Invariantes da ação de uma álgebra de Hopf em uma álgebra livre

Lucas Seidy Ogawa

Dissertação apresentada ao
Instituto de Matemática e Estatística
da Universidade de São Paulo
para obtenção do título de
Mestre em Ciências

Programa: Matemática
Orientadora: Prof.ª Lúcia Satie Ikemoto Murakami

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES

São Paulo
Fevereiro de 2024

Invariantes da ação de uma álgebra de Hopf em uma álgebra livre

Lucas Seidy Ogawa

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 20 de Fevereiro de 2024.

Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão julgadora:

Profª. Drª. Lúcia Satie Ikemoto Murakami (orientadora) – IME-USP
Prof. Dr. João Fernando Schwarz – Unicamp
Prof. Dr. Eliezer Batista – UFSC

Agradecimentos

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

Além disso, gostaria de agradecer a todos aqueles que me ajudaram ao longo desses dois anos. Mais especificamente, gostaria de agradecer aos meus amigos e colegas, aos professores, à minha família aos meus orientadores e todos aqueles que me ajudaram (de alguma forma) por todo o suporte oferecido.

Resumo

Lucas Seidy Ogawa. **Invariantes da ação de uma álgebra de Hopf em uma álgebra livre**. Dissertação (Mestrado). Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2024.

As álgebras de Hopf generalizam algumas classes bem abrangentes de álgebras como álgebras de grupo e álgebras envolventes universais de álgebras de Lie. Sendo assim, ao estudar as ações de álgebras de Hopf estamos generalizando o estudo de ações de grupos e de derivações de álgebras de Lie. Se H for uma álgebra de Hopf e V for um H-módulo, os invariantes são $V^H = \{v \in V \ : \ h \cdot v = \varepsilon(h)v \ \forall h \in H\}$. Assim, no caso particular em que a álgebra de Hopf é a álgebra de grupo, os invariantes coincidem exatamente com os elementos fixos pela ação de todos os elementos do grupo. E no outro caso conhecido, das álgebras de Lie, os invariantes são os elementos que são anulados pelos elementos da álgebra de Lie, ou seja, são as constantes. Sendo assim, podemos estender a ação de H em $R = T(V)$, de modo que R é uma H-módulo álgebra homogênea. Como essa ação é homogênea, os invariantes formarão uma subálgebra homogênea. Neste texto iremos estudar o comportamento dos invariantes desse tipo de ação.

Palavras-chave: Álgebras de Hopf. Ação homogênea. Invariantes.

Abstract

Lucas Seidy Ogawa. **Invariants of the action of a Hopf algebra in a free algebra**. Thesis (Master's). Institute of Mathematics and Statistics, University of São Paulo, São Paulo, 2024.

Hopf algebras generalize some big classes of algebras such as group algebras and universal enveloping algebras of Lie algebras. So, by studying their actions, we are generalizing the study of group actions and derivations of Lie algebras. If H is a Hopf algebra and V is a H-module, the invariants are $V^H = \{v \in V : h \cdot v = \varepsilon(h)v \ \forall h \in H\}$. So, in the case where H is a group algebra, the invariants are exactly the elements fixed by the action of all elements of the group. In the other case (Lie algebras), the invariants are the elements that are annihilated by the elements of the Lie algebra, that is, the constansts. So, we can extend the action of H in $R = T(V)$, the free algebra in V, making R an homogeneous H-module algebra. This means that the set of invariants will be an homogeneous subalgebra. In this text, we are going to study the behavior of the invariants of this action.

Keywords: Hopf algebras. Homogeneous actions. Invariants.

Sumário

Introdução

As álgebras de Hopf generalizam algumas classes de álgebras como álgebras de grupo e envolvente universal de álgebras de Lie. Além disso, se V é um H-módulo, em que H é uma álgebra de Hopf, essa ação de H se estende para uma ação em $T(V)$ e também para $\Bbbk[V]$. Sendo assim, iremos estudar os invariantes dessa ação.

No primeiro capítulo, vemos algumas dessas definições e outros resultados preliminares utilizados no texto, como o Lema de Higman e anel de quocientes simétricos de Martindale.

O segundo capítulo é o principal, nele verificamos que os invariantes são sempre livres e apresentamos algumas caracterizações para que eles sejam finitamente gerados. A primeira caracterização nos diz que essa subálgebra é finitamente gerada se e somente se o seu suporte é formado pelos elementos semi-invariantes de mesmo peso α de ordem finita. A segunda caracterização nos diz que essa álgebra é finitamente gerada se e somente se, sua série de Poincaré possuir inversa polinomial. A última nos diz que no caso em que a álgebra de Hopf é gerada por elementos group-like e skew primitivos, a subálgebra de invariantes é finitamente gerada exatamente no caso em que a ação é escalar.

No terceiro capítulo, colocamos algumas condições a mais para que a subálgebra de invariantes seja finitamente gerada como S-álgebra. Neste caso, estamos utilizando a ação dos grupos simétricos nas componentes homogêneas.

No último capítulo, estudamos o caso em que a álgebra de polinômios e temos um contraste com o caso não-comutativo. Neste caso, temos que a álgebra de invariantes é sempre finitamente gerada e em muitos casos é livre (teorema de Chevalley-Shephard-Todd).

Capítulo 1

Preliminares

Neste capítulo, iremos ver algumas preliminares, necessárias para o desenvolvimento do resto do texto. Neste capítulo, colocaremos algumas definições necessárias, mas alguns resultados mais básicos não serão demonstrados. As referências para as possíveis demonstrações se encontram no começo de cada seção.

1.1 Definições básicas

Nesta seção, veremos a definição de álgebra de Hopf. Álgebras de grupo e envolventes da álgebra de Lie são duas grandes classes de exemplos de álgebras de Hopf. As principais referências para esta seção são (Susan Montgomery, 1993), (Vitor O Ferreira e L. S. Murakami, 2020) e (Lam, 2001). Ao longo do texto, o seguinte lema será útil.

Lema 1.1.1. *Sejam U_1 e V_1 $\Bbbk$-subespaços de U_2 e V_2, respectivamente. Então $(U_1 \otimes V_2) \cap (U_2 \otimes V_1) = U_1 \otimes V_1$.*

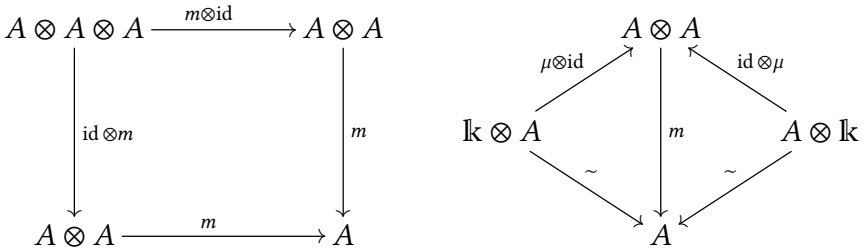
Demonstração: É claro que $U_1 \otimes V_1 \subseteq (U_1 \otimes V_2) \cap (U_2 \otimes V_1)$. Seja $x \in (U_1 \otimes V_2) \cap (U_2 \otimes V_1)$. Se $x = 0$, então $x \in U_1 \otimes V_1$. Suponha $x \neq 0$. Como, $x \in U_1 \otimes V_2$, podemos escrever $x = \sum_{i=1}^{n} u_i \otimes v_i$, com $u_i \in U_1$ para todo i e $\{u_i : i = 1, \dots, n\}$ linearmente independente. Para cada $j = 1, \dots, n$, seja $f_j \in U_2^*$ tal que $f_j(u_i) = \delta_{i,j}$. Como $x \in U_2 \otimes V_1$, $v_j = (f_j \otimes \mathrm{id})(x) \in V_1$, para todo j, isto é $x \in U_1 \otimes V_1$. □

1.1.1 Coálgebras

Sempre denotaremos por $\Bbbk$ um corpo e todas as álgebras serão associativas com unidade sobre $\Bbbk$. A multiplicação de uma álgebra A é um aplicação bilinear de $A \times A$ em A; assim podemos vê-la como aplicação linear $m : A \otimes A \to A$. Além disso, podemos considerar $\mu : \Bbbk \to A$, a única transformação linear tal que $\mu(1_\Bbbk) = 1_A$.

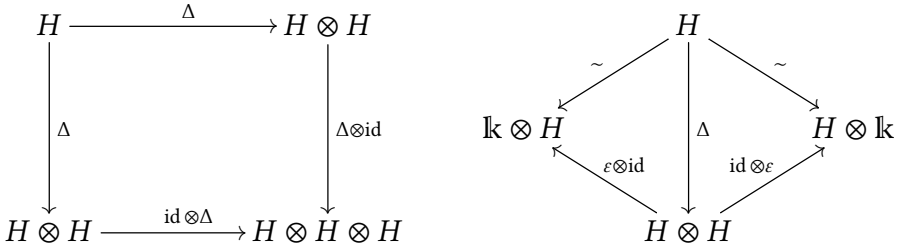
Com essas aplicações, as propriedades de associatividade e unidade são equivalentes à

comutatividade dos seguintes diagramas



onde os isomorfismos no último diagrama são os canônicos.

Definição 1.1.2. Uma *coálgebra* é uma terna (H, Δ, ε) em que H é um espaço vetorial e $\Delta : H \to H \otimes H$, $\varepsilon : \Bbbk \to H$ são aplicações lineares de modo que os seguintes diagramas são comutativos



As aplicações Δ e ε são chamados respectivamente de *comultiplicação* e *counidade*. Além disso, iremos nos referir à coálgebra como H.

Pode-se notar que para chegar na definição de uma coálgebra, basta invertermos os sentidos das flechas nos diagramas de álgebra associativa com unidade. Além disso, podemos aplicar a definição de álgebra sobre um anel comutativo, pois os diagramas são os mesmos.

Como os elementos do produto tensorial não são todos da forma $u \otimes v$, manusear elementos genéricos do produto tensorial pode ser trabalhoso. Dessa forma, utilizamos a notação de Sweddler para $\Delta(h)$. Denotamos

$$\Delta(h) = \sum_{(c)} h_{(1)} \otimes h_{(2)}.$$

Assim, a coassociatividade nos diz que

$$\sum_{(h)} \sum_{(h_{(1)})} h_{(1)_{(1)}} \otimes h_{(1)_{(2)}} \otimes h_{(2)} = \sum_{(h)} \sum_{(h_{(2)})} h_{(1)} \otimes h_{(2)_{(1)}} \otimes h_{(2)_{(2)}}.$$

Por causa dessa igualdade, iremos denotar qualquer um dos dois por $\sum_{(h)} h_{(1)} \otimes h_{(2)} \otimes h_{(3)}$. Ademais, a partir desse elemento, podemos aplicar $\Delta \otimes \mathrm{id} \otimes \mathrm{id}$, $\mathrm{id} \otimes \Delta \otimes \mathrm{id}$ ou $\mathrm{id} \otimes \mathrm{id} \otimes \Delta$ que chegará ao mesmo elemento (por causa da coassociatividade). Tal elemento será denotado por $\sum_{(h)} h_{(1)} \otimes h_{(2)} \otimes h_{(3)} \otimes h_{(4)}$. Assim, definimos indutivamente $\sum_{(h)} h_{(1)} \otimes \ldots \otimes h_{(n+1)} =$

$\Delta \otimes \mathrm{id}^{\otimes(n-1)} \left(\sum_{(h)} h_{(1)} \otimes \ldots \otimes h_{(n)} \right)$, para todo $n \geq 1$. Em (DĂSCĂLESCU *et al.*, 2001) 1.1.11, temos uma explicação do porquê essa notação funciona e como operar com ela.

Antes de prosseguirmos, vejamos alguns exemplos elucidativos. Aqui, a comultiplicação e a counidade estão definidas em uma base.

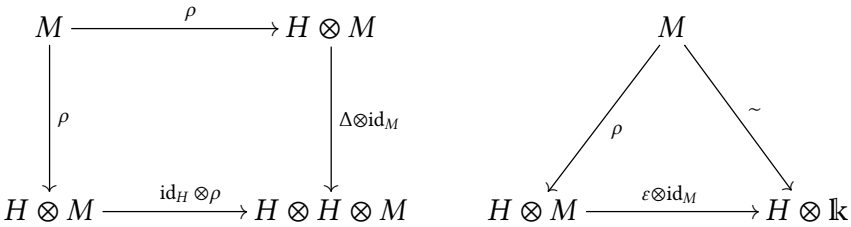
Exemplo 1.1.3. *Seja S um conjunto não vazio, e considere H o espaço vetorial de base S. Defina $\Delta(s) = s \otimes s$ e $\varepsilon(s) = 1$, para todo $s \in S$. Com essa estrutura H se torna uma coálgebra.*

Exemplo 1.1.4. *Seja n um inteiro positivo. Considere $S = \{e_{i,j} : 1 \leq i, j \leq n\}$ e H o espaço vetorial de base S. Defina $\Delta(e_{i,j}) = \sum_{k=1}^{n} e_{i,k} \otimes e_{k,j}$ e $\varepsilon(e_{i,j}) = \delta_{i,j}$. Essa coálgebra é chamada de coálgebra matricial e é denotada por $C_n(\Bbbk)$.*

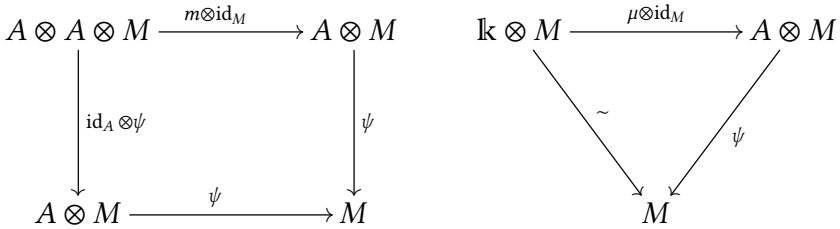
Os conceitos de ideais, subálgebras e módulos podem ser dualizados. Obtemos assim os equivalentes para coálgebras.

Definição 1.1.5. Seja (H, Δ, ε) uma coálgebra. Dizemos que um subespaço V de H é uma *subcoálgebra* (respectivamente *coideal à esquerda, coideal à direita*) se $\Delta(V) \subseteq V \otimes V$ (respectivamente: $\Delta(V) \subseteq H \otimes V$, $\Delta(V) \subseteq V \otimes H$). Dizemos que V é um *coideal* se $\Delta(V) \subseteq H \otimes V + V \otimes H$ e $\varepsilon(V) = 0$.

Se H é uma coálgebra, uma dupla (M, ρ) é um H-comódulo à esquerda, se M é um espaço vetorial e $\rho : M \to H \otimes M$ é uma aplicação linear tal que o seguinte diagrama seja comutativo



Observe que esses diagramas são a dualização dos diagramas de módulos, isto é, se A é uma álgebra então (M, ψ) é um A-módulo á esquerda se o seguinte diagrama for comutativo



Definição 1.1.6. Seja H uma coálgebra. Um elemento $g \in H$ é dito ser *group-like* se $g \neq 0$ e $\Delta(g) = g \otimes g$. O conjunto dos elementos group-like é denotado por $G(H)$. Sejam $g, h \in G(H)$. Um elemento c é dito ser (g, h)-*primitivo* se $\Delta(c) = c \otimes g + h \otimes c$. Podemos dizer simplesmente que c é *skew-primitivo* se não quisermos especificar os elementos g e h. O conjunto dos elementos (g, h)-primitivos são denotados por $P_{(g,h)}(H)$.

