otimes m_{[0]_{(1)}} \otimes n_{[0]_{(1)}} \otimes m_{(1)}n_{(1)} \\
&= \sum m_{[0]} \otimes n_{[0]} \otimes m_{(1)}n_{(1)} \otimes m_{(2)}n_{(2)} \\
&= ((id_{M\otimes N} \otimes \Delta) \circ \rho_{M\otimes N})(m \otimes n)
\end{aligned}$$

(5) *Se V é um $\Bbbk$-espaço vetorial qualquer, então V possui uma estrutura de H-comódulo 'a direita, via $\rho : V \to V \otimes H$, dada por $\rho(v) := v \otimes 1_H$, para todo $v \in V$. Assim, se $V = \Bbbk$, segue que $\Bbbk$ é um H-comódulo à direita. Esta coação definida acima é dita uma coação trivial de H em V. Assim, o exemplo* (2) *acima pode ser deduzido deste exemplo, do exemplo anterior e do primeiro.*

Definição 5.1.3. *Sejam C uma coálgebra e M um C-comódulo à direita via uma coação $\rho : M \to M \otimes C$. Dizemos que um subespaço N de M é um C-subcomódulo de M, se $\rho_{|N} : N \to N \otimes C$ define uma coação de C em N, isto é, se $\rho(N) \subseteq N \otimes C$.*

A propriedade de finitude local que vimos em uma coálgebra também vale para comódulos, como mostra nosso próximo resultado.

Teorema 5.1.4. (Teorema Fundamental dos Comódulos) *Seja C uma coálgebra e M um C-comódulo à direita. Então todo elemento de M pertence a um subcomódulo finito-dimensional de M.*

Demonstração. Dado $m \in M$, vamos escrever $\rho(m) = \sum_{i=1}^{r} m_i \otimes c_i \in M \otimes C$, onde $r = posto\, \rho(m)$. Assim, os conjuntos $\{m_i\} \subseteq M$ e $\{c_i\} \subseteq C$ são tomados linearmente independentes. Seja $N := \mathcal{G}er_{\Bbbk}\{m_1, ..., m_r\}$ o subespaço de M gerado pelos elementos $m_1, ..., m_r$. Portanto, $dim_{\Bbbk} N = r < \infty$. Agora, note que a propriedade da counidade nos diz que

$$m = (id_M \otimes \varepsilon)\rho(m) = \sum_{i=1}^{n} m_i \varepsilon(c_i) \in N$$

ou seja, $m \in N$. Vamos mostrar então que N é de fato um subcomódulo de M para finalizar nossa demonstração. De fato, pois se $x = \sum_{i=1}^{n} \alpha_i m_i \in N$, então temos

$$\rho(x) = \sum_{i=1}^{n} \alpha_i \rho(m_i) = \sum_{i=1}^{n} \alpha_i (m_i \otimes c_i) = \sum_{i=1}^{n} m_i \otimes \alpha_i c_i \in N \otimes C$$

e temos que N é um subcomódulo de M, como afirmado. □

Se A é uma $\Bbbk$-álgebra e $M = (M, \mu)$, $N = (N, \nu)$ são A-módulos à esquerda, onde $\mu : A \otimes M \to M$ e $\nu : A \otimes N \to N$ são as ações de A sobre M e N, respectivamente, então dizemos que uma aplicação $\Bbbk$-linear $f : M \to N$ é um morfismo de A-módulos, se $\nu \circ (id_A \otimes f) = f \circ \mu$, ou seja, se o diagrama abaixo comuta

$$\begin{array}{ccc} A \otimes M & \xrightarrow{id_A \otimes f} & A \otimes N \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \nu} \\ M & \xrightarrow[f]{} & N \end{array}$$

dualizando este diagrama, chegamos ao conceito de morfismo de coálgebras. Mais precisamente, temos a seguinte definição.

Definição 5.1.5. *Sejam C uma coálgebra e $M = (M, \rho_M)$, $N = (N, \rho_N)$ C-comódulos à direita com coações dadas por $\rho_M : M \to M \otimes C$ e $\rho_N : N \to N \otimes C$, respectivamente. Uma aplicação $\Bbbk$-linear $f : M \to N$ é dita um morfismo de coálgebras se $(f \otimes id_C) \circ \rho_M = \rho_N \circ f$, ou seja, se o diagrama abaixo comuta*

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

De maneira completamente analoga ao que fizemos na seção de coálgebras, podemos definir comódulos fatores e demonstrar um teorema de homomorfismos para comódulos. Enunciaremos estes resultados a seguir.

Proposição 5.1.6. *Sejam C uma coálgebra, $M = (M, \rho)$ um C-comódulo á direita e N um subcomódulo de M. Então existe uma única estrutura de comódulo à direita em M/N de modo que a projeção $\Bbbk$-linear $\pi : M \to M/N$ se torne um morfismo de C-comódulos.*

Demonstração. (ideia) Consideremos a projeção canônica de espaços vetoriais $\pi : M \to M/N$. Como $(\pi \otimes id_C)\rho(N) \subseteq (\pi \otimes id_C)(N \otimes C) = 0$, segue do Teorema dos Homomorfismos para espaços vetoriais que existe única aplicação $\Bbbk$-linear $\overline{\rho} : M/N \to M/N \otimes C$ tal que $\overline{\rho} \circ \rho = (\rho \otimes id_C) \circ \rho$. Isto vai significar que $\overline{\rho}$ é um morfismo de comódulos. Agora tem que ser mostrado que em relação a estrutura de comódulo introduzida desta forma em M/N faz com que π seja um morfismo de comódulos. Esta tarefa será deixada ao leitor interessado. □

Mimetizando o que se faz para módulos ou o que se fez para coálgebras, podemos mostrar o seguinte resultado.

Proposição 5.1.7. *Sejam C uma coálgebra, $m = (M, \rho_M)$ e $N = (N, \rho_N)$ C-comódulos à direita e $f : M \to N$ um morfismo de C-comódulos. Então:*

(i) $\mathcal{N}uc\, f$ é um subcomódulo de M e $\mathcal{I}m\, f$ é um subcomódulo de N.

(ii) Se L é um subespaço de $\mathcal{N}uc\, f$, então existe um único morfismo de comódulos $\overline{f} : M/L \to N$ tal que $\overline{f} \circ \pi = f$. Além disso, $\overline{f}$ é injetora se, e somente se, $L = \mathcal{N}uc\, f$.

Seja C uma coálgebra sobre um corpo $\Bbbk$. Então sabemos que C^* é uma álgebra com o produto convolução. Estamos interessados neste momento em saber como estão

relacionados os comódulos de C e os módulos de C^*, se alguma relação existir de fato. Veremos adiante que estas estruturas estão fortemente relacionadas. Consideremos então um $\Bbbk$-espaço vetorial M. Suponhamos que $\rho : M \to M \otimes C$ é uma aplicação $\Bbbk$-linear (por agora ρ é somente linear. Depois vamos supor que ela define uma coação). Definimos então uma aplicação $\Bbbk$-linear $\psi_\rho : C^* \otimes M \to M$ via a composição

$$C^* \otimes M \xrightarrow{id_{C^*} \otimes \rho} C^* \otimes M \otimes C \xrightarrow{id_{C^*} \otimes \tau} C^* \otimes C \otimes M \xrightarrow{\gamma \otimes id_M} \Bbbk \otimes M \xrightarrow{\sim} M$$

onde $\gamma : C^* \otimes C \to \Bbbk$ é a aplicação definida por $\gamma(f \otimes c) = f(c), \forall f \otimes c \in C^* \otimes C$ e $\tau : M \otimes C \to C \otimes M$ é a aplicação twist. Com estas notações, podemos mostrar o seguinte resultado

Proposição 5.1.8. *Sejam C uma coálgebra, C^* sua álgebra dual, M um $\Bbbk$-espaço vetorial e $\rho : M \to M \otimes C$ uma aplicação linear. Mantendo as notações acima, (M, ρ) é um C-comódulo à direita se, e somente se, (M, ψ_ρ) é um C^*-módulo à esquerda.*

Demonstração. Suponhamos que (M, ρ) é um C-comódulo à direita. Vamos definir uma ação de C^* em M por $f \cdot m := \psi_\rho(f \otimes m)$, onde ψ_ρ está definida como acima. Neste caso, teremos $f \cdot m = \sum_{[m]} f(m_{[1]}) m_{[0]}$, para todos $f \in C^*$ e $m \in M$. Primeiro, observe que $1_{C^*} = \varepsilon$ age trivialmente nos elementos de M, pois

$$1_{C^*} \cdot m = \sum_{[m]} 1_{C^*}(m_{[1]}) m_{[0]} = \sum_{[m]} \varepsilon(m_{[1]}) m_{[0]} = m$$

onde na última igualdade foi usada a propriedade deduzida do segundo diagrama da definição de comódulo. Além disso, se $f, g \in C^*$ e $m \in M$, então temos

$$\begin{aligned} f \cdot (g \cdot m) &= f \cdot \left(\sum_{[m]} g(m_{[1]}) m_{[0]} \right) = \sum_{[m],[m_0]} g(m_{[1]}) f \cdot m_{[0]} \\ &= \sum_{[m],[m_{[0]}]} g(m_{[1]}) f(m_{[0][1]}) m_{[0][0]} = \sum g(m_{[2]}) f(m_{[1]}) m_{[0]} \\ &= \sum (f * g)(m_{[1]}) m_{[0]} = (f * g) \cdot m \end{aligned}$$

e segue que (M, ψ_ρ) é um C^*-módulo à esquerda.