Assim, se H é uma coálgebra então $\varepsilon(G(H)) = 1$, e $G(H)$ é linearmente independente. Além disso, para todos $g, h \in G(H)$, o conjunto $P_{(g,h)}(H)$ é um subespaço de H e $\varepsilon(P_{(g,h)}(H)) = 0$ ((Vitor O Ferreira e L. S. Murakami, 2020) Proposição 2.4.9).

1.1.2 Dualidade

Nessa seção iremos definir uma álgebra a partir de uma coálgebra além de ver algumas propriedades dos espaços duais.

Definição 1.1.7. Seja V um espaço vetorial. Iremos denotar por $\langle ., . \rangle$ a seguinte aplicação bilinear

$$\begin{aligned} \langle ., . \rangle : V^* \times V &\to \Bbbk \\ (f, v) &\mapsto \langle f, v \rangle = f(v). \end{aligned}$$

Definição 1.1.8. Seja V um $\Bbbk$-espaço vetorial e X um subconjunto de V. Denotamos por $X^\perp$ o subespaço de V^* composto pelos elementos que se anulam em X, isto é $X^\perp = \{f \in V^* : \langle f, X \rangle = 0\}$. Analogamente, dado Y um subconjunto de V^*, denotamos por $Y^\perp = \{v \in V : \langle Y, v \rangle = 0\}$.

Proposição 1.1.9. *Sejam V um $\Bbbk$-espaço vetorial e W um subespaço de V e L um subespaço de V^*. Então $\dfrac{V^*}{W^\perp} \cong W^*$ e $\dfrac{V^*}{L} \cong L^\perp$ como espaços vetoriais.*

Demonstração: Seja U um subespaço de V tal que $V = U \oplus L^\perp$ e $p : V \to V$ a projeção em U nessa decomposição. Sendo assim, é fácil ver que podemos aplicar o teorema do isomorfismo nas aplicações

$$\begin{aligned} \phi : V^* &\to W^* \\ f &\mapsto f|_W \end{aligned}$$

e

$$\begin{aligned} \psi : V^* &\to L^\perp \\ f &\mapsto p \circ f. \end{aligned}$$

□

Lema 1.1.10. *Sejam V um $\Bbbk$-espaço vetorial e $\{M_\alpha\}$ uma família de subespaços de V. Então $\cap_\alpha (D_\alpha)^\perp = \left(\sum_\alpha D_\alpha\right)^\perp$.*

Demonstração: Para a primeira inclusão, seja $f \in \cap_\alpha (D_\alpha)^\perp$ e $v \in \sum_\alpha D_\alpha$. Escreva $v = v_1 + \cdots + v_n$, com $v_i \in D_{\alpha_i}$. Como $f \in D_{\alpha_i}^\perp$, segue que $f(v_i) = 0$, para todo i. Dessa forma $f(v) = 0$, ou seja $f \in \left(\sum_\alpha D_\alpha\right)^\perp$.

Para a outra inclusão, perceba que para todo β, vale $D_\beta \subseteq \sum_\alpha D_\alpha$. Dessa forma $\left(\sum_\alpha D_\alpha\right)^\perp \subseteq D_\beta^\perp$, e, portanto $\left(\sum_\alpha D_\alpha\right)^\perp \subseteq \cap_\alpha (D_\alpha)^\perp$. □

Lema 1.1.11. *Seja V um $\Bbbk$-espaço vetorial e sejam W um subespaço de V e L um subespaço de V^*. Então $(W^\perp)^\perp = W$ e $L \subseteq (L^\perp)^\perp$. Se V tiver dimensão finita, então a última igualdade é válida.*

Demonstração: Dado$w \in W$, para todo $f \in W\ \perp$, vale que $f(w) = 0$, de modo que $w \in (W^\perp)^\perp$. Por outro lado, seja $w \in (W^\perp)^\perp$ e considere $p \in V^*$ uma projeção em algum complemento de W (isto é, se $V = W \oplus U$, então p é a projeção em U). Assim dado $v \in V$, $p(v) = 0 \Leftrightarrow v \in W$. Dessa maneira, perceba que $p \in W^\perp$, e, portanto $p(w) = 0$. Podemos assim concluir que vale a primeira igualdade.

Mostrar que $L \subseteq (L^\perp)^\perp$ é análogo ao anterior. Se V possui dimensão finita, então pela Proposição 1.1.9, segue que

$$\begin{aligned}\dim(V^*) - \dim((L^\perp)^\perp) &= \dim\left(\frac{V^*}{(L^\perp)^\perp}\right)\\ &= \dim((L^\perp)^*) = \dim(L^\perp) \Rightarrow \dim((L^\perp)^\perp) = \dim(V) - \dim(L^\perp).\end{aligned}$$

Além disso,

$$\dim(L^\perp) = \dim\left(\frac{V^*}{L}\right) = \dim(V^*) - \dim(L).$$

Portanto $\dim(L) = \dim((L^\perp)^\perp)$. Como ambos possuem dimensão finita, vale a igualdade. □

Definição 1.1.12. Seja A uma álgebra. Então A^* é um A-módulo à esquerda via

$$\langle a \rightharpoonup f, b\rangle = \langle f, ba\rangle$$

e um A-módulo à direita via

$$\langle f \leftharpoonup a, b\rangle = \langle f, ab\rangle.$$

Dessa forma A^* é um A-bimódulo.

Proposição 1.1.13. *Sejam A uma álgebra e I um subespaço. Então I é um ideal à direita (resp. esquerda, bilateral) se e somente se $I^\perp$ é um A-submódulo à esquerda (resp. direita, bi-submódulo) de A^*. Além disso, dado $L \subseteq A^*$ um A-submódulo à esquerda (respectivamente direita, subbimódulo), temos que $L^\perp$ é um ideal à direita (resp. esquerda, bilateral) de A.*

Demonstração: Seja I um ideal à direita de A. Sejam $f \in I^\perp, a \in A, b \in I$. Assim $ba \in I$, pois I é um ideal à direita. Dessa forma,

$$\langle a \rightharpoonup f, b\rangle = \langle f, ba\rangle = 0.$$

Ou seja $A \rightharpoonup f \subseteq I^\perp$, de modo que $I^\perp$ é um A-submódulo à esquerda.

Por outro lado, suponha que $I^\perp$ seja um A-submódulo à esquerda e sejam $a \in A$, $b \in I$. Tome $p : A \to A$ uma projeção em um complemento de I (isto é, se U é um subespaço tal que $U \oplus I = A$, então p é a projeção em U). Perceba que dado $x \in A$, temos que $x \in I \Leftrightarrow p(x) = 0$. Como $I^\perp$ é um A-submódulo à esquerda, e $p \in I^\perp$, segue que $a \rightharpoonup p \in I^\perp$.

Dessa maneira

$$0 = \langle a \rightharpoonup p, b\rangle = \langle p, ba\rangle.$$

Dessa forma, $ba \in I$.

De modo análogo se prova o outro lado, e juntando os dois lados se chega no caso sem lateralidade.

Por fim, suponha que L seja um A-submódulo à esquerda de A^*, e sejam $a \in A, b \in L^\perp$, $f \in L$. Então, como L é submódulo, segue que $a \rightharpoonup f \in L$, e, portanto

$$0 = \langle a \rightharpoonup f, b\rangle = \langle f, ba\rangle \Rightarrow ba \in L^\perp.$$

□

Temos algumas relações entre a coálgebra, sua álgebra dual e o $\perp$.

Lema 1.1.14. *Se C uma coálgebra, então todo C^*-submódulo à esquerda de C é um coideal à direita de C (onde C é um C^*-módulo à esquerda via $\rightharpoonup$ com $f \rightharpoonup c = \sum_{(c)} f(c_{(2)})c_{(1)})$.*

Demonstração: Seja I um C^*-submódulo de C e seja $c \in I$. Seja $\{b_i : i \in \alpha\}$ uma base de C e escreva $\Delta(c) = \sum_{i\in\alpha} a_i \otimes b_i$. Para cada $l \in \alpha$, seja f_l o elemento dual de b_l nessa base. Assim, para todo $l \in \alpha$, temos

$$a_l = f_l \rightharpoonup c \in I.$$

Dessa forma, temos que $\Delta(c) \in I \otimes C$, ou seja, I é um coideal à direita. □

Lema 1.1.15. *Seja C uma coálgebra e sejam I subespaço de C^* e D subespaço de C.*

(i) Se I é um ideal à direita (esquerda) de C^*, então $I^\perp$ é um coideal à direita (esquerda) de C. Se C possuir dimensão finita, então vale a recíproca.

(ii) D é um coideal à direita (esquerda) se e somente se, $D^\perp$ é um ideal á direita (esquerda) de C^*.

(iii) D é uma subcoálgebra simples se e somente se D^* é uma álgebra simples (de dimensão finita) se e somente se $D^\perp$ é um ideal maximal de C^* de codimensão finita.

Demonstração: (i) Seja I um ideal à direita de C^*. Para mostrar que $I^\perp$ é um coideal de C, iremos mostrar que ele é submódulo, via $\leftharpoonup$. Sejam $c \in I^\perp$, $f \in C^*$ e $g \in I$. Assim $g * f \in I$, logo

$$\langle g, c \leftharpoonup f\rangle = \sum_{(c)} f(c_{(2)})g(c_{(1)}) = (g * f)(c) = 0.$$

Logo $I^\perp$ é um coideal à direita de C.

A recíproca pode ser mostrada usando o fato de que $(I^\perp)^\perp = I$ e o próximo item.

(ii) Seja D um coideal à direita de C^* e sejam $a \in D^\perp, b \in C^*$. Logo, para todo $d \in D$, temos

$$\langle ab, d\rangle = \sum_{(d)} \langle a, d_{(1)}\rangle\langle b, d_{(2)}\rangle \subseteq \langle a, D\rangle\langle b, C\rangle = 0.$$

Dessa forma, $ab \in D^\perp$, ou seja $D^\perp$ é um ideal à direita de C^*.

A recíproca pode ser mostrada usando o fato de que $(D^\perp)^\perp = D$ e o item anterior.

(iii) D é uma subcoálgebra se e somente se D é um coideal à direita e à esquerda de C, se e somente se $D^\perp$ é um ideal de C^*. Assim, se D é uma subcoálgebra simples, então D possui dimensão finita pelo Teorema Fundamental dos Comódulos (consultar por exemplo (Vitor O Ferreira e L. S. Murakami, 2020) Teorema 3.2.1), dessa forma D^* também possui dimensão finita.

Além disso, existe I ideal não nulo de C^* se e somente se, existe uma subcoálgebra não nula de D (basta pegar o $\perp$), isso mostra a equivalência entre as duas primeiras afirmações.

Para a equivalência entre a segunda e a terceira, utilize a função ϕ da Proposição 1.1.9. Com ela, podemos concluir que $\frac{C^*}{D^\perp} \cong D^*$ como $\Bbbk$-espaços. É fácil verificar que tal função é um morfismo de álgebras, de modo que $D^\perp$ seja um ideal de C^* e o último isomorfismo seja um isomorfismo de álgebras. O resultado segue do fato de que o quociente de uma álgebra por um ideal é simples se e somente se o ideal for maximal.

□

Dados V, W espaços vetoriais, existe uma aplicação linear

$$\begin{aligned} \iota : V^* \otimes W^* &\to (V \otimes W)^* \\ f \otimes g \mapsto \iota(f \otimes g) &: V \otimes W \to \Bbbk \\ v \otimes w &\mapsto f(v)g(w) \end{aligned}$$

Podemos agora construir uma álgebra no espaço dual de uma coálgebra da seguinte maneira. Seja (H, Δ, ε) uma coálgebra. Assim, H^* é uma álgebra com multiplicação $m = \Delta^* \circ \iota$ e unidade $\mu = \varepsilon^* \circ \Phi$, chamada de *álgebra dual*. A última função utilizada é o isomorfismo canônico Φ entre $\Bbbk$ e $\Bbbk^*$, em que $\Phi(\alpha)(\beta) = \alpha\beta$ cuja inversa é dada por $\Phi^{-1}(f) = f(1)$.

Exemplo 1.1.16. *Vejamos a estrutura de álgebra de H^* onde H é a coálgebra do Exemplo 1.1.3. Dados $f, g \in H^*$ e $s \in S$, temos*

$$m(f \otimes g)(s) = (\Delta^* \circ \iota)(f \otimes g)(s) = \iota(f \otimes g)(s \otimes s) = f(s)g(s).$$

Veja que como S é base de H, então H^* é isomorfa à álgebra das funções de S em $\Bbbk$ com produto ponto a ponto.

Exemplo 1.1.17. *Vejamos qual seria a estrutura de álgebra de H^* do Exemplo 1.1.4. Nova-*

mente, dados $f, g \in H^*$ *e* $1 \leq i, j \leq n$, *temos*

$$m(f \otimes g)(e_{i,j}) = (\Delta^* \circ \iota)(f \otimes g)(e_{i,j}) = \iota(f \otimes g)\left(\sum_{k=1}^{n} e_{i,k} \otimes e_{k,j}\right)$$
$$= \sum_{k=1}^{n} \iota(f \otimes g)\left(e_{i,k} \otimes e_{k,j}\right) = \sum_{k=1}^{n} f(e_{i,k})g(e_{k,j}).$$

Perceba que essa álgebra é isomorfa à algebra de matrizes $M_n(\Bbbk)$. *Como* H *tem dimensão finita, podemos considerar a base dual de* S, *denotada por* $S^* = \{e^*_{i,j} : 1 \leq i, j \leq n\}$. *Considere a transformação linear* $T : H^* \to M_n(\Bbbk)$ *tal que* $T(e^*_{i,j}) = b_{i,j}$ *em que* $b_{i,j}$ *é a matriz elementar, isto é:* $(b_{i,j})_{k,l} = \delta_{i,k}\delta_{j,l}$. *Usando as fórmulas anteriores e o fato de que essa transformação leva base em base, pode-se mostrar que isso é um isomorfismo de álgebras.*

Suponha agora que A seja uma $\Bbbk$-álgebra de dimensão finita. Então a aplicação ι é um isomorfismo, de modo que podemos considerar em A^*, a estrutura de coálgebra, dada por $\Delta_{A^*} = \iota^{-1} \circ m^*$ e $\varepsilon_{A^*} = \Phi^{-1} \circ \mu^*$. A demonstração da álgebra dual e coálgebra dual podem ser encontradas em (Vitor O Ferreira e L. S. Murakami, 2020), na seção 2.3.

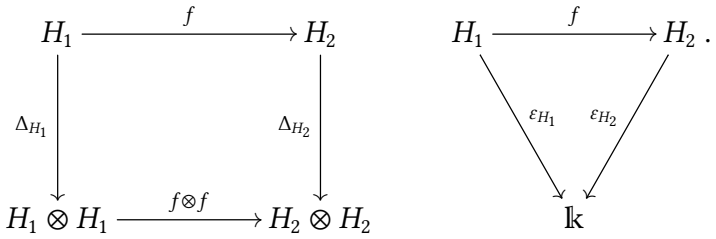
1.1.3 Morfismos

A partir de uma álgebra podemos falar de sua álgebra oposta e de uma coálgebra, podemos falar de sua coálgebra co-oposta.

Definição 1.1.18. Sejam (A, m, μ) uma álgebra e (C, Δ, ε) uma coálgebra. A *álgebra oposta* de A, denotada por A^{op} é a álgebra $(A, m \circ \tau, \mu)$, e *coálgebra co-oposta* denotada por C^{cop} é a coálgebra $(C, \tau \otimes \Delta, \varepsilon)$. Aqui $\tau : A \otimes B \to B \otimes A$ é definida por $\tau(a \otimes b) = b \otimes a$. Dizemos A é comutativa, se $A = A^{\text{op}}$ e que C é cocomutativa, se $C = C^{\text{cop}}$.