Reciprocamente, suponhamos que (M, ψ_ρ) é um C^*-módulo à esquerda, onde ψ_ρ está definida como acima. Denotando a imagem de $m \in M$ por ρ da forma $\rho(m) := \sum m_0 \otimes m_1 \in M \otimes C$, teremos que $m = 1_{C^*} \cdot m = \varepsilon \cdot m = \sum \varepsilon(m_0) m_1$, que é exatamente a segunda condição da definição de comódulo. Para ver que a primeira condição daquela definição

também vale, fazemos o seguinte cálculo. Por um lado, temos

$$\begin{aligned}(f*g)\cdot m &= \sum (f*g)(m_1)m_0 \\ &= \sum f(m_{1_1})g(m_{1_2})m_0 \\ &= (id_M \otimes f \otimes g)(id_M \otimes \Delta)\rho(m)\end{aligned}$$

e, por outro,

$$\begin{aligned}f\cdot(g\cdot m) &= f\cdot\Big(\sum g(m_1)m_0\Big) \\ &= \sum g(m_1) f\cdot m_0 \\ &= \sum g(m_1)f(m_{0_1})m_{0_0} \\ &= (id_M \otimes f \otimes g)(\rho \otimes Id_M)\rho(m)\end{aligned}$$

de onde segue que $(id_M \otimes f \otimes g)((id_M \otimes \Delta)\rho(m) - (\rho \otimes Id_M)\rho(m)) = 0$, para todos os funcionais $f, g \in C^*$. Portanto devemos ter $(id_M \otimes \Delta)\rho(m) - (\rho \otimes Id_M)\rho(m) = 0$, ou seja, $(id_M \otimes \Delta)\rho(m) = (\rho \otimes Id_M)\rho(m)$, isto é, $(id_M \otimes \Delta) \circ \rho = (\rho \otimes Id_M) \circ \rho$, como queríamos mostrar. Logo, (M, ρ) é um C-comódulo à direita e o resultado está demonstrado. □

O resultado acima nos diz que todo C-comódulo à direita tem uma estrutura natural de C^*-módulo à esquerda. Mas nem todo C^*-módulo à esquerda possui uma estrutura de C-comódulo à direita. A família dos C^*-módulos com esta propriedade são chamados de *módulos racionais*. Este fenômeno não chega a ser surpreendente, uma vez que os comódulos possuem a propriedade da finitude local, o que não acontece em geral com módulos. Assim, vamos estabelecer uma correspondência entre os C-comódulos à direita e os C^*-módulos racionais à esquerda.

Seja C uma coálgebra e consideremos M um C^*-módulo à esquerda, com ação denotada por $f \cdot m$, para todo $f \in C^*$ e $m \in M$. Definimos o seguinte subconjunto de M

$$M_r := \{m \in M : \exists! \rho_m \in M \otimes C \text{ tal que } f\cdot m = (id_M \otimes f)(\rho_m), \forall f \in C^*\}$$

Primeiro, vejamos que M_r está bem definido. De fato, pois se existirem elementos $\rho_m = \sum m_i \otimes c_i, \rho'_m = \sum m'_i \otimes c'_i \in M \otimes C$ tais que $(id_M \otimes f)(\rho_m) = (id_M \otimes f)(\rho'_m)$, para todo $f \in C^*$, então teremos que $\rho_m - \rho'_m = 0$, ou seja, $\rho_m = \rho'_m$.

Lembramos que C é um C^*-módulo à esquerda via a ação $f \rightharpoonup c := \sum_{(c)} c_1 f(c_2)$, onde $f \in C^*$ e $c \in C$. Assim, temos $f \rightharpoonup c := \sum_{(c)} c_1 f(c_2) = (id_C \otimes f)(\sum_{(c)} c_1 \otimes c_2) = (id_C \otimes f)(\rho_c)$, onde $\rho_c = \Delta(c) \in C \otimes C$. Portanto, $C_r = C$ neste caso. O próximo resultado mostra, entre outras coisas, que M_r é um C^*-submódulo de C.

Proposição 5.1.9. *Sejam C uma coálgebra sobre um corpo $\Bbbk$ e M um C^*-módulo à*

esquerda. Mantendo as notações acima, temos:

(i) M_r *é um* C^**-submódulo localmente finito de* M*.*

(ii) Se $m \in M_r$*, então* $dim_{\Bbbk}(f \cdot m) = posto\, \rho_m$*. Além disso, se* $0 \neq \rho_m = \sum_{i=1}^{t} m_i \otimes c_i \in M \otimes C$*, com* $posto\, \rho_m = t$*, então* $\{m_1, ..., m_t\}$ *é uma* $\Bbbk$*-base de* $f \cdot m$*.*

(iii) Se N *é um* C^**-submódulo de* M*, então* $N_r = N \cap M_r$*.*

(iv) Se $\varphi : M \to N$ *é um morfismo de* C^**-módulos, então* $\varphi(M_r) \subseteq N_r$ *e a restrição* $\varphi_1 | \, M_r : M_r \to N_r$ *é um morfismo de* C^**-módulos.*

Demonstração. Seja $0 \neq m \in M_r$ e suponhamos que $\rho_m = \sum_{i=1}^{t} m_i \otimes c_i \in M \otimes C$, onde $posto\, \rho_M = t$. Então $\{m_1, ..., m_t\}$ é linearmente independente em M, e como $f \cdot m = (id_M \otimes f)(\rho_m) = \sum_{i=1}^{t} f(c_i)m_i \subseteq \mathcal{G}er_{\Bbbk}\{m_1, ..., m_t\}$, para todo $f \in C^*$, segue que $C^* \cdot m \subseteq \mathcal{G}er_{\Bbbk}\{m_1, ..., m_t\}$. Além disso, como $\{c_1, ..., c_t\}$ também é linearmente independente em C, segue que existem funcionais lineares $f_i \in C^*$ tais que $f_i(c_j) = \delta_{i,j}$, $1 \leq i, j \leq t$. Fixando j, obtemos que $m_j = \sum_{i=1}^{t} f_i(c_j)m_i = (id_M \otimes f_j)(\rho_m) = f_j \cdot m$ e segue que $C^* \cdot m = \mathcal{G}er_{\Bbbk}\{m_1, ..., m_t\}$. isto mostra (ii).

Claramente M_r é um $\Bbbk$-subespaço de M. Para mostrar (i), basta verificar que $C^* \cdot M_r \subseteq M_r$, pois a propriedade da finitude local segue de (ii). Note que se fixamos $f \in C^*$ e $m \in M_r$, onde continuamos a denotar $\rho_m = \sum_{i=1}^{t} m_i \otimes c_i \in M \otimes C$, e tomamos $g \in C^*$ arbitrário, então temos

$$\begin{aligned} g \cdot (f \cdot m) &= (g * f) \cdot m \\ &= \sum (g * f)(c_i)m_i \\ &= \sum g(c_{i_1})f(c_{i_2})m_i \\ &= \sum g(c_{i_1} f(c_{i_2}))m_i \\ &= (id_M \otimes g)\left(\sum m_i \otimes f \rightharpoonup c_i\right) \end{aligned}$$

e como estas igualdades valem para todo $g \in C^*$, deduzimos que o elemento $\rho_{f \cdot m}$ existe e $\rho_{f \cdot m} = \sum m_i \otimes (f \rightharpoonup c_i) \in M \otimes C$. portanto, $C^* \cdot M_r \subseteq M_r$. Isto completa a demonstração de (i).

A afirmação do item (iii) segue diretamente de (ii), pois dado $n \in N$, temos que $C^* \cdot n$ é gerado, como $\Bbbk$-espaço vetorial, pelos elementos $n_1, ..., n_r \in N$ tais que $\rho_n = \sum n_i \otimes c_i \in N \otimes C \subseteq M \otimes N$.