Assim como existem morfismos de álgebras, podemos também falar de morfismos de coálgebras.

Definição 1.1.19. Sejam H_1, H_2 coálgebras e $f : H_1 \to H_2$ uma transformação linear. Dizemos que f é um *morfismo de coálgebras* se os seguintes diagramas comutam



Utilizando a notação de Sweedler, isto é equivalente a dizer que

$$\sum_{(f(h))} f(h)_{(1)} \otimes f(h)_{(2)} = \sum_{(h)} f(h_{(1)}) \otimes f(h_{(2)}) \text{ e } \varepsilon_{H_2}(f(h)) = \varepsilon_{H_1}(h), \forall h \in H_1.$$

Dizemos que f é um *antimorfismo de coálgebras* se $f : H_1 \to H_2^{\text{cop}}$ for um morfismo de coálgebras. Analogamente, um transformação linear $f : A_1 \to A_2$ é um *antimorfismo de*

álgebras, se $f : A_1 \to A_2^{\text{op}}$ for um morfismo de álgebras.

Sejam H_1, H_2 são coálgebras e $F : H_1 \to H_2$ um morfismo de coálgebras. Então a aplicação transposta $F^* : H_2^* \to H_1^*$ é um morfismo de álgebras. Reciprocamente, se A_1, A_2 são álgebras de dimensão finita e $G : A_1 \to A_2$ é um morfismo de álgebras, então $G^* : A_2^* \to A_1^*$ é um morfismo de coálgebras. Para verificar isso, basta dualizar os diagramas (percebendo que se $f : A \to B, g : B \to C$ são aplicações lineares, então $(g \circ f)^* = f^* \circ g^*$).

1.1.4 Álgebras de Hopf

As biálgebras são espaços vetoriais que possuem tanto uma estrutura de álgebra quanto de coálgebra com uma compatibilidade. Além disso, álgebras de Hopf são biálgebras que possuem uma propriedade adicional que será vista adiante. Primeiramente, perceba que se A e B são álgebras, então $A \otimes B$ é uma álgebra cujo produto é dado por $(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2)$.

Definição 1.1.20. Seja (H, m, μ) uma álgebra tal que (H, Δ, ε) seja uma coálgebra. Dizemos que $(H, m, \mu, \Delta, \varepsilon)$ é uma *biálgebra* se Δ e ε forem morfismos de álgebras.

Se H é uma biálgebra, então 1_H é um elemento group-like e $G(H)$ é um monoide.

Definição 1.1.21. Seja H uma biálgebra. Um elemento $c \in H$ é dito ser *primitivo*, se for $(1_H, 1_H)$-primitivo.

Se H é uma biálgebra de dimensão finita, então H^* também é uma biálgebra com as estruturas definidas nas páginas anteriores.

Antes de passarmos para a definição de álgebras de Hopf, precisamos da álgebra de convolução.

Definição 1.1.22. Sejam H uma coálgebra e A uma álgebra. Podemos então, definir uma estrutura de álgebra em $\text{Hom}(H, A)$, definindo o produto de f e g como sendo

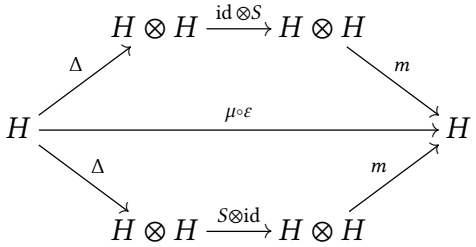
$$f * g = m_A \circ (f \otimes g) \circ \Delta_H.$$

Esse produto é chamado de *produto de convolução*.

Como uma biálgebra é tanto uma álgebra quanto uma coálgebra, podemos olhar para $\text{Hom}(H, H)$ com o produto de convolução. Com isso, conseguimos definir as álgebras de Hopf.

Definição 1.1.23. Seja H uma biálgebra. Se $\text{id}_H \in \text{Hom}(H, H)$ for inversível (no produto de convolução), então H será uma *álgebra de Hopf*. Geralmente a inversa é denotada por S

e chamada de *antípoda*. Isso quer dizer então que o seguinte diagrama comuta



ou pela notação de Sweddler,

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

para todo $h \in H$.

Seja H for uma álgebra de Hopf de dimensão finita com antípoda S. Então H^* também é uma álgebra de Hopf com $S_{H^*} = S^*$. Agora, se H é uma álgebra de Hopf (não necessariamente de dimensão finita), então sua antípoda é um antimorfismo de álgebras (isto é, $S(ab) = S(b)S(a)$). No caso em que a dimensão de H é finita, a antípoda é bijetora. Além disso, $G(H)$ é um grupo e $S(g) = g^{-1}$, para todo $g \in G(H)$. As demonstrações desses fatos podem ser encontrados em (Vitor O Ferreira e L. S. Murakami, 2020) seção 2.5.

Exemplo 1.1.24. *Uma álgebra de grupo possui uma estrutura de álgebra de Hopf. Mais especificamente, se* $\Bbbk$ *é um corpo e* G *é um grupo, então, a álgebra de grupo* $\Bbbk G$ *(com a estrutura de álgebra usual) é uma álgebra de Hopf, onde* $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$ *e* $S(g) = g^{-1}$ *para todo* $g \in G$ *(essas funções se estendem linearmente). As verificações das propriedades de álgebra de Hopf podem ser feitas facilmente através da base* G.

Exemplo 1.1.25. *Se* L *é uma álgebra de Lie, então, pode ser mostrado que a envolvente universal* $U(L)$ *é uma álgebra de Hopf, em que* $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0$ *e* $S(x) = -x$, *para todo* $x \in L$.

1.1.5 Integrais

Integrais são invariantes de H como módulo regular como veremos adiante. A existência de tal objeto ocorre somente em álgebras de Hopf de dimensão finita, e alguns resultados de álgebras de Hopf de dimensão finita estão ligados a ele.

Definição 1.1.26. Seja H uma biálgebra e seja $\Lambda \in H$. Dizemos que Λ é um *integral à esquerda*, se $\Lambda h = \varepsilon(h)\Lambda$, para todo $h \in H$. Tal espaço é denotado por $\int_H^l$. Analogamente, podemos definir *integral à direita*, e o conjunto de tais integrais será denotado por $\int_H^r$.

A existência de integrais não nulos ocorre se e somente se a álgebra de Hopf possui dimensão finita e nesse caso, ambos os espaços são unidimensionais((Vitor O Ferreira e L. S. Murakami, 2020) teorema 4.3.3). Um exemplo de resultado que mostra como podemos obter informações da álgebra de Hopf através dos integrais é o Teorema de Maschke.

Observação 1.1.27. Estamos adotando que um anel é *semissimples* se todo módulo for completamente redutível. De acordo com o teorema 2.5 do primeiro capítulo de (Lam, 2001), temos que A é semissimples se e somente se o módulo regular A for completamente redutível.

Teorema 1.1.28. *Se H é uma álgebra de Hopf, então H é uma álgebra semissimples se, e somente se, $\varepsilon(\Lambda) \neq 0$ para algum elemento integral à esquerda Λ.*

Demonstração: Suponha que H seja uma álgebra semissimples. Então, como ε é um morfismo de álgebras, $\ker(\varepsilon)$ é um ideal de H, ou seja, um submódulo.

Assim, tome I submódulo (ou seja ideal) à esquerda de H tal que $H = \ker(\varepsilon) \oplus I$. Perceba que I tem dimensão 1, pois, como espaço vetorial $I \cong H/\ker(\varepsilon) \cong \Bbbk$.

Seja $\Lambda \in I$ qualquer elemento não nulo. Vejamos que Λ é um integral à esquerda tal que $\varepsilon(\Lambda) \neq 0$. Se $\varepsilon(\Lambda) = 0$, então $\Lambda \in \ker(\varepsilon) \cap I = \{0\}$, contradição, logo, $\varepsilon(\Lambda) \neq 0$.

Para todo $h \in H$, temos $\varepsilon(h - \varepsilon(h)1) = \varepsilon(h) - \varepsilon(h)\varepsilon(1) = 0$, ou seja $h - \varepsilon(h)1 \in \ker(\varepsilon)$. Assim, $(h - \varepsilon(h)1)\Lambda \in \ker(\varepsilon) \cap I$, ou seja $(h - \varepsilon(h)1)\Lambda = 0$. Logo, temos,

$$h\Lambda = (h - \varepsilon(h)1)\Lambda + \varepsilon(h)\Lambda = \varepsilon(h)\Lambda.$$

Portanto $\Lambda \in \int_l^H$.

Suponha por outro lado que $\varepsilon(\int_l^H) \neq 0$, e tome $\Lambda \in \int_l^H$ com $\varepsilon(\Lambda) = 1$. Seja M um H-módulo à esquerda e N um H-submódulo. Podemos considerar uma projeção $\pi : M \to M$ sobre N qualquer (como espaços vetoriais). A partir dela, vamos construir um morfismo de H-módulos à esquerda $P : M \to M$ (que também será uma projeção) em N, dada por

$$\begin{aligned} P : M &\to M \\ m &\mapsto \sum_{(\Lambda)} \Lambda_{(1)} \cdot \pi(S(\Lambda_{(2)}) \cdot m) \end{aligned}$$

Como N é um submódulo de M, segue que a imagem de P está contida em N. Por outro lado, se $n \in N$, então

$$\begin{aligned} P(n) &= \sum_{(\Lambda)} \Lambda_{(1)} \cdot \pi(S(\Lambda_{(2)}) \cdot n) = \sum_{(\Lambda)} \Lambda_{(1)} \cdot (S(\Lambda_{(2)}) \cdot n) \\ &= \sum_{(\Lambda)} (\Lambda_{(1)} S(\Lambda_{(2)})) \cdot n = \mu\varepsilon(\Lambda) \cdot n = n. \end{aligned}$$

Logo, P é outra projeção em N, e assim $M = N \oplus \ker(P)$ (como espaço vetorial, por enquanto). Vejamos que P é um morfismo de módulos (daí $\ker(P)$ é um submódulo, o que mostra que M é completamente redutível).

Dados $h \in H$ e $m \in M$, perceba que

$$\begin{aligned}\sum_{(h)}\sum_{(\Lambda)} h_{(1)}\Lambda_{(1)} \otimes S(h_{(2)}\Lambda_{(2)}) \otimes h_{(3)} &= \sum_{(h)}\sum_{(\Lambda)} (\mathrm{id} \otimes S \otimes \mathrm{id})(h_{(1)}\Lambda_{(1)} \otimes h_{(2)}\Lambda_{(2)} \otimes h_{(3)}) \\ &= \sum_{(h)} (\mathrm{id} \otimes S \otimes \mathrm{id})(\Delta(h_{(1)}\Lambda) \otimes h_{(2)}) \\ &= \sum_{(h)} (\mathrm{id} \otimes S \otimes \mathrm{id})(\Delta(\varepsilon(h_{(1)})\Lambda) \otimes h_{(2)}) \\ &= (\mathrm{id} \otimes S \otimes \mathrm{id})(\Delta(\Lambda) \otimes h) = \sum_{(\Lambda)} \Lambda_{(1)} \otimes S(\Lambda_{(2)}) \otimes h.\end{aligned}$$

Assim

$$\begin{aligned}h \cdot P(m) = \sum_{(\Lambda)} h \cdot (\Lambda_{(1)} \cdot \pi(S(\Lambda_{(2)}) \cdot m)) &= \sum_{(\Lambda)} (h\Lambda_{(1)}) \cdot \pi(S(\Lambda_{(2)}) \cdot m) \\ &= \sum_{(\Lambda)}\sum_{(h)} (h_{(1)}\Lambda_{(1)}) \cdot \pi(S(\Lambda_{(2)})\varepsilon(h_{(2)}) \cdot m) \\ &= \sum_{(\Lambda)}\sum_{(h)} (h_{(1)}\Lambda_{(1)}) \cdot \pi(S(\Lambda_{(2)})S(h_{(2)})h_{(3)} \cdot m) \\ &= \sum_{(\Lambda)}\sum_{(h)} (h_{(1)}\Lambda_{(1)}) \cdot \pi(S(h_{(2)}\Lambda_{(2)})h_{(3)} \cdot m) \\ &= \sum_{(\Lambda)} \Lambda_{(1)} \cdot (\pi(S(\Lambda_{(2)})h \cdot m) = P(h \cdot m).\end{aligned}$$

□

Corolário 1.1.29. *Toda álgebra de Hopf semissimples tem dimensão finita.*

Demonstração: Se existe um elemento integral à esquerda Λ tal que $\varepsilon(\Lambda) \neq 0$, então $\Lambda \neq 0$, logo H tem dimensão finita. □

Podemos também aplicar para a álgebra de grupo.

Corolário 1.1.30. *Seja G um grupo finito e $\Bbbk$ um corpo. Assim $\Bbbk G$ é semissimples se e somente se a característica de $\Bbbk$ não divide a ordem de G.*

Demonstração: Perceba que $\Bbbk G$ tem a dimensão da ordem de G e portanto é finita. Assim, $\int_l^{\Bbbk G}$ tem dimensão 1. Assim, como $\Lambda = \sum_{g \in G} g$ é um integral à esquerda não nulo, todo integral à esquerda é um múltiplo escalar de Λ. Dessa forma, $\Bbbk G$ é semissimples, se e somente se existe um elemento integral à esquerda x tal que $\varepsilon(x) \neq 0$ se e somente se $|G| = \varepsilon(\Lambda) \neq 0$ se e somente se a caracterísitca de $\Bbbk$ não divide $|G|$. □

1.1.6 Ações de álgebras de Hopf

O nosso foco será o estudo de invariantes. Assim sendo, vamos estudar um pouco sobre eles e ver algumas construções.

Definição 1.1.31. Sejam H uma biálgebra e A uma álgebra. Dizemos que H age à esquerda em A, ou que A é uma *H-módulo àlgebra* à esquerda, se

(i) A é um H-módulo à esquerda (cuja ação será denotada por $h \cdot a$).

(ii) para todos $a, b \in A$ e $h \in H$, tem-se $h \cdot (ab) = \sum_{(h)} (h_{(1)} \cdot a)(h_{(2)} \cdot b)$.

(iii) $h \cdot 1_A = \varepsilon(h)1_A$.

Dado $h \in H$, dizemos que h age *trivialmente* em $a \in A$, se $h \cdot a = \varepsilon(h)a$. A subálgebra de invariantes de A sob a ação de H, denotada por A^H é formada pelos elementos de A nos quais todos os elementos de H agem trivialmente, isto é

$$A^H = \{a \in A \,:\, h \cdot a = \varepsilon(h)a \quad \forall h \in H\}.$$

Esse conjunto de invariantes forma uma subálgebra de A.

Exemplo 1.1.32. *Se A é uma álgebra e H é uma biálgebra, temos a ação trivial em que todos os elementos são invariantes. Ou seja, para todos $a \in A$ e $h \in H$, $h \cdot a = \varepsilon(h)a$.*

Antes do próximo exemplo, vamos precisar de uma definição importante que aparecerá recorrentemente ao longo do texto.