Para obter (iv), basta observar que se $\rho_m = \sum_{i=1}^{t} m_i \otimes c_i \in M \otimes C$, então temos $\rho_{f(m)} = \sum_{i=1}^{t} f(m_i) \otimes c_i \in N \otimes C$, pois se $g \in C^*$, segue que $g \cdot (f(m)) = f(g \cdot m) = f\left(\sum_{i=1}^{t} m_i g(c_i)\right) = \sum_{i=1}^{t} f(m_i)g(c_i) = (id_M \otimes g)\left(\sum_{i=1}^{t} f(m_i) \otimes c_i\right)$, de onde concluímos

que $\rho_{f(m)}$ existe e $\rho_{f(m)} = \sum_{i=1}^{t} f(m_i) \otimes c_i \in N \otimes C$. Portanto, $f(M_r) \subseteq N_r$. O resto é claro. □

O resultado acima induz a seguinte definição.

Definição 5.1.10. *Seja C uma coálgebra sobre um corpo $\Bbbk$. Um C^*-módulo à esquerda M é dito racional, se $M_r = M$.*

Como observamos antes, toda coálgebra C é um C^*-módulo racional. É uma consequência do resultado acima que se $dim_{\Bbbk} C < \infty$ então todo C^*-módulo é racional. Além disso, todo C^*-módulo M possui um maior submódulo racional, definido por

$$M^{rat} := \sum \{N : N \text{ é submódulo racional de } M\}$$

para ver esta igualdade, basta ver que se $x \in M^{rat}$, então o elemento ρ_x existe. Mas neste caso, temos $x = \sum_{i \in I} n_i$, com $n_i \in N_i$, sendo I um conjunto finito. Como todos os $N_i's$ são módulos racionais, o elemento $\rho_{n_i} \in N_i \otimes C$ existe. Não é difícil então concluir que $\rho_x = \sum_{i \in I} \rho_{n_i} \in \left(\sum_{i \in I} N_i\right) \otimes C = M \otimes C$.

Para finalizar esta discussão, se C é uma coálgebra e M é um C^*-módulo à esquerda racional, onde denotamos a ação de C^* sobre M da forma $f \cdot m$, para $f \in C^*$ e $m \in M$, então definindo $\rho : M \to M \otimes C$, por $\rho(m) = \rho_m$, onde $\rho_m \in M \otimes C$ é o único elemento tal que $f \cdot m = (id_M \otimes f)(\rho_m)$, para todo $f \in C^*$, segue que ρ está bem definida e é fácil verificar que ρ é uma aplicação $\Bbbk$-linear. Para ver que (M, ρ) é um comódulo à direita, fazemos uso da Proposição 5.1.8. De fato, basta observar que usando as notações prévias a dita Proposição, temos

$$f \cdot m = (id_M \otimes f)(\rho_m) = \sum_{i=1}^{t} f(c_i)m_i = (\gamma \otimes id_M)(id_{C^*} \otimes \tau)(id_{C^*} \otimes \rho)(f \otimes m) = \psi_\rho(f \otimes m)$$

Podemos então resumir toda esta discussão no seguinte resultado, mantendo-se as notações precedentes.

Proposição 5.1.11. *Seja C uma coálgebra sobre um corpo $\Bbbk$. Então:*

(i) Se (M, ρ) é um C-comódulo à direita, então (M, ψ_ρ) é um C^*-módulo à esquerda racional, onde $\rho_m := \rho(m)$, para todo $m \in M$.

(ii) Se (M, ψ) é um C^*-módulo à esquerda racional, então (M, ρ) é um C-comódulo à direita, onde $\rho(m) := \rho_m$, para todo $m \in M$.

5.2 Módulos de Hopf

Consideremos agora H uma álgebra de Hopf com antípoda S. Seja M um $\Bbbk$-espaço vetorial que possui uma estrutura de H-módulo à direita, digamos via $\triangleleft : M \otimes H \to M$, $\triangleleft : m \otimes h \mapsto m \triangleleft h$, e uma estrutura de H-comódulo à direita, digamos via $\rho : M \to M \otimes H$, $\rho : m \mapsto \sum_{[m]} m_{[0]} \otimes m_{[1]} \in M \otimes H$. Com estas notações, fazemos a seguinte definição.

Definição 5.2.1. *Sejam H uma álgebra de Hopf e M um $\Bbbk$-espaço vetorial que possui estrutura de H-módulo à direita e de H-comódulo à direita. Mantendo as notações acima, dizemos que M é um H-módulo de Hopf à direita, se o diagrama abaixo comutar*

$$\begin{array}{ccccc} M \otimes H & \xrightarrow{\triangleleft} & M & \xrightarrow{\rho} & M \otimes H \\ {\scriptstyle \rho\otimes\Delta}\downarrow & & & & \downarrow{\scriptstyle =} \\ M \otimes H \otimes H \otimes H & & \xrightarrow[id_M \otimes \tau \otimes \mathrm{id}_H]{} & & M \otimes H \end{array}$$

Em notação de Sweedler, o diagrama da definição acima pode ser escrito da forma

$$\rho(m \triangleleft h) = \sum_{(h),[m]} (m_{[0]} \triangleleft h) \otimes (m_{(1)} h_{(2)})$$

Podemos definir um módulo de Hopf à esquerda de maneira similar, com as devidas adaptações. Observe que não usamos a antípoda de H na definição de módulo de Hopf, de modo que este conceito poderia ser introduzido para biálgebras, mas é no contexto de álgebras de Hopf que ele ganha importância e tem consequências mais profundas.

Note também que a condição de compatibilidade acima significa o mesmo que dizer que M é um módulo de Hopf à direita, com ação $\triangleleft : M \otimes M \to M$, $m \otimes h \mapsto m \triangleleft h$, e coação $\rho : M \to M \otimes H$, $\rho(m) = \sum_{[m]} m_{[0]} \otimes m_{[1]}$, se e somente se $\triangleleft$ é um morfismo de comódulos, se e somente se, ρ é um morfismo de módulos, pois

$$\begin{aligned} \rho(m \triangleleft h) &= \sum_{(h),[m]} (m_{[0]} \triangleleft h) \otimes (m_{(1)} h_{(2)}) \\ &= \sum_{[m]} (m_{[0]} \otimes m_{[1]}) \triangleleft h \\ &= \rho(m) \triangleleft h \end{aligned}$$

e

$$\begin{aligned}(\rho \circ \triangleleft)(m \otimes h) &= \rho(m \triangleleft h) \\ &= \sum_{(h),[m]} (m_{[0]} \triangleleft h) \otimes (m_{(1)} h_{(2)}) \\ &= (\triangleleft \otimes id_H)(m_{[0]} \otimes h_{(1)} \otimes m_{[1]} h_{(2)}) \\ &= ((\triangleleft \otimes id_H) \circ \rho_{M \otimes H})(m \otimes h)\end{aligned}$$

Vejamos alguns exemplos de módulos de Hopf.

Exemplo 5.2.2. (1) *Toda álgebra de Hopf é um módulo de Hopf sobre si mesma, tanto à direita quanto à esquerda.*

(2) *Seja H uma álgebra de Hopf finito-dimensional. Então podemos introduzir uma estrutura de H-módulo de Hopf à direita em H^*, da seguinte forma. Primeiro observamos que H^* tem uma estrutura de H-comódulo à direita dada por $\rho : H^* \to H^* \otimes H$, onde $\rho(\alpha) := \sum_{[f]} \alpha_0 \otimes \alpha_1$, sendo que as famílias $\{\alpha_0\} \subseteq H^*$ e $\{\alpha_1\} \subseteq H$ são unicamente determinadas de modo que, para todo $\beta \in H^*$, temos $\beta * \alpha = \sum \beta(\alpha_1)\alpha_0$. Precisamos encontrar uma ação de H em H^* que seja compatível com a coação acima. Para tanto, consideramos a ação à direita de H sobre H^* dada por*

$$\begin{array}{rccccccc} \leftharpoonup: & H^* \otimes H & \longrightarrow & H^* & & & & \\ & \alpha \otimes h & \mapsto & \alpha \leftharpoonup h : & H & \to & \Bbbk \\ & & & & g & \mapsto & \alpha(gS(h)) \end{array}$$

Vejamos que a aplicação $\Bbbk$-linear acima define uma ação de H em H^*. De fato pois se $\alpha \in H^*$ e $g, hk \in H$, temos

$$(\alpha \leftharpoonup 1_H)(g) = \alpha(gS(1_H)) = \alpha(g)$$

ou seja, $\alpha \leftharpoonup 1_H = \alpha$. Além disso,

$$\begin{aligned}((\alpha \leftharpoonup h) \leftharpoonup k)(g) &= (\alpha \leftharpoonup h)(gS(k)) \\ &= \alpha(gS(k)S(h)) \\ &= \alpha(gS(hk)) \\ &= (\alpha \leftharpoonup hk)(g)\end{aligned}$$

ou seja, $(\alpha \leftharpoonup h) \leftharpoonup k = \alpha \leftharpoonup hk$. Precisamos agora verificar a compatibilidade entre a ação e coação dadas acima. De acordo com a definição de módulo de Hopf, precisamos mostrar que

$$\rho(\alpha \leftharpoonup h) = \sum \alpha_0 \leftharpoonup h_1 \otimes \alpha_1 h_2$$

e como vimos acima, isto é equivalente a mostrar que

$$\beta * (\alpha \leftharpoonup h) = \sum \beta(\alpha_1 h_2)(\alpha_0 \leftharpoonup h_1)$$

para todos $\beta, \alpha \in H^*$ *e* $h \in H$*. Portanto, vamos verificar que esta última relação é verdadeira em nosso exemplo. Tomando* $g \in H$*, temos, por um lado,*

$$\begin{aligned}(\beta * (\alpha \leftharpoonup h))(g) &= \sum \beta(g_1)\alpha(g_2 S(h)) \\ &= \beta(g_1)\alpha(g_2 S(h_1\varepsilon(h_2))) \\ &= \beta(g_1\varepsilon(h_2))\alpha(g_2 S(h_1)) \\ &= \beta(g_1 S(h_2)h_3)\alpha(g_2 S(h_1)) \\ &= (h_3 \triangleright \beta)(g_1 S(h_2))\alpha(g_2 S(h_1))\end{aligned}$$

e, por outro lado,

$$\begin{aligned}\sum \beta(\alpha_1 h_2)(\alpha_0 \leftharpoonup h_1)(g) &= \beta(\alpha_1 h_2)\alpha_0(gS(h_1)) \\ &= (h_2 \triangleright \beta)(\alpha_1)\alpha_0(gS(h_1)) \\ &= (h_2 \triangleleft \beta)((gS(h_1))_1)\alpha((gS(h_1))_2) \\ &= (h_2 \triangleleft \beta)(g_1(S(h_1))_1)\alpha(g_2(S(h_1))_2) \\ &= (h_3 \triangleright \beta)(g_1 S(h_2))\alpha(g_2 S(h_1))\end{aligned}$$

de modo que $(\beta * (\alpha \leftharpoonup h)) = \sum \beta(\alpha_1 h_2)(\alpha_0 \leftharpoonup h_1)$*. Portanto,* H^* *é um* H*-módulo de Hopf à direita.*

(3) *Sejam* H *uma álgebra de Hopf e* V *um* $\Bbbk$*-espaço vetorial. Então* $M = V \otimes_{\Bbbk} H$ *possui uma estrutura de módulo de Hopf à direita sobre* H*. De fato, pois* M *se torna um* H*-módulo à direita via a ação* $\triangleleft : V \otimes H \otimes H \to V \otimes H$*, dada por* $(v \otimes h) \triangleleft g := v \otimes hg$*, para todo* $v \in V$*,* $h, g \in H$*, como é fácil verificar. Além disso, a aplicação linear* $\rho : V \otimes H \to V \otimes H \otimes H$ *definida por* $\rho(v \otimes h) := \sum_{(h)} v \otimes h_1 \otimes h_2$*, para todo* $v \in V$*,* $h \in H$ *produz uma estrutura de* H*-comódulo à direita, visto que*

$$(\rho \otimes id_H) \circ \rho(v \otimes h) = \sum_{(h)} v \otimes h_{1_1} \otimes h_{1_2} \otimes h_2 = \sum_{(h)} v \otimes h_1 \otimes h_{2_1} \otimes h_{2_2} = (id_{V\otimes H} \otimes \Delta) \circ \rho(v \otimes h)$$

e

$$(id_{V\otimes H} \otimes \varepsilon) \circ \rho(v \otimes h) = \sum_{(h)} v \otimes h_2\varepsilon(h_2) = v \otimes \sum_{(h)} h_1\varepsilon(h_2) = v \otimes h = id_{V\otimes H}.$$

A compatibilidade entre a ação e coação dadas acima é verificada da seguinte forma

$$\begin{aligned}
\rho(v \otimes h) \triangleleft g &= \rho(v \otimes hg) \\
&= \sum_{(hg)} v \otimes (hg)_1 \otimes (hg)_2 \\
&= \sum_{(h),(g)} v \otimes h_1 g_1 \otimes h_2 g_2 \\
&= \sum_{(h),(g)} ((v \otimes h_1) \triangleleft g_1) \otimes h_2 g_2 \\
&= \sum_{(h),(g)} ((v \otimes h)_{[0]} \triangleleft g_1) \otimes (v \otimes h)_{[1]} g_2
\end{aligned}$$

Definição 5.2.3. *Sejam H uma álgebra de Hopf e M, N H-módulos de Hopf à direita e $f : M \to N$ uma aplicação $\Bbbk$-linear. Dizemos que f é um morfismo de H-módulos de Hopf, se f for um morfismo tanto de H-módulos quanto de H-comódulos.*

Os subespaços dos elementos inveriantes por uma ação ou coação de uma álgebra de Hopf são importantes na teoria. Faremos as definições precisas destes subespaços.

Definição 5.2.4. *Sejam H uma álgebra de Hopf e M um H-módulo à esquerda. O subespaço*

$$M^H := \{m \in M : h \cdot m = \varepsilon(h)m, \forall h \in H\}$$

é chamado de espaço dos elementos invariantes de M

Definição 5.2.5. *Sejam H uma álgebra de Hopf e M um H-comódulo à direita via $\rho : M \to M \otimes H$. O subespaço*

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

é chamado de espaço dos elementos coinvariantes de M

É fácil verificar que se M é um H-módulo à esquerda, então o subespaço M^H é um H-submódulo de M. Analogamente, se M é um H-comódulo à direita, então M^{coH} é um H-subcomódulo de M.

Note que se M é um H-módulo de Hopf à direita, com ação $\triangleleft : M \otimes H \to M$ e coação $\rho : M \to M \otimes H$, então segue do Exemplo 5.2.2(3) que $M^{coH} \otimes H$ é um H-módulo de Hopf à direita. Consideremos $\psi : M^{coH} \otimes H \to M$ a aplicação linear definida por $\psi(m \otimes h) := m \triangleleft h$. Vamos mostrar que ψ assim definida é um morfismo de módulos de Hopf. De fato, pois se $m \in M$, $h, g \in H$, temos

$$\psi((m \otimes h) \triangleleft g) = \psi(m \otimes hg) = m \triangleleft (hg) = (m \triangleleft h) \triangleleft g = \psi(m \otimes h) \triangleleft g$$

e segue que ψ é um morfismo de H-módulos. Para mostrarmos que ψ é também um morfismo de H-comódulos, precisamos mostrar a comutatividade do seguinte diagrama

$$\begin{array}{ccc} M^{coH} \otimes H & \xrightarrow{\quad\psi\quad} & M \\ {\scriptstyle id_{M^{coH}} \otimes \Delta}\downarrow & & \downarrow{\scriptstyle \rho} \\ M^{coH} \otimes H \otimes H & \xrightarrow[\psi \otimes id_H]{} & M \otimes H \end{array}$$

mas se $m \in M$ e $h \in H$, temos

$$\begin{aligned} (\rho \circ \psi)(m \otimes h) &= \rho(m \triangleleft h) \\ &= \rho(m) \triangleleft h \\ &= (m \otimes 1) \triangleleft h \\ &= \sum_{(h)} m \triangleleft h_1 \otimes h_2 \\ &= \sum_{(h)} (\psi \otimes id_H)(m \otimes h_1 \otimes h_2) \\ &= ((\psi \otimes id_H) \circ (id_M \otimes \Delta))(m \otimes h) \end{aligned}$$

e segue que ψ é um morfismo de módulos de Hopf, como queríamos mostrar. O próximo resultado vai nos dizer que de fato ψ é um isomorfismo de módulos de Hopf, de onde segue que todo módulo de Hopf é da forma dada no Exemplo 5.2.2(3).