Definição 1.1.33. Seja V um $\Bbbk$-espaço. O espaço $T(V) = \bigoplus_{n \geq 0} V^{\otimes n}$ tem uma estrutura de álgebra, onde dados $v_1 \otimes \ldots \otimes v_n, w_1 \otimes \ldots w_m \in T(V)$ vale $(v_1 \otimes \ldots \otimes v_n)(w_1 \otimes \ldots w_m) = v_1 \otimes \ldots \otimes v_n \otimes w_1 \otimes \ldots w_m$. Essa álgebra é chamada de *álgebra tensorial.*

Observação 1.1.34. Se V é um $\Bbbk$-espaço de base X, então $T(V) \cong \Bbbk\langle X \rangle$.

Exemplo 1.1.35. *Sejam H uma biálgebra e V um H-módulo. Então, H induz uma ação em $T(V)$, por $h \cdot (v_1 \otimes \ldots \otimes v_n) = \sum_{(h)} (h_{(1)} \cdot v_1) \otimes \ldots \otimes (h_{(n)} \cdot v_n)$. Assim, $T(V)$ é uma H-módulo álgebra. Os invariantes dessa ação serão o nosso principal objeto de estudo.*

Exemplo 1.1.36. *No caso em que $H = \Bbbk G$ age em A, temos uma ação do grupo G em A, via a restrição da ação de $\Bbbk G$. Dessa forma, G age em A por automorfismos. Nesse caso, os invariantes são todos os elementos que são fixos por todos os elementos de G. No caso em que $H = U(L)$, temos uma ação por meio de derivações. Nesse caso, os invariantes são os elementos de A que se anulam quando um elemento de L age nele.*

Exemplo 1.1.37. *Seja G um grupo finito e considere a base dual $\{p_g \,:\, g \in G\}$ da base G de $\Bbbk G$. Assim, $H = (\Bbbk G)^*$ possui uma estrutura de álgebra de Hopf, em que a estrutura de álgebra é herdada da coálgebra $\Bbbk G$. Sua comultiplicação e counidade são dadas por*

$$\Delta(p_g) = \sum_{h \in G} p_h \otimes p_{h^{-1}g}; \quad \varepsilon(p_g) = \delta_{g,e} \quad \textit{para todo } g \in G.$$

Vejamos que uma álgebra A é uma H-módulo álgebra se e somente se for G-graduada. A álgebra A ser graduada significa que existe uma família de subespaços $\{A_g \,:\, g \in G\}$ tais que

(i) $A = \bigoplus_{x \in G} A_x$.

(ii) $1_A \in A_e$ *(e é a identidade de G).*

(iii) $A_gA_h \subseteq A_{gh}$.

Nesse caso temos que $A^H = A_e$.

Suponha que A seja G-graduada. Defina a estrutura de H-módulo em A da seguinte maneira: $p_g \cdot a = a_g$, *onde* a_g *é a componente homogênea de grau g de a. É fácil ver que* $p_g \cdot 1_A = \varepsilon(p_g)1_A$.

Dados $a, b \in A$, *temos*

$$ab = \left(\sum_{g\in G} a_g\right)\left(\sum_{g\in G} b_g\right) = \sum_{g\in G}\sum_{h\in G} a_g b_h = \sum_{g\in G}\left(\sum_{h\in G} a_{gh^{-1}}b_h\right).$$

Assim,

$$p_g \cdot (ab) = \sum_{h\in G} a_{gh^{-1}}b_h = \sum_{h\in G}(p_{gh^{-1}} \cdot a)(p_h \cdot b).$$

Suponha agora que A seja uma H-módulo álgebra. Para cada $g \in G$, *considere* $A_g = \{p_g \cdot a : a \in A\}$. *Assim, dado* $a \in A$, *temos*

$$a = 1_H \cdot a = \left(\sum_{g\in G} p_g\right) \cdot a = \sum_{g\in G}(p_g \cdot a).$$

Observe que dados $h, t \in G$ *e* $a_t \in A_t$ *vale* $p_h \cdot a_t = \delta_{h,t}a_t$. *De fato, considere* $a \in A$ *tal que* $a_t = p_t \cdot a$, *então*

$$p_h \cdot a_t = p_h \cdot (p_t \cdot a) = p_h p_t \cdot a = \delta_{h,t}p_t \cdot a = \delta_{h,t}a_t.$$

Assim, sejam $a_g \in A_g$ *tais que* $\sum_{g\in G} a_g = 0$. *Dado* $h \in G$, *temos*

$$0 = p_h \cdot 0 = p_h \cdot \left(\sum_{g\in G} a_g\right) = \sum_{g\in G} p_h \cdot a_g = \sum_{g\in G} \delta_{h,g}a_g = a_h.$$

Logo $a_h = 0$, *para todo* $h \in G$, *ou seja* $A = \bigoplus_{g\in G} A_g$.

Para todos $a, b \in A$, *temos*

$$\begin{aligned} p_{gh} \cdot ((p_g \cdot a)(p_h \cdot b)) &= \sum_{t\in G} \left(p_{ght^{-1}} \cdot (p_g \cdot a)\right)\left(p_t \cdot (p_h \cdot b)\right) \\ &= \sum_{t\in G} \left(p_{ght^{-1}}p_g\right) \cdot a\right)\left((p_t p_h) \cdot b\right) = (p_g \cdot a)(p_h \cdot b). \end{aligned}$$

Assim, $(p_g \cdot a)(p_h \cdot b) = p_{gh} \cdot ((p_g \cdot a)(p_h \cdot b))$, *o que mostra que* $A_gA_h \subseteq A_{gh}$.

Por fim, seja $a \in A^H$. *Então,* $p_e \cdot a = \varepsilon(e)a = a$, *e, portanto,* $A^H \subseteq A_e$. *Reciprocamente, seja* $a \in A_e$. *Então, como visto acima, temos que* $p_g \cdot a = \delta_{e,g}a = \varepsilon(p_g)a$. *Logo* $a \in A^H$, *de modo que* $A^H = A_e$.

Definição 1.1.38. Sejam H uma biálgebra e A uma H-módulo álgebra (à esquerda). Definimos o *produto smash*, denotado por $A\#H$ como sendo a álgebra cujo espaço vetorial

subjacente é $A \otimes H$ e cujo produto é dado por

$$(a\#h)(b\#g) = \sum_{(h)} a(h_{(1)} \cdot b)\#h_{(2)}g, \quad \text{para todos } a, b \in A, g, h \in H$$

onde $a\#g$ é o elemento $a \otimes g$.

Essa definição é parecida com o anel de grupo skew (na verdade coincide, se considerarmos a álgebra de grupo).

Definição 1.1.39. Sejam G um grupo finito, A um anel e $\phi : G \to \mathrm{Aut}(A)$ um homomorfismo de grupos. O anel de grupo skew, como conjunto, é $A * G = \{\sum_{g\in G} a_g g : a_g \in A, g \in G\}$ em que a soma é definida por

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g)g$$

e, dados $g, h \in G$ e $a, b \in A$

$$(ag)(bh) = a\phi(g)(b)gh.$$

Assim, define-se o produto em $A * G$ de modo a ser distributivo.

Observação 1.1.40. Sejam $H = \Bbbk G$ e A uma H-módulo álgebra. Temos um morfismo de grupos $\phi : G \to \mathrm{Aut}(A)$, dado por $\phi(g)(a) = g \cdot a$. Dessa forma, dados $g, h \in G$ e $a, b \in A$

$$(a\#h)(b\#g) = \sum_{(h)} a(h_{(1)} \cdot b)\#h_{(2)}g = a(h \cdot b)\#hg = a\phi(h)b\#hg.$$

Assim, observamos que a multiplicação coincide com a de $A * G$, e portanto $A * G = A\#\Bbbk G$.

Exemplo 1.1.41. *Sejam $H = U(L)$ e A é uma H-módulo álgebra. Assim, a ação de $U(L)$ é determinada pela ação de L. No caso em que $L = \Bbbk x$ é a álgebra de Lie de dimensão 1, o produto smash torna-se uma anel de polinômios skew $A\#U(L) = A[x; \delta]$, em que δ é derivação usual $\delta(a) = xa - ax$.*

Proposição 1.1.42. *Se H é uma biálgebra e A um H-módulo à esquerda, então as funções*

$$A \to A\#H$$
$$a \mapsto a\#1_H$$

e

$$H \to A\#H$$
$$h \mapsto 1_A\#h$$

são morfismos de álgebras.

Demonstração: Temos $(a\#1_H)(b\#1_H) = \sum_{(1_H)} a(1_{H(1)} \cdot b)\#1_{H(2)}1_H = ab\#1_H$.

Também temos $(1_A\#h)(1_A\#g) = \sum_{(h)} 1_A(h_{(1)} \cdot 1_A)\#h_{(2)}g = \sum_{(h)} 1_A\#\varepsilon(h_{(1)})h_{(2)}g = 1_A\#hg$. □

Sendo assim, iremos ver A e H como subálgebras de$A\#H$. Através dessa identificação, é fácil ver que, se $a \in A$ e $h \in H$, então $ah = a\#h$ (isto é, que $(a\#1_H)(1_A\#h) = a\#h$).

Como A é uma subálgebra de $A\#H$, podemos vê-lo tanto quanto A-módulo à esquerda como à direita. Quando H é uma álgebra de Hopf de dimensão finita, o produto smash é na verdade um A-módulo livre (dos dois lados).

Proposição 1.1.43. *Seja H uma álgebra de Hopf com antípoda S inversível (com inversa $\overline{S}$), agindo em uma álgebra A. Se $\{h_i : i \in I\}$ é uma base de H, então $\{1_A\#h_i : i \in I\}$ é uma base de $A\#H$ como A-módulo à esquerda e à direita. Em particular, se B é um subconjunto de A linearmente independente sobre $\Bbbk$, então, em $A\#H$, B será linearmente independente sobre H.*

Demonstração: Perceba que como A-módulo à esquerda, $A\#H$ é isomorfo a $A \otimes H$, e, portanto, como $A \otimes H$ é livre de base $\{1_A \otimes h_i : i \in I\}$ e a primeira afirmação vale.

Considere a transformação linear

$$\begin{aligned} \varphi : A\#H &\to H \otimes A \\ a\#h &\mapsto \sum_{(h)} h_{(2)} \otimes \overline{S}(h_{(1)}) \cdot a. \end{aligned}$$

Perceba que φ é um morfismo de A-módulos à direita, pois, dados $a, b \in A$ e $h \in H$, temos

$$\begin{aligned} \varphi((a\#h)(b\#1_H)) &= \varphi\left(\sum_{(h)} (a(h_{(1)}) \cdot b)\#h_{(2)}\right) \\ &= \sum_{(h)} h_{(3)} \otimes \overline{S}(h_{(2)}) \cdot (a(h_{(1)} \cdot b)) = \sum_{(h)} h_{(4)} \otimes (\overline{S}(h_{(3)}) \cdot a)(\overline{S}(h_{(2)})h_{(1)} \cdot b) \\ &= \sum_{(h)} h_{(2)} \otimes (\overline{S}(h_{(1)}) \cdot a)b = \varphi(a\#h)b. \end{aligned}$$

Considere a seguinte transformação linear

$$\begin{aligned} \psi : H \otimes A &\to A\#H \\ h \otimes a &\mapsto \sum_{(h)} h_{(1)} \cdot a\#h_{(2)} \end{aligned}$$

Dados $a \in A$ e $h \in H$, temos

$$\begin{aligned} \varphi(\psi(h \otimes a)) = \varphi\left(\sum_{(h)} h_{(1)} \cdot a\#h_{(2)}\right) &= \sum_{(h)} h_{(3)} \otimes \overline{S}(h_{(2)}) \cdot (h_{(1)} \cdot a) \\ = \sum_{(h)} h_{(2)} \otimes \varepsilon(h_{(1)})a &= h \otimes a. \end{aligned}$$

Também temos que

$$\psi(\varphi(a\#h)) = \psi\left(\sum_{(h)} h_{(2)} \otimes \overline{S}(h_{(1)}) \cdot a\right) = \sum_{(h)} h_{(2)} \cdot (\overline{S}(h_{(1)}) \cdot a)\#h_{(3)}$$
$$= \sum_{(h)} h_{(2)}\overline{S}(h_{(1)}) \cdot a\#h_{(3)} = \sum_{(h)} \varepsilon(h_{(1)})a\#h_{(2)} = a\#h,$$

o que mostra que $A\#H$ e $H \otimes A$ são isomorfos como A-módulos à direita. Além disso, $\{h_i \otimes 1_A : i \in I\}$ é base de $H \otimes A$ (como A-módulo à direita), e portanto, $\{1_A\#h_i : i \in I\}$ é base de $A\#H$ como A-módulo à direita. □

1.1.7 Álgebras de Hopf pontuadas

Definição 1.1.44. Seja C uma coálgebra.

1. O *coradical* C_0 de C é a soma de todas as subcoálgebras simples de C.
2. Dizemos que C é uma coálgebra *pontuada* se toda subcoálgebra simples de C for unidimensional.

Observação 1.1.45. Uma subcoálgebra tem dimensão 1 se e somente se for o subespaço gerado por um elemento group-like e C é pontuada se e somente se $C_0 = \Bbbk G(C)$.

Definição 1.1.46. Uma *filtração de coálgebra* é uma sequência de subcoálgebras $\{A_n\}_{n\geq 0}$ de C que satisfazem

1. $A_n \subseteq A_{n+1}$, para todo n.
2. $C = \bigcup_{n\geq 0} A_n$.
3. $\Delta(A_n) \subseteq \sum_{i=0}^{n} A_i \otimes A_{n-i}$, para todo n.

Vamos precisar dos seguintes lemas.

Lema 1.1.47. *Sejam C uma coálgebra e D uma subcoálgebra. Então, $D_0 = D \cap C_0$.*

Demonstração: É claro que $D_0 \subseteq D \cap C_0$. Para a outra inclusão, escreva $C_0 = \bigoplus_\alpha T_\alpha$, onde T_α são subcoálgebras simples. Vejamos que $D \cap C_0 = \bigoplus_\alpha (D \cap T_\alpha)$, e por ser soma de subcoálgebras simples de D, teremos a outra inclusão. Seja $d \in D \cap C_0$, e escreva $d = \sum_{i=1}^{n} t_i$, onde $t_i \in T_{\alpha_i}$. Para cada $i = 1, \dots, n$, seja $f_i \in C_0^*$, tal que $f_i|_{T_{\alpha_i}} = \varepsilon$ e $f_i|_{T_\beta} = 0$, para todo $\beta \neq \alpha_i$.

Assim, seja $d_i = \sum_{(d)} f_i(d_{(1)})d_{(2)}$. Como $D \cap C_0$ é subcoálgebra, temos que $d_i \in D \cap C_0$.

Por outro lado, como $d = \sum_{j=1}^{n} t_i$, temos que $\sum_{(d)} d_{(1)} \otimes d_{(2)} = \sum_{j=1}^{n} \sum_{(t_j)} t_{j(1)} \otimes t_{j(2)}$. Dessa forma

$$d_i = \sum_{(d)} f_i(d_{(1)})d_{(2)} = \sum_{j=1}^{n} \sum_{(t_j)} f_i(t_{j(1)})t_{j(2)} = \sum_{j\neq i} 0 + \sum_{(t_i)} \varepsilon(t_{i(1)})t_{i(2)} = t_i.$$

Assim, $t_i \in D \cap C_0$, para todo i. □

Definição 1.1.48. Seja R um anel. Definimos o *radical de Jacobson* de R como sendo $\mathrm{rad}(R) = \{r \in R : rM = 0 \quad \forall M \text{módulo simples}\}$.

As propriedades do Radical de Jacobson podem ser encontradas no segundo capítulo de (Lam, 2001).