Teorema 5.2.6. (Teorema Fundamental dos Módulos de Hopf) *Sejam H uma álgebra de Hopf com antípoda S e M um H-módulo de Hopf. Então M é isomorfo a $M^{coH} \otimes H$ como H-módulos de Hopf.*

Demonstração. Consideremos a aplicação $\psi : M^{coH} \otimes H \to M$ definida por $\psi(m \otimes h) = m \triangleleft h$ descrita acima. Então sabemos que ψ é um morfismo de módulos de Hopf. Para mostrar que ψ é de fato um isomorfismo, vamos construir uma inversa linear para ψ. Para tanto, primeiro vamos observar que a aplicação linear $\pi : M \to M$ definida por $\pi(m) := m_{[0]} S(m_{[1]})$, para todo $m \in M$, é uma projeção linear de M em M^{coH}. Inicialmente, note que π é definida pela composição

$$M \xrightarrow{\rho} M \otimes H \xrightarrow{id_M \otimes S} M \otimes H \xrightarrow{\triangleleft} M$$

Assim, como a antípoda é um anti-morfismo de álgebras e M é um módulo de Hopf, temos

$$\begin{aligned}
\rho(\pi(m)) &= \sum_{[m]} \rho(m_{[0]} \triangleleft S(m_{[1]})) \\
&= \sum_{[m],(S(m_{[1]}))} m_{[0]_{[0]}} \triangleleft S(m_{[1]})_{(1)} \otimes m_{[0]_{[1]}} S(m_{[1]})_{(2)} \\
&= \sum m_{[0]} \triangleleft S(m_{[3]}) \otimes m_{[1]} S(m_{[2]}) \\
&= \sum m_{[0]} \triangleleft S(m_{[2]}) \otimes \varepsilon(m_{[1]}) \\
&= \sum m_{[0]} \triangleleft S(m_{[2]}) \varepsilon(m_{[1]}) \otimes 1_H \\
&= \sum m_{[0]} \triangleleft S(m_{[i]}) \otimes 1_H \\
&= \pi(m) \otimes 1_H \\
&\subseteq M^{coH}
\end{aligned}$$

de onde segue que $\mathcal{I}m\,\pi \subseteq M^{coH}$. Além disso, se $m \in M^{coH}$, então $\rho(m) = m \otimes 1_H$, de onde segue que $\pi(m) = \sum_{[m]} m_{[0]} \triangleleft S(m_{[1]}) = m \triangleleft S(1_H) = m \triangleleft 1_H = m$, isto é, $\pi_{|M^{coH}} = id_{M^{coH}}$. Portanto, π é uma projeção linear de M em M^{coH}.

Como $\pi(M) \subseteq M^{coH}$, segue que $\varphi : M \to M^{coH} \otimes H$, dada por $\varphi(M) = \sum_{[m]} \pi(m_{[0]}) \otimes m_{[1]} = \sum_{[m]} m_{[0]} \triangleleft S(m_{[1]}) \otimes m_{[2]} = ((\pi \otimes id_H) \circ \rho)(m)$ está bem definida e é uma aplicação linear. Vamos mostrar que φ é a inversa linear de ψ. De fato, pois se $m \in M^{coH}$ e $h \in H$, então

$$\begin{aligned}
(\varphi \circ \psi)(m \otimes h) &= \varphi(m \triangleleft h) \\
&= (\pi \otimes id_H)\rho(m \triangleleft h) \\
&= (\pi \otimes id_H)(\sum_{(h)} m \triangleleft h_{(1)} \otimes h_{(2)}) \\
&= \sum_{(h)} (m \triangleleft h_{(1)}) \triangleleft S(h_{(2)}) \otimes h_{(3)} \\
&= \sum_{(h)} m \triangleleft (h_{(1)} S(h_{(2)}) \otimes h_{(3)} \\
&= \sum_{(h)} m \triangleleft \varepsilon(h_{(1)}) \otimes h_{(2)} \\
&= m \otimes \left(\sum_{(h)} \varepsilon(h_{(1)}) h_{(2)} \right) \\
&= m \otimes h
\end{aligned}$$

ou seja, $(\varphi \circ \psi) = id_{M^{coH} \otimes H}$. Por outro lado, se $m \in M$, então

$$\begin{aligned}(\psi \circ \varphi)(m) &= \psi\left(\sum_{[m]} m_{[0]} \triangleleft S(m_{[1]}) \otimes m_{[2]}\right) \\ &= \sum_{[m]} (m_{[0]} \triangleleft S(m_{[1]})) \triangleleft m_{[2]} \\ &= \sum_{[m]} \triangleleft (S(m_{[1]}) m_{[2]}) \\ &= \sum_{[m]} m_{[0]} \triangleleft \varepsilon(m_{[1]}) \\ &= m\end{aligned}$$

ou seja, temos $(\psi \circ \varphi) = id_M$. Isto finaliza nossa demonstração. □

Sejam H uma álgebra de Hopf e V um $\Bbbk$-espaço vetorial. Vimos antes que $M := V \otimes H$ possui uma estrutur natural de módulo de Hopf. Consideremos $\{v_i\}_{i \in I}$ uma $\Bbbk$-base de V. Então não é difícil verificar que M é um H-módulo à direita livre com base $\{v_i \otimes 1_H\}_{i \in I}$. Além disso, se escrevemos $H_i := (v_i \otimes 1_H) \triangleleft H$, para cada $i \in I$ fixado, então temos $M \simeq \oplus_{i \in I} H_i$, onde $H_i \simeq H$ como H-módulo à direita. Além disso, se $h \in H$ e fixamos $i \in I$, então $\rho(v_i \otimes h) = v_i \otimes h_{(1)} \otimes h_{(2)} = ((v_i \otimes 1_H) \triangleleft h_{(1)}) \otimes h_{(2)} \in H_i \otimes H$, de onde segue que $H_i = (v_i \otimes 1_H) \triangleleft H$ é um H-subcomódulo de M. Assim, temos que $M \simeq \oplus_{i \in I} H_i$ também como H-comódulo à direita. Combinando esta observação com o Teorema acima, obtemos o seguinte resultado.

Corolário 5.2.7. *Sejam H uma álgebra de Hopf e M um H-módulo de Hopf à direita não nulo. Então:*

(i) $M^{coH} \neq 0$.

(ii) *M é um H-módulo à direita livre com base formada por elementos coinvariantes de M.*

(iii) *M é uma uma soma direta de cópias de H como H-módulo de Hopf à direita.*

De fato, Radford mostrou em [11] que estas propriedades acima caracterizam um álgebra de Hopf, ou seja, se H é uma biálgebra tal que todo módulo de Hopf finitamente gerado sobre H é livre, com uma base formada por elementos coinvarintes, como H-módulo, então a biálgebra H H é uma álgebra de Hopf. Note que estamos aqui usando o fato de módulos de Hopf podem ser definidos sobre biálgebras, como observado antes.

O resultado acima pode transmitir uma ideia de que os módulos de Hopf não são muito úteis no desenvolvimento da teoria, uma vez que são triviais num certo sentido. Os próximos resultados, ajudam a desmistificar esta ideia.

Proposição 5.2.8. *Sejam H uma álgebra de Hopf de dimensão finita e I um subespaço de H que é um ideal à direita e um coideal à direita de H. Então $I = 0$ ou $I = H$.*

Demonstração. Nas hipóteses acima, segue que I é um submódulo de Hopf à direita de H, pois I possui estrutura de H-módulo à direita e de H-comódulo à direita, sendo que a compatibilidade entre estas duas estruturas é herdada da estrutura de H-módulo de Hopf de H. Aplicando o Teorema Fundamental dos módulos de Hopf, obtemos $I \simeq I^{coH} \otimes H$. assim, se $I \neq 0$, então $dim_{\Bbbk} H > dim_{\Bbbk} I = (dim_{\Bbbk} I^{coH})(dim_{\Bbbk} H)$, de onde segue que $dim_{\Bbbk} I^{coH} = 1$ e, portanto, $dim_{\Bbbk} H = dim_{\Bbbk} I$, ou seja, $I = H$. □

Para o próximo resultado, lembramos que se H é uma álgebra de Hopf de dimensão finita, então H^* tem uma estrutura de H-módulo de Hopf à direita dada no Exemplo 5.2.2(2).

Proposição 5.2.9. *Mantendo as notações do Exemplo 5.2.2(2), se H tem dimensão finita, então o espaço $(H^*)^{coH}$ é unidimensional.*

Demonstração. Segue do Teorema Fundamental dos módulos de Hopf que $H^* \simeq (H^*)^{coH} \otimes H$. Como H é finito-dimensional, segue que $dim_{\Bbbk} H = dim_{\Bbbk} H^*$, de onde concluímos que $dim_{\Bbbk} H^* = (dim_{\Bbbk} H^{*^{coH}})(dim_{\Bbbk} H^*)$, ou seja, $dim_{\Bbbk} (H^*)^{coH} = 1$ □

Capítulo 6

Ações e coações de álgebras de Hopf

Na seção anterior vimos que os módulos de Hopf são triviais num certo sentido. Na teoria de representações de álgebras de Hopf, os H-módulos que possuem uma estrutura de $\Bbbk$-álgebra desempenham um papel estratégico. Vamos estudá-los a partir de agora. Assim, estamos interessados nos espaços vetoriais que possuem estrutura tanto de H-módulo quanto de $\Bbbk$-álgebra, de modo que estas estruturas sejam compatíveis. Assim surge o conceito de ações de álgebras de Hopf sobre outras álgebras. Dualizando este conceito, obtemos uma coação de álgebras de Hopf. Vamos trabalhar com estes dois conceitos neste capítulo, dando maior ênfase às ações.