Lema 1.1.49. *Seja C uma coálgebra. Então* $\mathrm{rad}(C^*) = C_0^\perp$.

Demonstração: Seja $J = C_0^\perp$ e escreva $C_0 = \sum_\alpha D_\alpha$, com D_α subcoálgebras simples. Pelo Lema 1.1.15, $M_\alpha = D_\alpha^\perp$ é um ideal maximal de C^* de codimensão finita. Então

$$\mathrm{rad}(C^*) \subseteq \cap_\alpha M_\alpha = \cap_\alpha (D_\alpha)^\perp = \left(\sum_\alpha D_\alpha\right)^\perp = J.$$

Por outro lado, como $J^\perp = (C_0^\perp)^\perp = C_0$, temos que $J \subseteq (J^\perp)^\perp = C_0^\perp$. □

Lema 1.1.50. *Seja $0 = V_0 \subseteq V_1 \subseteq \ldots$ uma cadeia infinita de subespaços de V. Então, para todo n*

$$\bigcap_{i=0}^{n+1} (V \otimes V_{n+1-i} + V_i \otimes V) = \sum_{i=1}^{n+1} V_i \otimes V_{n+2-i}.$$

Demonstração: Sejam $A = \bigcap_{i=0}^{n+1}(V \otimes V_{n+1-i} + V_i \otimes V)$ e $B = \sum_{i=1}^{n+1} V_i \otimes V_{n+2-i}$. Vejamos que $B \subseteq A$. Para isso, basta mostrar que, para cada i, j, $V_i \otimes V_{n+2-i} \subseteq V \otimes V_{n+1-j} + V_j \otimes V$. Se $i \leq j$, então $V_i \subseteq V_j$ e temos o que queremos. Caso contrário, $j < i \Rightarrow n+2-i \leq n+1-j$ e também temos o que queremos.

Para provar a outra inclusão, seja $v \in A$. Então $v \in V \otimes V_0 + V_{n+1} \otimes V = V_{n+1} \otimes V$. Para cada $i = 1, \ldots, n+1$, seja B_i base de V_i tal que se $j < k$, então $B_j \subseteq B_k$ e seja C base de V tal que $B_{n+1} \subseteq C$. Assim, como $v \in V_{n+1} \otimes V$, escreva $v = \sum_{j=1}^{n+1} \sum_{v_{j_i} \in B_j} v_{j_i} \otimes w_{j_i}$. Para concluir, vejamos que para cada $v_{j_i} \in B_j$, $w_{j_i} \in V_{n+2-j}$. Seja $f \in V^*$ o dual de v_{j_i} na base C. Como $v \in V \otimes V_{n+2-j} + V_{j-1} \otimes V$, segue que $w_{j_i} = (f \otimes \mathrm{id})(v) \in f(V) \otimes V_{n+2-j} + f(V_{j-1}) \otimes V = V_{n+2-j}$.

□

Temos assim, uma filtração canônica.

Proposição 1.1.51. *Seja C uma coálgebra e seja C_0 o seu coradical. Para cada $n > 0$, defina indutivamente $C_n = \Delta^{-1}(C \otimes C_{n-1} + C_0 \otimes C)$. Assim $\{C_n\}_{n \geq 0}$ é uma filtração, chamada de filtração coradical.*

Demonstração: Começamos definindo o wedge. Dados X e Y subespaços de C, $X \wedge Y$ é definido como $\ker(f)$, onde $f : C \to \frac{C}{X} \otimes \frac{C}{Y}$ é a aplicação dada por $f(c) = (c+X) \otimes (c+Y)$.

Assim, dados X, Y, Z subespaços de C, são válidos

1. $X \wedge Y = \Delta^{-1}(C \otimes Y + X \otimes C) = X^{\perp}Y^{\perp}$, onde o último produto é o produto de C^* como álgebra.

2. Dados X, Y, Z subespaços de C, vale $(X \wedge Y) \wedge Z = X \wedge (Y \wedge Z)$.

Assim, dado X subespaço de C, definimos $\wedge^0 X = \{0\}$ e para $n \geq 1$, $\wedge^n X = \wedge^{n-1} X \wedge X$. Dessa forma, vemos que $C_n = \wedge^{n+1} C_0$.

Além disso, se X e Y são subcoálgebras, então $X + Y \subseteq X \wedge Y$ pois dado $x \in X$, temos que $\Delta(x) \in X \otimes X \subseteq X \otimes C \subseteq C \otimes Y + X \otimes C$. Dessa forma, temos que $X \subseteq X \wedge Y$. De modo análogo, mostra-se que $Y \subseteq X \wedge Y$, e, portanto $X + Y \subseteq X \wedge Y$. Pelo Lema 1.1.15, temos que $X^{\perp}$ e $Y^{\perp}$ serão ideais (bilatereais) de C^*. Assim, $I = X^{\perp}Y^{\perp}$ é um ideal bilateral. Logo $I^{\perp} = (X^{\perp}Y^{\perp})^{\perp} = X \wedge Y$ será um coideal à esquerda e à direita, por causa do Lema 1.1.15, e, portanto, uma subcoálgebra.

Logo, como $C_{n+1} = C_n \wedge C_0$, temos que $C_n = C_n + C_0 \subseteq C_n \wedge C_0 = C_{n+1}$. Portanto, temos que C_n é uma cadeia ascendente de coálgebras.

Pela associatividade do wedge, temos que $C_n = (\wedge^i C_0) \wedge (\wedge^{n+1-i} C_0)$, para todo $0 \leq i \leq n+1$. Dessa forma

$$\Delta(C_n) \subseteq C \otimes \wedge^{n+1-i} C_0 + \wedge^i C_0 \otimes C = C \otimes C_{n-i} + C_{i-1} \otimes C,$$

para todo $1 \leq i \leq n$. Além disso, como C_n é uma coálgebra, essa inclusão também é válida para $i = 0$ e $i = n + 1$.

Portanto, pelo Lema 1.1.50, temos

$$\Delta(C_n) \subseteq \bigcap_{i=0}^{n+1} C \otimes C_{n-1} + C_{i-1} \otimes C = \sum_{i=1}^{n} C_i \otimes C_{n-i}.$$

Dessa forma, para que $\{C_n\}_{n \geq 0}$ seja uma filtração de coálgebras, basta mostrarmos que $\bigcup_{n \geq 0} C_n = C$. Como C é a união de todas as subcoálgebras de dimensão finita, basta mostrarmos que se D é uma subcoálgebra de dimensão finita, então $D \subseteq C_n$, para algum n.

Pelos Lemas 1.1.47 e 1.1.49, segue que $D_0 = D \cap C_0$ e $\mathrm{rad}(D^*) = D_0^{\perp}$. Como D tem dimensão finita, D_0 também, de modo que $(D_0^{\perp})^n = \mathrm{rad}(D^*)^n = 0$, para algum n, pois D^* é uma álgebra de dimensão finita. Assim

$$\wedge_D^n D_0 = ((D_0^{\perp})^n)^{\perp} = 0^{\perp} = D,$$

onde $\wedge_D$ é a operação wedge definida em D. É fácil ver que $\wedge_D^n D_0 \subseteq \wedge_C^n D_0$, de modo que

$$\wedge_D^n D_0 \subseteq \wedge_C^n D_0 \subseteq \wedge_C^n C_0 = C_{n-1}.$$

□

Antes do nosso resultado final, vamos precisar de mais um lema sobre dessa filtração canônica.

Lema 1.1.52. *Seja C uma coálgebra e $\{A_n\}_{n\geq 0}$ uma filtração de coálgebras de C. Então $C_0 \subseteq A_0$.*

Demonstração: Seja D uma subcoálgebra de $C = \bigcup_{n\geq 0} A_n$. Tome n mínimo tal que $D \cap A_n \neq 0$. Suponha por absurdo que $n > 0$ e escolha $0 \neq d \in D \cap A_n$. Então

1. $d \in A_n \Rightarrow \Delta(d) \in \sum_{i=0}^{n} A_i \otimes A_{n-i}$.
2. $d \in D \Rightarrow \Delta(d) \in D \otimes D$.

Se $\Delta(d) \in C \otimes A_0$, então $d = (\varepsilon \otimes \mathrm{id})(\Delta(d)) \in A_0$, de modo que $d \in (D \cap A_n) \cap A_0 \subseteq D \cap A_0$, absurdo, pois $d \neq 0$.

Assim, $\Delta(d) \notin C \otimes A_0$. Seja B uma base de A_0 e complete para B' base de C. Escreva $\Delta(d) = \sum_{x\in B'} d_x \otimes x$. Como $d \notin C \otimes A_0$, segue que existe $y \in B' \setminus B$ tal que $d_y \neq 0$. Seja f o elemento dual de y na base B'. Temos

$$\bar{d} = (\mathrm{id} \otimes f)(\Delta(d)) = d_y y \neq 0.$$

Dessa forma, por 1 e usando o fato de que $f|_{A_n} = 0$, segue que $\bar{d} \in A_{n-1}$ e por 2 $\bar{d} \in D$. Ou seja $0 \neq \bar{d} \in A_{n-1} \cap D$, contradição, logo $n = 0$.

Se D for uma coálgebra simples, então $D \subseteq A_0$. Como C_0 é a soma de todas as subcoálgebras simples, segue que $C_0 \subseteq A_0$. □

Chegamos então ao principal resultado desta seção.

Proposição 1.1.53. *Seja H uma álgebra de Hopf que contenha subespaços $A_0 \subseteq A_1$, onde A_0 é uma subálgebra com 1 tal que*

(i) A_1 gera H como álgebra e $A_0A_1, A_1A_0 \subseteq A_1$.

(ii) $\Delta(A_0) \subseteq A_0 \otimes A_0$, $\Delta(A_1) \subseteq A_0 \otimes A_1 + A_1 \otimes A_0$.

Para todo $n \geq 2$, seja $A_n = (A_1)^n$. Dessa maneira, $\{A_n\}_{n\geq 0}$ é uma filtração de coálgebras de H e $H_0 \subseteq A_0$. Se $A_0 = H_0$, então $A_n \subseteq H_n$, para todo n.

Demonstração: Como $1 \in A_0$, A_0 é uma subálgebra e A_1 é um A_0 bi-módulo, para todo $n > 0$, temos

$$\Delta(A_n) = \Delta((A_1)^n) = \Delta(A_1)^n \subseteq (A_1 \otimes A_0 + A_0 \otimes A_1)^n \subseteq \sum_{i=0}^{n} A_i \otimes A_{n-i}.$$

Como A_1 gera H como álgebra, segue que $\bigcup_{n\geq 0} A_n = H$. Logo, $\{A_n\}$ é uma filtração de coálgebra. Pelo Lema 1.1.52, temos que $H_0 \subseteq A_0$. Suponha que $A_0 = H_0$, e por indução, suponha também que $A_{n-1} \subseteq H_{n-1}$. Pelas inclusões anteriores, temos que

$$\Delta(A_n) \subseteq H_0 \otimes A_n + A_n \otimes A_{n-1} \subseteq H_0 \otimes H_n + H \otimes H_{n-1} \Rightarrow A_n \subseteq H_n.$$

□

Corolário 1.1.54. *Seja H uma álgebra de Hopf que é gerada por elementos group-like e skew primitivos (como álgebra). Então H é uma álgebra de Hopf pontuada.*

Demonstração: Sejam $A_0 = \Bbbk G(H)$ e $A_1 = A_0 + \sum_{g,h \in G(H)} P_{g,h}(H)$. Vejamos que A_0 e A_1 são subespaços que satisfazem às propriedades do Lema 1.1.53.

- A_0 é uma subálgebra de H, pois $G(H)$ é um grupo multiplicativo e base de A_0.
- A_1 gera H como álgebra por hipótese.
- Vejamos que $A_0 A_1 \subseteq A_1$.

  Como A_0 é uma subálgbra de H, basta mostrarmos que $A_0 P_{g,h}(H) \subseteq A_1$, para todos $g, h \in G(H)$. Sejam $g, g_1, h \in G(H)$ e $x \in H$ tais que

  $$\Delta(x) = x \otimes g + h \otimes x.$$

  Então

  $$\Delta(g_1 x) = \Delta(g_1)\Delta(x) = (g_1 \otimes g_1)(x \otimes g + h \otimes x) = g_1 x \otimes g_1 g + g_1 h \otimes g_1 x \Rightarrow g_1 x \in A_1.$$

- A_0 é uma subcoálgebra, e, portanto $\Delta(A_0) \subseteq A_0 \otimes A_0$
- É claro que $\Delta(A_0) \subseteq A_0 \otimes A_0$. Além disso, dado $x \in P_{g,h}(H)$, vale que $\Delta(x) = x \otimes g + h \otimes x \in A_1 \otimes A_0 + A_0 \otimes A_1$.

Assim A_0 e A_1 satisfazem tais propriedades. Logo $H_0 \subseteq A_0$. Logo, como H_0 é a soma de todas as subcoálgebras simples, segue que H possui apenas subcoálgebras simples de dimensão 1. □

1.2 Anéis graduados

Ao longo desta seção, iremos denotar por G um monoide (diferentemente do resto do texto em que G denotará um grupo) a menos que especificado o contrário, cuja operação será denotada por justaposição. Denotaremos por e a sua identidade. A principal referência é (Cohn, 1971).

Definição 1.2.1. Seja R um anel. Dizemos que R é *G-graduado*, se existe uma família $\{R_g : g \in G\}$ de subgrupos aditivos de R indexada por G tal que

(i) $1 \in R_e$.

(ii) $R = \bigoplus_{g \in G} R_g$.

(iii) Para todos $g, h \in G$, vale $R_g R_h \subseteq R_{gh}$.

Dado $g \in G$, um elemento $r \in R$ é dito ser homogêneo de grau g, se $r \in R_g$, e um elemento $r \in R$ será dito simplesmente homogêneo se existir $g \in G$ tal que r é homogêneo de grau g.

Quando dizemos que um anel R é G-graduado, já estamos deixando implícito a família de subgrupos aditivos $\{R_g : g \in G\}$. Além disso, poderemos simplesmente dizer que o anel R é graduado quando G estiver implícito.

Exemplo 1.2.2. *Seja S um anel e $R = S[x]$ o anel de polinômios. Para cada $n \geq 0$, considere $R_n = Sx^n$. Dessa forma, R é um anel $\mathbb{N}$-graduado.*

Exemplo 1.2.3. *Se R é um anel qualquer. Assim, podemos colocar $R_e = R$ e $R_g = 0$, para todo $g \neq e$. Entretanto, essa graduação não nos dá nenhuma estrutura interessante.*

Definição 1.2.4. Seja R um anel graduado. Um subgrupo aditivo S de R é dito ser *homogêneo* se $S = \bigoplus_{g\in G}(S \cap R_g)$. Neste caso, denotaremos $S_g = R_g \cap S$, para todo $g \in G$. Dada uma classe de objetos (por exemplo, subanel, ideal, etc...), dizemos que S é um objeto homogêneo dessa classe se for um objeto da classe e como subgrupo aditivo for homogêneo também.

Observação 1.2.5. Seja S um subgrupo aditivo de R. Assim, S será homogêneo se e somente se, para todo $s \in S$, com decomposição $s = \sum_{g\in G} s_g$, devemos ter que $s_g \in S$, para todo $g \in G$.

Proposição 1.2.6. *Seja R um anel graduado. Então*

(i) R_e é um subanel de R. Se G possuir a propriedadade do cancelamento (isto é, se dados $f, g, h \in G$ tais que $gf = gh$ ou $fg = hg$, devemos ter que $f = h$), então os dois últimos itens de 1.2.1 implicam em 1.2.1.