6.1 Ações e coações

Vamos introduzir os conceitos de ações e coações de álgebras de Hopf nesta seção e discutir o caso de ações e coações de álgebras de grupo.

Definição 6.1.1. *Sejam H uma álgebra de Hopf e A uma $\Bbbk$-álgebra. Dizemos que H age à esquerda de A, ou que A é um H-módulo álgebra à esquerda, se existir uma aplicação $\Bbbk$-linear $\cdot : H \otimes A \to A$, definida por $(h, a) \mapsto h \cdot a$, satisfazendo as seguintes condições:*

(i) A *é um* H*-módulo à esquerda via* $\cdot$.

(ii) $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b), \forall h \in H, a, b \in A$

(iii) $h \cdot 1_A = \varepsilon(h) 1_A, \forall h \in H$.

Observemos que as condições (ii) e (iii) da Definição acima nos dizem que a multiplicação $m_A : A \otimes A \to A$ e a unidade $u_A : \Bbbk \to A$ são morfismos de H-módulos à esquerda, pois se $h \in H$ e $a, b \in A$, temos $m_A(h \triangleright a \otimes b) = m_A(\sum h_1 \cdot a \otimes h_2 \cdot b) = \sum (h_1 \cdot a)(h_2 \cdot b)$ e $u_A(h \cdot 1_\Bbbk) = u_A(\varepsilon(h) 1_\Bbbk) = \varepsilon(h) \cdot u_A(1_\Bbbk) = \varepsilon(h) 1_A = \varepsilon(h) \cdot u_A(1_\Bbbk)$.

Visto desta maneira, podemos dualizar o conceito de ação de uma álgebra de Hopf, obtendo o conceito de coação de álgebra de Hopf. Mais precisamente, temos a seguinte definição.

Definição 6.1.2. *Sejam H uma álgebra de Hopf e A uma $\Bbbk$-álgebra. Dizemos que A é um H-comódulo à direita, se existir uma aplicação $\Bbbk$-linear $\rho : A \to A \otimes H$ tal que*

(i) A é um H-comódulo à direita via ρ.

(ii) A multiplicação m_A e a unidade u_A são morfismos de H-comódulos à direita.

Usando a notação de Sweedler e denotando $\rho(a) = a_0 \otimes a_1$, a condição (ii) da Definição acima pode ser reescrita como

(i') $\rho(ab) = \sum a_0 b_0 \otimes a_1 b_1, \forall a, b \in A.$

(ii') $\rho(1_A) = 1_A \otimes 1_A.$

Note que se H é um álgebra de Hopf finito-dimensional, então A é um H-módulo à esquerda se, e somente se, A é um H^*-comódulo à direita. Além disso, o subespaço dos elementos invariantes A^H é uma subálgebra de A. De fato, pois se $a, b \in A^H$, e $h \in H$, temos

$$h \cdot (ab) = \sum_{(h)} (h_1 \cdot a)(h_2 \cdot b) = \sum_{(h)} (\varepsilon(h_1)a)(\varepsilon(h_2)b) = \sum_{(h)} \varepsilon(h_1\varepsilon(h_2))ab = \varepsilon(h)ab$$

Exemplo 6.1.3. *Sejam H uma álgebra de Hopf e A uma $\Bbbk$-álgebra qualquer. Então H age à esquerda sobre A via a aplicação $\cdot : H \otimes A \to A$, definida por $h \cdot a := \varepsilon(h)a$, para todo $a \in A$. Esta ação é chamada de ação trivial.*

Exemplo 6.1.4. *Sejam H uma álgebra de Hopf, A uma $\Bbbk$-álgebra e $f \in Hom_{\Bbbk}(H, A)$. Suponhamos adicionalmente que f é um morfismo de álgebras que possui um inverso convolutivo, o qual será denotado por f^{-1}. Neste caso, A possui uma estrutura de H-módulo álgebra à esquerda dada por $h \cdot a := \sum_{(h)} f(h_1)af^{-1}(h_2)$, onde $h \in H$ e $a \in A$. De fato, pois tomando $a, b \in A$ e $h \in H$, temos*

$$\begin{aligned} h \cdot (ab) &= \sum f(h_1)abf^{-1}(h_2) \\ &= \sum f(h_1)af^{-1}(h_2)f(h_3)bf^{-1}(h_2) \\ &= \sum (h_1 \cdot a)(h_2 \cdot b) \end{aligned}$$

e $h \cdot 1_A = \sum f(h_1)1_A f^{-1}(h_2) = \sum f(h_1)f^{-1}(h_2) = \varepsilon(h)1_A$. Esta ação é chamada de ação interna de H sobre A. Neste caso, também dizemos que a ação interna é implementada por f.

Observamos neste momento que na situação do exemplo acima, se I é um ideal de A, então I é um H-submódulo de A, pois $h \cdot a = f(h_1)af^{-1}(h_2) \in I$, para todos $a \in I$ e $h \in H$.

Suponhamos que H age em A pela esquerda, como no exemplo acima. Seja $B = \mathcal{I}m\, f$. Então B é uma subálgebra de A. Denotando agora por $\mathcal{Z}_A(B)$ o *centralizador de B em A*, ou seja, $\mathcal{Z}_A(B) := \{a \in A : ab = ba, \forall b \in B\}$ (Note que se $B = A$ então $\mathcal{Z}_A(A) = \mathcal{Z}(A)$, isto é, o centralizador de A em si mesmo é exatamente o centro de A. Assim, o centralizador generaliza o conceito de centro). Neste caso, se $a \in \mathcal{Z}_A(B)$, então $h \cdot a = \sum f(h_1)af^{-1}(h_2) = \sum f(h_1)f^{-1}(h_2)a = \varepsilon(h)a$, de onde segue que $a \in A^H$. Reciprocamente, se $a \in A^H$ e $b \in B$, então existe $h \in H$ tal que $f(h) = b$, e temos

$$\begin{aligned} ba = f(h)a &= \sum f(h_1\varepsilon(h_2))a \\ &= \sum f(h_1)a\varepsilon(h_2) \\ &= \sum f(h_1)af^{-1}(h_2)f(h_3) \\ &= \sum (h_1 \cdot a)f(h_2) \\ &= (\varepsilon(h_1)a)f(h_2) \\ &= af(\varepsilon(h_1)h_2) \\ &= af(h) \\ &= ab \end{aligned}$$

e segue que $a \in \mathcal{Z}_A(B)$. Portanto, $\mathcal{Z}_A(B) = A^H$. Como consequência deste fato, se tomamos f sobrejetora, então temos que $\mathcal{Z}(A) = A^H$, ou seja, neste caso o centro de A é exatamente o conjunto dos elementos de A sobre os quais H age trivialmente.

Exemplo 6.1.5. *Seja H uma álgebra de Hopf com antípoda S. Então podemos considerar $End_{\Bbbk}(H)$ com a estrutura de álgebra de convolução. Sabemos que neste caso, S é a inversa convolutiva da identidade. Assim, pelo exemplo anterior, segue que a aplicação linear $\cdot : H \otimes H \to H$ dada por $h \cdot g := \sum_{(h)} h_1 g S(h_2)$ define uma ação de H em si mesmo. Esta ação é costumeiramente chamada de ação adjunta e denotada por ad. Assim, $ad : H \to End_{\Bbbk}(H)$, definida por $ad(h) := ad_h : g \mapsto h_1 g S(h_2)$ é um morfismo de álgebras. Como identidade é sobrejetor, segue que $\mathcal{Z}(H) = H^H$.*

Observamos agora que se G é um grupo e tomamos $H = \Bbbk G$, então a ação adjunta nada mais é do que a conjugação. De fato, pois neste caso, temos $S(g) = g^{-1}$, para todo $g \in G$. Assim, $ad_h(g) = h_1 g S(h_2) = hgh^{-1}$, uma vez que $\Delta(h) = h \otimes h$, para todo $h \in G$.

O próximo exemplo classifica as ações das álgebras de grupos em outras álgebras.

Exemplo 6.1.6. *Sejam G um grupo, $H = \Bbbk G$ e A um H-módulo álgebra. Então como $\Delta(g) = g \otimes g$, para todo $g \in G$, segue que $g \cdot ab = (g \cdot a)(g \cdot b)$, para todos $a, b \in A$, de*

modo que se definimos $\varphi : G \to \mathcal{A}ut_{\Bbbk}(A)$, *por* $\varphi(g) = \varphi_g : a \mapsto g \cdot a$, *onde* $\mathcal{A}ut_{\Bbbk}(A)$ *é o grupo dos* $\Bbbk$*-automorfismos de* A, *obtemos que* φ *é um homomorfismo de grupos. De fato, pois se* $g, h \in G$ *e* $a \in A$, *então* $\varphi(gh)(a) = (gh) \cdot a) = g \cdot (h \cdot a) = \varphi_g \circ \varphi_h(a)$. *Note que* φ_g *é um automorfismo de* A, *pois* $(\varphi_g \circ \varphi_{g^{-1}})(a) = g \cdot (g^{-1} \cdot a) = gg^{-1} \cdot a = a$, *para todo* $a \in A$. *Portanto, toda ação de* $\Bbbk G$ *em uma álgebra* A *determina um homomorfismo de grupos de* G *no grupo dos* $\Bbbk$*-automorfismos de* A.