(ii) Seja I um ideal (à esquerda, à direita ou bilateral) de R, então I é homogêneo se e somente se for gerado por elementos homogêneos.

(iii) Se I é um ideal homogêneo, então $\frac{R}{I}$ é um anel graduado com $\left(\frac{R}{I}\right)_g = \frac{R_g + I}{I}$.

(iv) Se $\Bbbk$ é um corpo e R é uma $\Bbbk$-álgebra tal que $\Bbbk 1 \subseteq R_e$, então, existe uma base de R como $\Bbbk$-espaço formado por elementos homogêneos.

Demonstração: (i) Sabemos que R_e é um subgrupo aditivo. Para verificar que R_e é um subanel, basta verificar que $1 \in R_e$ e que R_e é fechado pelo produto. Como $ee = e$, temos que $R_eR_e \subseteq R_e$.

Seja $1 = \sum_{g\in G} 1_g$, a decomposição de 1 e seja h um elemento homogêneo de grau g'. Assim

$$h = h1 = h\left(\sum_{g\in G} 1_g\right) = \sum_{g\in G} h1_g.$$

Para cada $g \in G$, $h1_g$ é um elemento homogêneo de grau $g'g$. Como G possui a propriedade do cancelamento, sabemos que o grau de $h1_g$ é diferente de g', para todo $g \neq e$. Sendo assim, $h = h1_e$ (pois a decomposição de h é única). Logo 1_e age como unidade à direita para os elementos homogêneos, de modo a ser uma unidade à direita. De modo análogo, 1_e é uma unidade à esquerda, e, portanto, $1_e = 1$ (poderia concluir $1_e = 1$ só do fato de ser uma unidade à direita, pois toda unidade à direita é uma unidade em um anel com unidade). Assim $1 \in R_e$.

(ii) Nessa demonstração faremos para ideal à esquerda, mas qualquer outro caso é análogo. Suponha que I seja gerado por elementos homogêneos e seja $x \in I$. Sejam $h_1, \dots, h_t \in I$ homogêneos e $r_1, \dots, r_t \in R$ tais que $x = \sum_{i=1}^{t} r_i h_i$. Podemos supor sem perda de generalidade que r_i é homogêneo para todo i. Assim, para todo i, $r_i h_i \in I$ e é homogêneo. Dessa forma, se a decomposição de x for $x = \sum_{g \in G} x_g$, devemos ter que para cada $g \in G$, x_g será a soma de alguns $r_i h_i$ (pois a decomposição de x como soma de elementos homogêneos é única), e portanto $x_g \in I$, para todo $g \in G$, ou seja I é um ideal homogêneo.

Por outro lado, suponha que I seja um ideal (à esquerda) homogêneo. Se $x \in I$, com decomposição $x = \sum_{g \in G} x_g$, então $x_g \in I$ para todo $g \in G$, pois I é homogêneo. Assim x está no ideal (à esquerda) gerado pelos elementos homogêneos de I.

(iii) É claro que $\frac{R_g + I}{I}$ é um subgrupo aditivo de $\frac{R}{I}$, para todo $g \in G$ e que $\frac{R}{I} = \sum_{g \in G} \frac{R_g + I}{I}$ (pois $R = \sum_{g \in G} R_g$). Sejam $g_1, \dots, g_t \in G$ elementos distintos, e, para cada $i = 1, \dots, t$, tome $r_{g_i} + I \in \frac{R_{g_i} + I}{I}$ tais que $r_{g_1} + I + \cdots + r_{g_t} + I = 0 + I$. Assim, temos que $r_{g_1} + \cdots + r_{g_t} \in I$. Como I é um ideal homogêneo e os g_i são todos distintos, segue que $r_{g_i} \in I$, para todo i, ou seja, $r_{g_i} + I = 0 + I$, de modo que a soma anteriormente anunciada era direta.

(iv) Como $\Bbbk 1 \subseteq R_e$, para todo $g \in G$, temos $\Bbbk R_g = \Bbbk 1 R_g \subseteq R_e R_g \subseteq R_g$, de modo que R_g é um $\Bbbk$-espaço. Sendo assim, para cada $g \in G$, existe B_g uma base de R_g como $\Bbbk$-espaço. Se $B = \bigcup_{g \in G} B_g$, então B é uma base de R como $\Bbbk$-espaço formada por elementos homogêneos.

□

Definição 1.2.7. Sejam R e S anéis graduados. Um *homomorfismo de anéis graduados* é um homomorfismo de anéis $f : R \to S$ tal que $f(R_g) \subseteq S_g$. Um isomorfismo de anéis graduados é um homomorfismo de anéis graduados que é um isomorfismo de anéis.

Com isso, temos o teorema do isomorfismo para anéis graduados

Teorema 1.2.8. *Sejam R e S anéis graduados e $f : R \to S$ um homomorfismo de anéis graduados. Então*

(i) $\ker(f)$ *é um ideal homogêneo de R;*

(ii) $\mathrm{im}(f)$ *é um subanel homogêneo de S;*

(iii) existe um isomorfismo de anéis graduados $\bar{f} : \frac{R}{\ker(f)} \to \mathrm{im}(f)$ [1].

Demonstração: (i) Seja $x \in \ker(f)$, com decomposição $x = \sum_{g \in G} x_g$. Assim, para todo

[1] Como $\mathrm{im}(f)$ é um subanel homogêneo de um anel graduado, então $\mathrm{im}(f)$ é um anel graduado, com a gradução induzida de S.

$g \in G$, temos que $f(x_g) \in S_g$. Além disso,

$$0 = f(x) = \sum_{g \in G} f(x_g) \Rightarrow f(x_g) = 0 \quad \text{para todo } g \in G.$$

Assim, $x_g \in \ker(f)$, para todo $g \in G$, ou seja, $\ker(f)$ é um ideal homogêneo.

(ii) Seja $y \in \text{im}(f)$. Então, existe $x \in R$ tal que $f(x) = y$ e seja $x = \sum_{g \in G} x_g$ a sua decomposição. Como f é um homomorfismo de anéis graduados, segue que $f(x_g) \in S_g$, para todo $g \in G$. Dessa maneira, temos que

$$\sum_{g \in G} y_g = y = f(x) = \sum_{g \in G} f(x_g).$$

Ou seja $y_g = f(x_g) \in \text{im}(f)$, para todo $g \in G$. Assim, $\text{im}(f)$ é um subanel homogêneo.

(iii) Como f é um homomorfismo de anéis, então, tal isomorfismo $\bar{f}$ de anéis existe. Vejamos que $\bar{f}$ é um homomorfismo de anéis graduados. Sejam $g \in G$ e $x_g + I \in \left(\frac{R}{I}\right)_g = \frac{R_g + I}{I}$. Assim $\bar{f}(x_g + I) = f(x_g) \in S_g$, pois $x_g \in R_g$.

□

O próximo resultado será útil nos resultados principais. Como os invariantes da ação de uma álgebra de Hopf é uma subálgebra homogênea, sempre podemos considerar um conjunto gerador homogêneo.

Proposição 1.2.9. *Sejam $\Bbbk$ um corpo, H uma $\Bbbk$-biálgebra e A uma H-módulo álgebra (à esquerda) graduada tal que $\Bbbk 1_A \subseteq A_e$. Suponha que a ação de H em A seja graduada (isto é, $H \cdot A_g \subseteq A_g$, para todo $g \in G$). Então, A^H é uma subálgebra homogênea.*

Demonstração: Seja $a \in A^H$. Vejamos que $a_g \in A^H$, para todo $g \in G$. Como $a \in A^H$, temos

$$\sum_{g \in G} \varepsilon(h) a_g = \varepsilon(h) a = h \cdot a = h \cdot \left(\sum_{g \in G} a_g \right) = \sum_{g \in G} h \cdot a_g.$$

Como a ação é homogênea, segue que $h \cdot a_g \in A_g$, para todo $g \in G$. Por outro lado, como $\Bbbk 1_A \subseteq A_e$, então $\varepsilon(h) a_g = (\varepsilon(h) 1_A) a_g \in A_e A_g \subseteq A_g$. Assim, segue que $h \cdot a_g = \varepsilon(h) a_g$, para todo $g \in G$ e $h \in H$, isto é, $a_g \in A^H$, para todo $g \in G$. □

1.2.1 Anéis com algoritmo fraco

Nesta seção, iremos ver a definição de anéis com algoritmo fraco. Este conceito é um conceito auxiliar utilizado para uma demonstração do próximo capítulo sobre o fato da álgebra de invariantes ser livre. Seja R um anel (com unidade) com uma $\mathbb{N}$-graduação. Dado $n \in \mathbb{N}$, seja F_n como sendo o subgrupo aditivo gerado pelos elementos homogêneos de R de grau $\leq n$. Perceba que a família de subgrupos $(F_n)_{n \in \mathbb{N}}$ satisfaz

(i) $F_i \subseteq F_{i+1}$, para todo $i \in \mathbb{N}$.

(ii) $\bigcup_{n\geq 0} F_n = R$.

(iii) $F_iF_j \subseteq F_{i+j}$, para todos $i, j \in \mathbb{N}$.

(iv) $1 \in F_0$.

Qualquer família de subgrupos aditivos de R indexados por $\mathbb{N}$ que satisfaçam essas propriedades é chamada de *filtração* e o anel R é dito um *anel filtrado.*

Com essa definição, podemos considerar para todo anel filtrado a função $v : R \to \mathbb{N}_{-\infty} = \mathbb{N} \cup \{-\infty\}$ dada por

$$v(0) = -\infty \text{ e se } x \neq 0, v(x) = \min\{n \in \mathbb{N} : x \in F_n\} \tag{1.1}$$

Essa função possui as seguintes propriedades

(i) $v(x) \geq 0$, para todo $x \neq 0$ e $v(0) = -\infty$.

(ii) $v(x - y) \leq \max\{v(x), v(y)\}$.

(iii) $v(xy) \leq v(x) + v(y)$.

(iv) $v(1) = 0$.

Uma função com tais propriedades é chamada de *pseudo-valoração.* Podemos também fazer o caminho inverso e obter uma filtração através de uma pseudo-valoração ao considerar $F_n = \{x \in R : v(x) \leq n\}$. Ao longo desta subseção, se $X \subseteq R$, denotaremos por $\langle X \rangle$ o conjunto dos monômios em X (isto é o semigrupo gerado por X).

Exemplo 1.2.10. *Seja $\Bbbk$ um corpo (na verdade, poderia ser só um anel comutativo sem divisores de zero) qualquer. Para todo $f \in \Bbbk[x_1, \dots, x_n]$ (ou em $\Bbbk\langle x_1, \dots, x_n\rangle$) , seja $v(f)$ o grau do monômio lider. Essa pseudo-valoração veio da $\mathbb{N}$-graduação natural.*

Exemplo 1.2.11. *Seja p um primo. A valoração p-ádica $v_p : \mathbb{Z} \to \mathbb{N} \cup \{-\infty\}$ em $\mathbb{Z}$ é dada da seguinte forma: $v_p(0) = -\infty$ e dado $n \neq 0$ inteiro, $v_p(n) = x$ se p^x divide n e p^{x+1} não divide n.*

Assim como em álgebra linear podemos falar em depêndencia linear, aqui temos algo parecido, com o conceito de R-depêndencia.

Definição 1.2.12. Seja R um anel filtrado com pseudo-valoração associada v.

- Dizemos que uma família de elementos $(a_i)_{i\in I}$ é *R-dependente* à direita, se para algum $i \in I$ $a_i = 0$ ou se existem $i_1, \dots, i_r \in I$ e $b_1, \dots, b_r \in R$ tais que $v\left(\sum_{j=1}^{r} a_{i_j} b_j\right) < \max_j\{v(a_j) + v(b_j)\}$. Caso contrário, dizemos que essa família é R-independente à esquerda.
- Dizemos que b é *R-dependente* à direita em relação a uma família $(a_i)_{i\in I}$ se $b = 0$ ou se existem $i_1, \dots i_r \in I$ e $c_1, \dots, c_r \in R$ tais que $v\left(b - \sum_{j=1}^{r} a_{i_j} c_j\right) < v(b)$ e $\max_{j\leq r}\{v(a_{i_j}) + v(c_j)\} \leq v(b)$.

Por fim, temos a definição de anel com algoritmo fraco.

Definição 1.2.13. Seja R um anel filtrado com pseudo-valoração v. Dizemos que R possui o primeiro algoritmo fraco (à direita) se $v(ab) = v(a) + v(b)$, para todos $a, b \in R$. Dado $n \geq 2$, dizemos que R possui o *n-ésimo algoritmo fraco à direita* (com respeito a v) se

i R possui o primeiro algoritmo fraco (à direita).

ii Para todos $a_1, \dots, a_m$ elementos de R ($m \leq n$) tais que $\{a_1, \dots, a_m\}$ é R-dependente à direita e $v(a_1) \leq v(a_2) \leq \cdots \leq v(a_m)$ existe $i \leq n$ tal que a_i é R-dependente (à direita) de $\{a_1, \dots, a_{i-1}\}$.

Dizemos que R possui o *algoritmo fraco* se R possuir o n-ésimo algoritmo fraco (à direita), para todo $n \geq 1$.

Podemos definir todos esses conceitos de maneira análoga à esquerda. Neste texto iremos fazer somente com o lado direito por simplicidade de notação e o termo "à direita"será omitido.

Além disso, se $m \leq n$ são inteiros e R possui o n-ésimo algoritmo fraco então R possui o m-ésimo algoritmo fraco.

Podemos definir de maneira análoga todos esses conceitos à esquerda. Entretanto, um anel possui o n-ésimo algoritmo fraco à esquerda se e somente se possui n-ésimo algoritmo fraco à direita. Assim, dizemos que um anel filtrado R possui o algoritmo fraco se possuir alguma das duas condições equivalentes. Uma demonstração para este fato pode ser encontrada em (Cohn, 1971).

Nosso objetivo ao estudar esses conceitos é compreender como eles estão relacionados com álgebras livres.

Seja R um anel com uma pseudo-valoração v que possua o primeiro algoritmo fraco e seja X um conjunto R-independente. Para todos $a_{11}, a_{12}, \dots, a_{1n_1}, \dots a_{j1}, a_{j2}, a_{jn_j} \in R$, vale $v(\sum a_{ik}) \leq \max_i\{v(a_{i1}) + \cdots + v(a_{in_i})\}$. Esse último é chamado de *grau formal* dessa expressão. Suponha que $\{a_{ik}\} \subseteq X$ de modo que $\{a_{1k} : k = 1, \dots, j\}$ é R-independente. Suponha que $v(\sum a_{ik}) < \max_i\{v(a_{i1}) + \cdots + v(a_{in_i})\}$, e para cada $i = 1, \dots, j$, tome

$$b_i = \begin{cases} 1, & \text{se } n_i = 1 \\ a_{i2} \dots a_{in_i}, & \text{caso contrário} \end{cases}$$

Se $n_i > 1$, perceba que $v(a_{i2}) + \cdots + v(a_{in_i}) = v(a_{i2} \dots a_{in_i}) = v(a_{i2} \dots a_{in_i}) = v(b_i)$. Em qualquer caso, vale $v(a_{i1}) + v(a_{i2}) + \cdots + v(a_{in_i}) = v(a_{i1}) + v(b_i)$. Dessa maneira

$$v\left(\sum_{i=1}^{k} a_{i1}b_i\right) = v(\sum a_{ik}) < \max_i\{v(a_{i1}) + \cdots + v(a_{in_i})\} = \max_i\{v(a_{i1}) + v(b_i)\}.$$

Contradição com o fato de que $\{a_{1k} : k = 1, \dots, j\}$ é R-independente. Logo $v(\sum a_{ik}) = \max_i\{v(a_{i1}) + \cdots + v(a_{in_i})\}$.