Reciprocamente, se G *é um grupo,* A *é uma* $\Bbbk$*-álgebra e* $\varphi : G \to \mathcal{A}ut_{\Bbbk}(A)$ *é um homomorfismo de grupos, então a aplicação* $\Bbbk$*-linear* $\cdot : H \otimes A \to A$, *definida por* $(h, a) \mapsto h \cdot a := \varphi(h)(a)$ *define uma ação de* $\Bbbk G$ *em* A.

É comum dizermos então que um grupo age por automorfismos em uma álgebra. Note também que a subálgebra de invariantes não é nada mais que a parte fixa pela ação do grupo, pois se G é um grupo agindo numa álgebra A, ou seja, A é um $\Bbbk G$-módulo álgebra, então $A^G = A^{\Bbbk G} = \{a \in A : g \cdot a = \varepsilon(g)a, \forall g \in G\}$. Mantendo as notações do exemplo acima, temos que $a \in A^G$ se, e somente se, $\varphi_g(a) = \varepsilon(g)a = a$, para todo $g \in G$, ou seja, a é um ponto fixo para todo automorfismo da forma φ_g, $g \in G$.

No próximo exemplo queremos caracterizar as álgebras A que possuem uma estrutura de $\Bbbk G$-comódulo álgebra. Para tanto será necessário introduzir o conceito de álgebras graduadas, o que faremos a seguir.

Definição 6.1.7. *Sejam* G *um grupo e* A *uma* $\Bbbk$*-álgebra. Dizemos que* A *é uma álgebra graduada por* G, *ou que* A *é uma álgebra* G*-graduada, se existir uma família de subgrupos aditivos* $\{A_g\}_{g \in G}$ *de* A, *tais que* $A = \oplus_{g \in G} A_g$ *e* $A_g A_h \subseteq A_{gh}$, *para todos* $g, h \in G$.

A álgebra de grupo $\Bbbk G$ é claramente graduada por G. O anel de polinômios $\Bbbk[X]$ é $\mathbb{Z}$-graduado, bastando definir $\Bbbk[X]_n = 0$, se $n < 0$, $\Bbbk[X]_0 = \Bbbk$ e $\Bbbk[X]_n = \{p(X) : \partial p(X) = n\}$, se $n > 0$.

Exemplo 6.1.8. *Sejam* G *um grupo e* A *um* $\Bbbk G$*-comódulo álgebra via* $\rho : A \to A \otimes \Bbbk G$. *Então* A *é uma álgebra* G*-graduada. De fato, pois denotando* $\rho(a) = \sum_{g \in G} a_g \otimes g$, *vamos obter*

$$\sum_{g \in G} a_g \otimes g \otimes g = (id \otimes \Delta)\rho(a) = (\rho \otimes id)\rho(a) = \sum_{g,h \in G} (a_g)_h \otimes h \otimes g$$

e da independência linear dos elementos group-like de uma coálgebra, segue que $(a_g)_h = \delta_{gh}$, *de onde segue que* $\rho(a_g) = a_g \otimes g$. *Definindo* $A_g := \{a_g : a \in A\}$, *vamos obter que* $\{A_g\}_{g \in G}$ *é uma família de subgrupos aditivos de* A *tal que* $\sum_{g \in G} A_g = \oplus_{g \in G} A_g$, *pela injetividade de* ρ. *Além disso, como* $a = id(a) = (id \otimes \varepsilon)\rho(a) = \sum_{g \in G} a_g$, *segue que* $A = \oplus_{g \in G} A_g$. *Tomando agora* $a \in A_g$ *e* $b \in A_h$, *temos* $\rho(a) = a \otimes g$ *e* $\rho(b) = b \otimes h$, *de modo que* $\rho(ab) = \rho(a)\rho(b) = (a \otimes g)(b \otimes h) = ab \otimes gh$, *de onde se conclui que* $ab \in A_{gh}$. *Portanto,* $A_g A_h \subseteq A_{gh}$, *e, consequentemente,* A *é uma álgebra* G*-graduada, como queríamos mostrar.*

Reciprocamente, seja $A = \oplus_{g\in G} A_g$ uma álgebra G-graduada. Definindo $\rho : A \to A \otimes \Bbbk G$, por $\rho(a_g) = a_g \otimes g$ e estendendo por linearidade, obtemos que ρ define uma coação de $\Bbbk G$ em A à direita. Deixaremos os cálculos sob a responsabilidade do leitor.

6.2 O produto smash

Quando uma álgebra de Hopf age sobre uma $\Bbbk$-álgebra A, podemos introduzir uma nova estrutura de álgebra (associativa e unitária) no produto tensorial $A \otimes H$ da seguinte forma: na estrutura do $\Bbbk$-espaço vetorial $A \otimes H$ definimos uma multiplicação induzida pela fórmula

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

estendido por linearidade, onde $1_A \otimes 1_H$ é a unidade desta álgebra. De fato, pois se $a \otimes h \in A \otimes H$, então temos

$$(a \otimes h)(1_A \otimes 1_H) = \sum_{(h)} a(h_1 \cdot 1_A) \otimes h_2 1_H = \sum_{(h)} a\varepsilon(h_1) \otimes h_2 = \sum_{(h)} a \otimes \varepsilon(h_1)h_2 = \sum_{(h)} a \otimes h$$

e, de forma análoga, $(1_A \otimes 1_H)(a \otimes h) = a \otimes h$. Além disso, se $a, b, c \in A$ e $h, g, k \in H$, temos

$$\begin{aligned}
((a \otimes h)(b \otimes g))(c \otimes k) &= (a(h_1 \cdot b) \otimes h_2 g)(c \otimes k) \\
&= a(h_1 \cdot b)((h_2 g)_1 \cdot c) \otimes (h_2 g)_2 k \\
&= a(h_1 \cdot b)(h_2 g_1 \cdot c) \otimes h_3 g_2 k \\
&= a(h_1 \cdot b)(h_2 \cdot (g_1 \cdot c)) \otimes h_3 g_2 k \\
&= (a \otimes h)(b(g_1 \cdot c)) \otimes g_2 k \\
&= (a \otimes h)((b \otimes g)(c \otimes k))
\end{aligned}$$

Portanto, a regra acima define uma multiplicação associativa no produto tensorial. Para distinguir esta álgebra da álgebra do produto tensorial canônica, vamos denotá-la por $A\#H$ em lugar de $A \otimes H$. Também, um elemento desta nova álgebra será denotado por $a\#h$. Assim, temos $(a\#h)(b\#g) = a(h_1 \cdot b)\#h_2 g$, para todos $a, b \in A$ e $h, g \in H$. Vamos dar uma denominação para esta nova álgebra.

Definição 6.2.1. *A álgebra $A\#H$ introduzida acima é chamada de produto smash de A por H.*

Suponhamos que A seja um $\Bbbk G$-módulo à esquerda. Então, se $a\#h, b\#g \in A\#\Bbbk G$, temos que

$$(a\#h)(b\#g) = a(h_1 \cdot b)\#h_2 g = a(h \cdot b)\#hg$$

e segue que $A\#\Bbbk G$ nada mais é do que o skew anel de grupo costumeiramente denotado por $A * G$.

Vamos agora classificar os módulos sobre esta nova álgebra. Começamos observando o seguinte resultado.

Proposição 6.2.2. *Sejam H uma álgebra de Hopf e A um H-módulo álgebra à esquerda. Então A e H são subálgebras de $A\#H$.*

Demonstração. Basta observar que as aplicações $\Bbbk$-lineares $\varphi : A \to A\#H$ e $\psi : H \to A\#H$ definidas por $\varphi(a) = a\#1_H$ e $\psi(h) = 1_A\#h$, respectivamente, são monomorfismos de álgebras. De fato, pois se $a, b \in A$ e $h, g \in H$, temos

$$\varphi(ab) = (a\#1_H)(b\#1_H) = a(1_H \cdot b)\#1_H 1_H = ab\#1_H$$

e

$$\begin{aligned}
\psi(hg) &= (1_A\#h)(1_A\#g) \\
&= \sum_{(h)} 1_A(h_1 \cdot 1_A)\#h_2 g \\
&= \sum_{(h)} 1_A \varepsilon(h_1) 1_A \# h_2 g \\
&= \sum_{(h)} 1_A \# \varepsilon(h_1) h_2 g \\
&= 1_A \# hg
\end{aligned}$$

□

Segue deste resultado que todo $A\#H$-módulo à esquerda é um A-módulo à esquerda e também um H-módulo à esquerda. Isto induz a seguinte definição.

Definição 6.2.3. *Sejam H uma álgebra de Hopf, A um H-módulo álgebra à esquerda e M um $\Bbbk$-espaço vetorial. Dizemos que M é um (A, H)-módulo à esquerda, se:*

(i) M é um A-módulo à esquerda, via ação $\xi : a \otimes m \mapsto \xi(a \otimes m) := am$, $\forall a \in A, m \in M$.

(ii) M é um H-módulo à esquerda, via a ação $\triangleright : h \otimes m \mapsto h \triangleright m$, $\forall h \in H, m \in M$.

(iii) $h \triangleright (a(g \triangleright m)) = \sum_{(h)} (h_1 \cdot a)(h_2 g \triangleright m)$, $\forall a \in A, h, g \in H, m \in M$.

Observamos que a condição de compatibilidade (iii) pode ser substituida por

(iii′) $h \triangleright (am) = \sum_{(h)} (h_1 \cdot a)(h_2 \triangleright m)$, $\forall a \in A, h \in H, m \in M$.

De fato, pois tomando $g = 1_H$ em (iii), obtemos (iii′). Reciprocamente, tomando $g \triangleright m$ em lugar de m em (iii′), obtemos (iii). A condição (iii′) tem a seguinte interpretação. A condição de compatibilidade (iii) ou (iii′) equivale a dizer que o seguinte diagrama é comutativo

$$\begin{array}{ccc} H \otimes (A \otimes M) & \xrightarrow{id_H \otimes \xi} & H \otimes M \\ \Big\downarrow{\scriptstyle \cdot} & & \Big\downarrow{\scriptstyle \triangleright} \\ A \otimes M & \xrightarrow[\xi]{} & M \end{array}$$

o próximo resultado caracteriza os $A\#H$-módulos à esquerda.

Teorema 6.2.4. *Sejam H uma álgebra de Hopf, A um H-módulo à esquerda e M um $\Bbbk$-espaço vetorial. Então M é um $A\#H$-módulo à esquerda se, e somente se, M é um (A, H)-módulo à esuqerda.*

Demonstração. Se M é um $A\#H$-módulo à esquerda, então sabemos que M é tanto um A-módulo à esquerda como um H-módulo à esquerda, como visto antes. A condição de compatibilidade decorre do fato que as ações de A e de H sobre M são definidas via os monomorfismos que caracterizam A e H como subalgebras de $A\#H$ visto antes. Assim, se $h, \in H, a \in A$ e $m \in M$, então

$$\begin{aligned} h \triangleright (am)) &= (1_A \# h) \triangleright ((a \# 1_H) \triangleright m) \\ &= \Big(\sum_{(h)} 1_A (h_1 \cdot a) \# h_2 1_H \Big) \triangleright m \\ &= \sum_{(h)} ((h_1 \cdot a) \# h_2) \triangleright m \\ &= \Big(\sum_{(h)} (h_1 \cdot a)(1_H \cdot 1_A) \# 1_H h_2 \Big) \triangleright m \\ &= \sum_{(h)} \big((h_1 \cdot a) \# 1_H \big) \triangleright \big((1_A \# h_2) \triangleright m \big) \\ &= \sum_{(h)} (h_1 \cdot a)(h_2 \triangleright m) \end{aligned}$$

Reciprocamente, suponhamos que M é um (A, H)-módulo à esquerda. Definimos a ação de $A\#H$ sobre M da seguinte forma

$$\begin{array}{rccc} \bullet : & A\#H \otimes M & \longrightarrow & M \\ & a\#h & \mapsto & a(h \triangleright m) \end{array}$$

Vamos verificar que esta aplicação $\Bbbk$-linear de fato define uma ação de $A\#H$ sobre M.

Tomando $a, b \in A, h, g \in H, m \in M$, temos

$$1_{A\#H} \bullet m = (1_A \# 1_H) \bullet m = 1_A(1_H \triangleright m) = 1_A m = m$$

e

$$\begin{aligned}
(a\#h) \bullet \big((b\#g) \bullet m\big) &= (a\#h) \bullet \big(b(g \triangleright m)\big) \\
&= a\big(h \triangleright (b(g \triangleright m))\big) \\
&\overset{(iii)}{=} \sum_{(h)} a\big((h_1 \cdot b)(h_2 g \triangleright m)\big) \\
&= \sum_{(h)} \big(a(h_1 \cdot b)\#h_2 g\big) \bullet m \\
&= \big((a\#h)(b\#g)\big) \bullet m
\end{aligned}$$

Isto completa nossa prova. □

Exemplo 6.2.5. *Consideremos H uma álgebra de Hopf agindo sobre si m mesma via ação adjunta. Então $H\#H \simeq H \otimes H$, e segue que os (H,H)-módulos neste caso nada mais são do que os $H \otimes H$-módulos. De fato, basta observar que a aplicação $\varphi : H\#H \to H \otimes H$, definida por $\varphi(x\#h) = \sum_{(h)} xh_1 \otimes h_2$ define um isomorfismo de álgebras. Note que φ é claramente uma aplicação unitária. Além disso, se $x, y, g, h \in H$, então*

$$\begin{aligned}
\varphi\big((x\#h)(y\#g)\big) &= \varphi\big(\sum_{(h)} x(h_1 \cdot y)\#h_2 g\big) \\
&= \sum_{(h)} x(h_1 \cdot y)(h_2 g)_1 \otimes h_3 g_2 \\
&= \sum_{(h)} x(h_1 y S(h_2))h_3 g_1 \otimes h_4 g_2 \\
&= \sum_{(h)} xh_1 y\varepsilon(h_2) g_1 \otimes h_3 g_2 \\
&= \sum_{(h)} xh_1 y g_1 \otimes h_2 g_2 \\
&= \sum_{(h)} (xh_1 \otimes h_2)(y g_1 \otimes g_2) \\
&= \varphi(x\#h)\varphi(y\#g)
\end{aligned}$$

ou seja, φ é um morfismo de álgebras. Para ver que φ é um isomorfismo, basta mostrar que $\psi : H \otimes H \to H\#H$, definida por $\psi(x \otimes h) = \sum_{(h)} xS(h_1)\#h_2$ é uma inversa de φ. Um cálculo análogo ao feito acima mostra que ψ é um morfismo de álgebras. Além disso,

é claro que

$$x \otimes h \overset{\psi}{\to} \sum_{(h)} xS(h_1)\#h_2 \overset{\varphi}{\to} \sum_{(h)} xS(h_1)h_2 \otimes h_3 = \sum_{(h)} x\varepsilon(h_1) \otimes h_2 = x \otimes h$$

e também

$$x\#h \overset{\varphi}{\to} \sum_{(h)} xh_1 \otimes h_2 \overset{\psi}{\to} \sum_{(h)} xh_1S(h_2)\#h_3 = \sum_{(h)} x\varepsilon(h_1)\#h_2 = x\#h$$

Referências Bibliográficas

[1] N. Andruskiewitsch and W. Ferrer, *The beginnings of the theory of Hopf algebras*, Acta Appl. Math. 108(1)(2009), 3-17.

[2] M. Cohen and D. Fischman, *Hopf algebra actions*, J. Algebra 100 (1986), 363-379.

[3] M. Cohen and S. Montgomery, *Group-graded rings, smash products and group actions*, Trans. Amer. Math. Soc. 282 (1984), 237-258.

[4] S. Dăscălescu, C. Năstăsescu and S. Raianu, Hopf algebras: an introduction, Marcel Dekker, 2001.

[5] J. Dauns; Modules and rings, Cambridge University Press, 1994.

[6] V. Ferreira e L. Murakami, Álgebras de Hopf, Notas de Minicurso, XVIII Escola de Álgebra, Campinas, 2004.

[7] J. R. Fischer, *A Jacobson radical for Hopf module algebras*, J. Algebra, 34 (1975), 217-231.

[8] T. Y. Lam, Lecture on modules and rings, Graduate Texts in Mathematics 189, Springer-Verlang, 1999.

[9] S. Montgomery, Hopf algebras and their actions on rings, CBMS n. 82, American Mathematical Society, 1993.

[10] M. E. Sweedler, Hopf algebras, Benjamin, 1969.

[11] D. E. Radford, *A Hopf module characterization of Hopf algebras*, Trans. Amer. Math. Soc. 38(1)(1983), 8-10.

[12] D. E. Radford, Hopf Algebras, Series on Knots and Everything, v. 49, World Scientific Publishing Co., 2012.

[13] R. Underwood; Fundamental of Hopf algebras, Universitext, Springer, 2015.