Assim, se X é um subconjunto de R de modo que $\langle X \rangle$ gere R como $\Bbbk$-espaço, e $\overline{v} : X \to \mathbb{N}$ é uma função, definimos a valoração formal induzida de $v(\sum a_{ik}) = \max_i\{v(a_{i1} + a_{i2} + \cdots + a_{in_i})\}$.

Definição 1.2.14. Seja R um anel filtrado tal que $F_0 = \Bbbk$ é um anel de divisão.Um conjunto X formado por elementos de valoração positiva tal que $\langle X\rangle$ gera R como $\Bbbk$-espaço à direita e se $x \in X$, então x não é R-dependente de $X \setminus \{x\}$ é chamado de *base fraca de álgebra* de R.

Proposição 1.2.15. *Seja R um anel filtrado tal que $F_0 = \Bbbk$ é um anel de divisão. Então R possui uma base fraca de álgebra.*

Demonstração: Perceba que F_n é um $\Bbbk$-espaço para todo n, pois $F_nF_0 \subseteq F_n$. Dado $n > 0$, seja F'_n o subespaço de F_n gerado por $\{ab : a, b \in F_{n-1}, v(a) + v(b) < n\}$. Tome $X_n \subseteq F_n$ de modo que a sua projeção em $\dfrac{F_n}{F'_n}$ seja uma base desse espaço. Vejamos que se $X = \cup_{n>0} X_n$, então X é uma base fraca de álgebra de R.

Vejamos inicialmente que dado $x \in X$, x é R-independente de $X \setminus \{x\}$. Suponha que não seja e tome $x_1, \dots, x_h \in X \setminus \{x\}$, $b_1, \dots, b_h \in R$ tais que $v\left(x - \sum_{i=1}^{h} x_i b_i\right) < v(x) = n > 0$ e $v(x_i) + v(b_i) \leq n$, para todo $i = 1, \dots, h$, e sem perda de generalidade suponha que $v(x_1), \dots, v(x_m) < n$ e $v(x_{m+1}) = \cdots = v(x_h) = n$.

Assim, temos que $x - \sum_{i=1}^{h} x_i b_i \in F_{n-1} \subseteq F'_n$. Pela construção de F'_n sabemos que $x_1b_1 + \cdots + x_mb_m \in F'_n$, de modo que $x - \sum_{i=m+1}^{h} x_i b_i \in F'_n$. Nesse caso, $v(b_i) = 0$, para todo $i > m$, isto é, $b_i \in \Bbbk$. Assim, $x + F'_n$ seria combinação linear de $x_{m+1} + F'_n, \dots, x_m + F'_n$, contradição com a forma como X_n foi escolhido (perceba que um elemento de $y \in X_n$ deve satisfazer $v(y) = n$, pois $F_{n-1} \subseteq F'_{n-1}$).

Por fim, vejamos que todo elemento x de R é uma combinação linear de elementos em $\langle X\rangle$, por indução em $v(x)$. Se $v(x) = 0$, então $x \in \Bbbk$ é o polinômio constante. Suponha que $v(x) = n > 0$. Logo, existem $x_1, \dots, x_h \in F_n$ e $\alpha_1, \dots, \alpha_h \in \Bbbk$ tais que $x - \sum_{i=1}^{h} x_i\alpha_i \in F'_n \subseteq F_{n-1}F_{n-1}$. Vejamos que todo elemento de $F_{n-1}F_{n-1}$ é uma combinação linear de monômios em X. Seja $\alpha \in \Bbbk$ e $z \in F_{n-1}$. Assim, $v(\alpha z) \leq v(\alpha) + v(z) = v(z) < n$. Pela hipótese de indução αz é uma combinação linear de elementos em $\langle X\rangle$. Se $y, z \in F_{n-1}$, escreva $y = \sum_j x'_j\alpha_j$, onde x'_j é um monômio em X, para todo j. Dessa forma

$$yz = \sum_j (x'_j\alpha_j)z = \sum_j x'_j(\alpha_j z).$$

Pelo visto anterior $\alpha_j z$ deve ser uma combinação linear de elementos em $\langle X\rangle$, de modo que yz também é, isto é todo elemento de F'_n é combinação linear de elementos de $\langle X\rangle$. É claro que $\sum_i x_i\alpha_i$ é uma combinação linear de elementos de $\langle X\rangle$. Podemos concluir portanto que x é uma combinação linear de elementos em $\langle X\rangle$. □

O próximo teorema nos diz que o caso em que podemos tomar X R-independente é exatamente o caso em que R possui o algoritmo fraco.

Teorema 1.2.16. *Seja R um anel filtrado. Então R possui o algoritmo fraco se e somente se R possui o primeiro algoritmo fraco, $F_0 = \Bbbk$ é um anel de divisão e existe X uma base fraca de*

álgebra R-independente.

Demonstração: Suponha que R possui o algoritmo fraco. Então, R possui o primeiro algoritmo fraco. Vejamos que F_0 é um anel de divisão. Seja $a \in F_0$ não-nulo. Perceba que $\{a, 1\}$ é R-dependente, pois $v(a * 1 + 1 * (-a)) = v(0) < 0 = \max\{0, 0\} = \max\{v(a) + v(1), v(1) + v(-a)\}$. Logo, 1 é R-dependente de $\{a\}$, isto é, existe $b \in R$ tal que $v(b) = v(a)+v(b) \leq v(1) = 0$ e $v(1 - ab) < v(1)$, ou seja $1 - ab = 0$. Portanto, todo elemento possui de F_0 possui inverso à direita em F_0, de modo que F_0 é um anel de divisão.

Por fim, como F_0 é um anel de divisão, pela proposição anterior segue que R possui uma base fraca de álgebra X. Se X não for R-independente, então existe um subconjunto finito $\{x_1, \dots, x_m\}$ de X que é R-dependente. Sem perda de generalidade, podemos supor que $v(x_1) \leq \cdots \leq v(x_m)$. Logo, existiria $i \leq m$ tal que x_i é R-dependente de $a_1, \dots, a_{i-1}$, e, portanto R-dependente de $X \setminus \{x_i\}$, contradição. Logo X é R-independente.

Suponha agora que R satisfaz às segundas propriedade. Vejamos que R satisfaz o algoritmo fraco (à esquerda). Inicialmente, vejamos que $\langle X \rangle$ é linearmente independente como $\Bbbk$-espaço à direita. Suponha que $\langle X \rangle$ seja linearmente dependente com

$$\sum_{i \in I} x_i \alpha_i = 0,$$

onde $x_i \in \langle X \rangle$ e $\alpha_i \in \Bbbk$, para todo $i \in I$. Agrupando os monômios que começam com x em α_x, conseguimos achar

$$\alpha + \sum_{x \in X} x \alpha_x = 0,$$

com $\alpha \in \Bbbk$ e $\alpha_x \in R$, para todo $x \in X$. Assim, como X é R-independente, segue que

$$v(-\alpha) = v\left(\sum_{x \in X} x \alpha_x\right) = \max_{x \in X}\{v(x) + v(\alpha_x)\}.$$

Podemos concluir que para todo $x \in X$, vale $v(\alpha_x) < v(x) + v(\alpha_x) \leq v(-\alpha) \leq 0$, ou seja $\alpha_x = 0$, para todo $x \in X$. Dessa forma, segue que $\alpha = 0$. Contradição, ou seja, $\langle X \rangle$ é linearmente independente.

Fixe um monômio $y = x_1 \dots x_i$ com $v(y) = r$. Dado um monômio a que começa com y, defina a^* de modo que $a = ya^*$ e defina $a^* = 0$ caso contrário. Assim, temos um operador bem definido $*$ em R (pois os $\langle X \rangle$ é uma base).

Primeiramente, perceba que para todo $a \in R$, vale $v(a^*) \leq v(a) - r$. Para isso, escreva $a = ya^* + c$, com $c^* = 0$. Dessa forma, como X é R-independente, $\langle X \rangle$ é uma base e $a \in \langle X \rangle$, segue que

$$v(a) = \max\{v(ya^*), v(c)\} \Rightarrow v(y) + v(a^*) = v(ya^*) \leq v(a) \Rightarrow v(a^*) \leq v(a) - r.$$

Vejamos agora que para todos $a, b \in R$, vale

$$(ab)^* \equiv a^* b(\mod F_{v(b)-1}).$$

Suponha inicialmente que a é um monômio. Se $(ab)^* = 0$, então $a^* = 0$, e, portanto $(ab)^* = 0 = a^*b$. Se $a^* \neq 0$, então $a = ya^*$, de modo que $ab = ya^*b \Rightarrow (ab)^* = a^*b$. Suponha então que $a^* = 0$, mas $(ab)^* \neq 0$. Então $a = x_1 \dots x_l$, para algum $l < i$ (e $b = x_{l+1} \dots x_i (ab)^* + z$, onde nenhum monômio de z começa com $x_{l+1} \dots x_i$). Assim, $v(a) < v(y) = r$, e, portanto

$$v((ab^*)) \leq v(ab) - r = v(a) + v(b) - r < v(b) \Rightarrow v((ab)^*) \leq v(b) - 1,$$

de modo que $(ab)^* \equiv 0 = a^*b(\mod F_{v(b)-1})$. O caso para a geral segue por linearidade. Vejamos agora que R possui o algoritmo fraco, utilizando $*$ para algum monômio de forma específica. Seja $B = \{b_1, \dots, b_n\} \subseteq R$ um conjuntpo R-dependente à esquerda com $v(b_1) \geq v(b_2) \geq \cdots \geq v(b_n)$. Para concluir, vejamos que algum b_i é R-dependente à esquerda dos que seguem. Como B é R-dependente à esquerda, existem $a_1, \dots, a_n \in R$ tais que $v(a_1b_1 + \dots a_nb_n) < \max_i\{v(a_i) + v(b_i)\} = d$. Sem perda de generalidade, podemos omitir os termos em que $v(a_i) + v(b_i) < d$. De fato, sejam $I = \{i \in \{1, \dots, n\} : v(a_i) + v(b_i) = d\}$ e $J = \{1, \dots, n\} \setminus I$. Assim, temos $v\left(\sum_{i\in J} a_ib_i\right) \leq \max_{i\in J}\{v(a_ib_i)\} < d$. Portanto

$$\begin{aligned} v\left(\sum_{i\in I} a_ib_i\right) &= v\left(\sum_{i=1}^{n} a_ib_i - \sum_{i\in J} a_ib_i\right) \\ &\leq \max\left\{v\left(\sum_{i=1}^{n} a_ib_i\right), v\left(\sum_{i\in J} a_ib_i\right)\right\} < d = \max_{i\in I}\{v(a_ib_i)\}. \end{aligned}$$

Dessa maneira, temos que $\{b_i : i \in I\}$ também é R-dependente à esquerda. Fazendo essa omissão, vejamos que b_1 é R-dependente à esquerda de $B \setminus \{b_1\}$. Como $v(a_i) + v(b_i) = d$, segue que $v(a_i) \leq v(a_i)$, para todo i. Seja $r = v(a_1) = d - v(b_1)$ e seja y um monômio de a_1 com coeficiente $\alpha \neq 0$. Para y, vamos tomar o operador definido anterioremente.

Para todo $i = 1, \dots, n$, pelo que foi visto anteriormente, vale $v(a_i^*b_i - (a_ib_i)^*) < v(b_i) \leq v(b_1)$. Assim

$$v\left(\sum_{i=1}^{n} a_i^*b_i - \sum_{i=1}^{n}(a_ib_i)^*\right) \leq \max_i\{v(a_i^*b_i - (a_ib_i)^*)\} < v(b_1).$$

Como $v\left(\sum_{i=1}^{n}(a_ib_i)^*\right) = v\left(\left(\sum_{i=1}^{n} a_ib_i\right)^*\right) \leq v\left(\sum_{i=1}^{n} a_ib_i\right) - r = d - r = v(b_1)$, segue que

$$v\left(\sum_{i=1}^{n} a_i^*b_i\right) \leq \max\left\{v\left(\sum_{i=1}^{n} a_i^*b_i - \sum_{i=1}^{n}(a_ib_i)^*\right), v\left(\sum_{i=1}^{n}(a_ib_i)^*\right)\right\} < v(b_1).$$

Como $a_1^* \in \Bbbk \setminus \{0\}$, segue que $v(a_1^*) = 0$ e a_1^* possui inverso. Dividindo à direita pelo inverso de a_1^*, obtemos

$$v(b_1 + \sum_{i=2}^{n}(a_1^*)^{-1}a_i^*b_i) < v(b_1).$$

Por fim, perceba que

$$\begin{aligned}\max_{i\geq 2}\{v((a_1^*)^{-1}a_i^*)+v(b_i)\} &= \max_{i\geq 2}\{v(a_i^*)+v(b_i)\}\\ &\leq \max_{i\geq 2}\{v(a_i)-r+v(b_i)\}\\ &= d-r = v(b_1)\leq v(b_1).\end{aligned}$$

□

Com isso, temos o seguinte corolário.

Corolário 1.2.17. *Seja R um anel filtrado tal que $F_0 = \Bbbk$ é um corpo e R seja uma $\Bbbk$-álgebra (isto é $F_0 \subseteq Z(R)$). Então R é uma álgebra livre em um conjunto X e v é a valoração formal induzida de $v|_X$ se e somente se R possui o algoritmo fraco.*

Demonstração: Se R possui o algoritmo fraco, vimos que existe X uma base fraca de álgebra R-independente. Logo, a valoração v é induzida de $v|_X$. Além disso, como $\langle X\rangle$ é uma base de R (de acordo com a demonstração anterior), segue que R é livre em X.

Por outro lado, se R é uma álgebra livre em um conjunto X e v é a valoração formal induzida de $v|_X$, então R possui o primeiro algortimo fraco. Além disso, é claro que X é uma base fraca de álgebras R-independente. Portanto, R possui o algoritmo fraco. □

1.3 Anel de quocientes de Martindale simétrico

Nesta seção, iremos construir o anel de quocientes de Martindale simétrico de um anel primo. Este anel será útil no teorema da correspondência que será visto no próximo capítulo. Vamos sempre considerar R um anel primo. A principal referência utilizada foi (Passman, 1987).

Definição 1.3.1. Seja R um anel. Dizemos que um ideal I de R é *primo*, se dados A, B ideais de R tais que $AB \subseteq I$, devemos ter que $A \subseteq I$ ou $B \subseteq I$. Equivalentemente, se A e B são ideais à esquerda (ou à direita) de R tais que $AB \subseteq I$, então $A \subseteq I$ ou $B \subseteq I$. Dizemos que o anel R é *primo* se o ideal nulo for um ideal primo. Se A é um ideal à esquerda (respectivamente direita) de R, então A é um R-módulo à esquerda, que denotaremos por ${}_RA$ (resp. A_R).

Seja R um anel primo. Considere o conjunto $L = \{f : A \to R : 0 \neq A \lhd R, f \in {}_R\mathrm{Hom}(A,R)\}$. Dados $f : {}_RA \to {}_RR, g : {}_RB \to {}_RR$, dizemos que $f \sim g$, se $f|_{A\cap B} = g|_{A\cap B}$. Se $A \cap B = 0$, como R é um anel primo, então $AB \subseteq A\cap B = 0 \Rightarrow A = 0$ ou $B = 0$, de modo que $f|_{A\cap B}, g|_{A\cap B} \in L$. Dessa forma, veremos que $\sim$ é uma relação de equivalência e o conjunto quociente é um anel. Para isso, vamos precisar de um lema.

Lema 1.3.2. *Sejam $f \in L$ com domínio A e $0 \neq B \lhd R$, tal que $B\,\mathrm{im}(f) = 0$. Então $f = 0$. Em particular, $B \subseteq A$ é tal que $f(B) = 0$, então $f = 0$.*

Demonstração: Seja I o ideal gerado por $\mathrm{im}(f)$. Como B e I são ideais de R, $B \neq 0$ e R é um anel primo, segue que $\mathrm{im}(f) \subseteq I = 0$, e, portanto $f = 0$. Além disso, se $B \subseteq A$, então

dados $a \in A, b \in B$, temos $bf(a) = f(ba) = 0$, pois $ba \in B$. Assim $B\,\mathrm{im}(f) = 0$, e novamente, podemos concluir o resultado. □

Proposição 1.3.3. *A relação $\sim$ é uma relação de equivalência. Assim, denotaremos por $Q_l(R)$ o conjunto das classes de equivalência de L e $\overline{f}$ a classe de equivalência de $f \in {}_R\mathrm{Hom}(A, R)$. Então $Q_l(R)$ é um anel, cujas operações são dadas de forma natural. Tal anel é chamado de anel de Martindale à esquerda (podemos definir similarmente, o anel $Q_r(R)$ tomando homomorfismo de ideais à direita e o anel será chamado de anel de Martindale à direita).*

Demonstração: É claro que $\sim$ é reflexiva e simétrica. Sejam $f, g, h \in L$ com domínios A, B, C respectivamente, tais que $f \sim g$ e $g \sim h$. Assim, temos que $f|_{A\cap B} = g|_{A\cap B}$ e $g|_{B\cap C} = h|_{B\cap C}$. Dessa maneira

$$f|_{A\cap B\cap C} = (f|_{A\cap B})\,|_{A\cap B\cap C} = (g|_{A\cap B})\,|_{A\cap B\cap C} = g|_{A\cap B\cap C}.$$

De modo análogo, temos $h|_{A\cap B\cap C} = g|_{A\cap B\cap C}$. Logo $f|_{A\cap B\cap C} - h|_{A\cap B\cap C} = 0$. Assim, tome $f' = f|_{A\cap C}, f'' = f|_{A\cap B\cap C}, h' = h|_{A\cap C}$ e $h'' = h|_{A\cap B\cap C}$. Dado $x \in A\cap B\cap C$, temos $(f'-h')(x) = (f''-h'')(x) = 0$. Logo $(f'-h')(A\cap B\cap C) = 0$. Pelo Lema 1.3.2, segue que $f'-h' = 0$, isto é $f \sim h$.

Por fim, vejamos que as operações estão bem definidas, e que $Q_l(R)$ é de fato um anel.

Sejam $f, g \in L$ com domínios A, B respectivamente. Defina $h : f^{-1}(B) \to R$, por $h(x) = g(f(x))$. Essa h está, de fato bem definida, pois para todo $x \in f^{-1}(B)$, existe $f(x)$ e $f(x) \in B$, de modo que existe $g(f(x))$. Por fim, perceba que $0 \neq BA \subseteq f^{-1}(B)$, pois dados $a \in A$ e $b \in B$, temos que $f(ba) = bf(a) \in B$. Assim, é claro que $h \in L$. Seja $s = f|_{A\cap B} + g|_{A\cap B} \in L$. Defina, $\overline{f} + \overline{g} := \overline{s}$ e $\overline{f}\,\overline{g} := \overline{h}$.

É claro que se as operações estiverem bem definidas, então $Q_l(R)$ é um anel com unidade $\overline{\mathrm{id}_R}$. Assim, sejam $f_1, f_2, g_1, g_2 \in L$ com domínios respectivamente A_1, A_2, B_1, B_2 tais que $f_1 \sim f_2$ e $g_1 \sim g_2$. Dessa maneira, temos que $f_1|_{A_1\cap A_2} = f_2|_{A_1\cap A_2}$ e $g_1|_{B_1\cap B_2} = g_2|_{B_1\cap B_2}$. Assim, denote por $C = (A_1\cap A_2)\cap(B_1\cap B_2)$. Dado $x \in C$, temos

$$\begin{aligned}(f_1|_C + g_1|_C)(x) &= f_1|_C(x) + g_1|_C(x) = f_1|_{A_1\cap A_2}(x) + g_1|_{B_1\cap B_2}(x)\\ &= f_2|_{A_1\cap A_2}(x) + g_2|_{B_1\cap B_2}(x) = f_2|_C(x) + g_2|_C(x) = (f_2|_C + g_2|_C)(x).\end{aligned}$$

Dessa forma, a soma está bem definida. Seja $D = f_1^{-1}(B_1)\cap f_2^{-1}(B_2)$ e tome $x \in D$. Por definição, devemos ter que $x \in A_1\cap A_2$, de modo que $f_1(x) = f_1|_{A_1\cap A_2}(x) = f_2|_{A_1\cap A_2}(x) = f_2(x)$. Seja $y = f_1(x) = f_2(x)$. Como $x \in f_1^{-1}(B_1)$, segue que $f_1(x) \in B_1$. De modo análogo, segue que $f_2(x) \in B_2$, isto é, $y \in B_1\cap B_2$. Logo $g_1(y) = g_1|_{B_1\cap B_2}(y) = g_2|_{B_1\cap B_2}(y) = g_2(y)$. Portanto

$$(g_1f_1|_D)(x) = g_1f_1(x) = g_2f_2(x) = (g_2f_2|_D)(x).$$

Segue portanto que o produto está bem definido. □

Temos então o seguinte morfismo de anéis

$$\begin{aligned} \rho : R &\to Q_l(R) \\ r &\mapsto \overline{r_\rho} \end{aligned}$$

onde $r_\rho(a) = ar$, para todos $a, r \in R$. Seja $r \in R$ tal que $\overline{r_\rho} = 0$. Logo, existe $A \lhd R$ ideal não nulo tal que $r_\rho|_A = 0$. Assim, segue do Lema 1.3.2, que $r_\rho = 0$. Assim, $r = 1r = r_\rho(1) = 0$, ou seja ρ é injetora. Dessa forma, podemos ver R como um subanel de $Q_l(R)$. As próximas propriedades de $Q_l(R)$ vão o caracterizar de forma única.

Proposição 1.3.4. *Seja R um anel primo, com anel de Martindale à esquerda $Q_l = Q_l(R)$.*

(i) R é um subanel de $Q(R)$ com a mesma unidade.

(ii) Para todo $q \in Q_l$, existe um ideal não nulo A de R tal que $Aq \subseteq R$.

(iii) Dados $q \in Q_l$ e A ideal não nulo de R, se $Aq = 0$, então $q = 0$.

(iv) Para todo $f \in L$, com domínio A, existe $q \in Q_l$, tal que $aq = f(a)$, para todo $a \in A$.

Além disso, Q_l é o único R-anel que satisfaz essas propriedades (isto é, se existir um anel Q' que satisfaça as quatro propriedades, então existe um isomorfismo $\sigma : Q \to Q'$ de anéis e de R-módulos à esquerda simultaneamente).

Demonstração: Antes de demonstrarmos que Q_l possui essas propriedades, vamos precisar do seguinte fato: dados $f \in L$ com domínio A e $a \in A$, então $a_\rho f$ possui domínio R. Sendo assim, dado $r \in R$, temos

$$(a_\rho f)(r) = f(ra) = rf(a) = (f(a))_\rho(r).$$

Portanto $a_\rho f = (f(a))_\rho$. Assim, podemos demonstrar cada um dos itens da proposição.

(i) Segue dos comentários anteriores.

(ii) Seja $q \in Q_l$. Então existe $f \in L$ tal que $q = \overline{f}$. Seja A o domínio da f. Dado $a \in A$, temos $aq = \overline{a_\rho}\overline{f} = \overline{a_\rho f} = \overline{(f(a))_\rho} \in R$. Assim, $Aq \subseteq R$.

(iii) Sejam $q \in Q_l$ e $A \lhd R$ um ideal não nulo tal que $Aq = 0$. Seja $f \in L$ de domínio B tal que $q = \overline{f}$. Assim, seja $C = A \cap B$, e tome $c \in C$. De $Cq \subseteq Aq = 0$, segue que $\rho(f(c)) = \overline{(f(c))_\rho} = \overline{c_\rho f} = cq = 0$. Como ρ é injetora, segue que $f(C) = 0$. Assim, $q = \overline{f} = \overline{f|_C} = 0$.

(iv) Seja $q = \overline{f}$. Assim, dado $a \in A$, temos

$$aq = \overline{a_\rho}\overline{f} = \overline{a_\rho f} = \overline{(f(a))_\rho} = f(a).$$

Vejamos a recíproca agora. Sejam Q, Q' anéis com essas propriedades. Para cada $q \in Q$, seja $0 \neq A$ um ideal de R tal que $Aq \subseteq R$. Assim $f : {}_RA \to {}_RR$ dada por $f(a) = aq$ é um morfismo de R-módulos à esquerda. Logo, existe $q' \in Q'$ tal que $aq = f(a) = aq'$, para todo $a \in A$. Assim, q' é o único elemento de Q', para o qual existe um ideal A de R não nulo tal

que $aq = aq'$, para todo $a \in A$. De fato, se existir $q'' \in Q'$ e um ideal não nulo B de R tal que $bq = bq''$, para todo $b \in B$, então $A \cap B \neq 0$ e para todo $c \in C = A \cap B$, temos $cq' = cq = cq''$, de modo que $c(q' - q'') = 0$. Assim, $q' - q'' = 0$, ou seja, q' é de fato único. Sendo assim, defina $\sigma : Q \to Q'$ como sendo $\sigma(q) = q'$ o único elemento de Q' tal que $aq' = aq$, para todo a em algum ideal não nulo. Analogamente, construa $\tau : Q' \to Q$, de modo que, para todo $q' \in Q'$, exista um ideal A de R não nulo tal que, para todo $a \in A$, $aq' = a\tau(q')$.

Vejamos que $\tau = \sigma^{-1}$. Dado $q \in Q$, temos que $q_1 = \tau(\sigma(q))$ é um elemento de Q para o qual existe um $0 \neq A \lhd R$ tal que, para todo $a \in A$, vale $a\sigma(q) = aq_1$. Além disso, existe $0 \neq B \lhd R$ tal que $bq = b\sigma(q)$, para todo $b \in B$. Sendo assim, para todo $c \in A \cap B$, temos $cq = c\sigma(q) = cq_1$. Pela unicidade (mostrada acima), segue que $q_1 = q$. De modo análogo, mostra-se que $\tau\sigma$ é a identidade, ou seja, $\tau = \sigma^{-1}$.

Para concluir, vejamos que σ é um morfismo de anéis e de R-módulos à esquerda. Dados $q_1, q_2 \in Q$ e $r \in R$, existe um ideal $A_i \neq 0$, tal que $a_i q_i = a_i\sigma(q_i)$, para todo $a_i \in A_i$, com $i = 1, 2$. Seja $A = A_1 \cap A_2 \neq 0$. Assim, para todo $a \in A$, vale

$$a(q_1 + rq_2) = aq_1 + arq_2 = a\sigma(q_1) + ar\sigma(q_2) = a(\sigma(q_1) + r\sigma(q_2)).$$

Assim, $\sigma(q_1 + rq_2) = \sigma(q_1) + r\sigma(q_2)$, pela unicidade. Portanto, σ é um morfismo de R-módulos. Além disso, perceba que $B = A_2A_1 \subseteq A_1$ é um ideal não nulo. Dessa forma, $Bq_1 = A_2(A_1q_1) \subseteq A_2R = A_2$. Dado $b \in B$, temos

$$b(q_1q_2) = (bq_1)q_2 = (bq_1)\sigma(q_2) = (b\sigma(q_1))\sigma(q_2) = b(\sigma(q_1)\sigma(q_2)).$$

Logo, σ é multiplicativo, e, portanto, um morfismo de anéis. □

Com isso, podemos definir o objeto principal desta seção, chamado de anel de quocientes de Martindale simétrico. Iremos definir pelas propriedades que ele possui. Começaremos mostrando a unicidade, para depois, provarmos a existência.

Proposição 1.3.5. *Seja R um anel primo. Então, existe no máximo um anel $Q = Q(R)$ que satisfaz às seguintes propriedades.*

1 *R é um subanel de $Q(R)$ com a mesma unidade.*

2 *Para todo $q \in Q$, existem $A, B \lhd R$ ideais não nulos tais que $Aq, qB \subseteq R$.*

3 *Sejam $q \in Q$ e $I \lhd R$ ideal não nulo. Se $qI = 0$ ou $Iq = 0$, então $q = 0$.*

3' *Sejam $q \in Q$ e $I \lhd R$ ideal não nulo. Se $qI = 0$, então $q = 0$.*

3" *Sejam $q \in Q$ e $I \lhd R$ ideal não nulo. Se $Iq = 0$, então $q = 0$.*

4 *Sejam $A, B \lhd R$ ideais não nulos e $f : {}_RA \to {}_RR$, $g : B_R \to R_R$ morfismos de R-módulos à esquerda e à direita respectivamente. Suponha que, para todos $a \in A$ e $b \in B$, tenhamos $f(a)b = ag(b)$ (isto é, f e g são balanceados). Então, existe $q \in Q$ tal que $f(a) = aq$ e $g(b) = qb$, para todos $a \in A, b \in B$.*

Tal anel é chamado de anel de quocientes de Martindale simétrico.

Demonstração: Vejamos inicialmente que, se um anel satisfizer (2), então, qualquer um entre (3), (3′), (3″) é equivalente aos outros. É claro que (3) implica em (3′) e (3″). Por outro lado, e sejam $q \in Q$, $A \lhd R$ não nulo tal que $Aq = 0$. Por (2), existe $B \lhd R$ ideal não nulo tal que $qB \subseteq R$. Assim, $0 = (Aq)B = A(qB)$. Como R é primo, segue que $qB = 0$. Logo, se vale (3′), então $q = 0$. Assim, (3′) implica em (3) e em (3″). De modo análogo, (3″) implica em (3) e em (3′).

Sejam Q, Q' dois anéis satisfazendo essas 4 propriedades, e seja $q \in Q$. Assim, tome $A, B \lhd R$ ideais não nulos tais que $Aq, qB \subseteq R$. Sendo assim, tome $f : {}_RA \to {}_RR$ e $g : B_R \to R_R$ definidas por $f(a) = aq$ e $g(b) = qb$. Perceba que, para todos $a \in A, b \in B$, temos $f(a)b = (aq)b = a(qb) = ag(b)$.

Assim, existe $q' \in Q'$ tal que, para todos $a \in A$, $b \in B$, vale $aq = f(a) = aq'$ e $bq = g(b) = bq'$. Assim como no resultado anterior, o q' é único. Construa, portanto, uma função $\sigma : Q \to Q'$ por $\sigma(q) = q'$, e da mesma forma como foi mostrado no resultado anterior σ é um isomorfismo de anéis e de R-bimódulos. □

Vamos agora construir um anel que satisfaça essas propriedades. Isso pode ser feito encontrando um subanel de Q_l que satisfaça essa propriedade. Também pode ser feito encontrando um subanel de Q_r que também satisfaça essa propriedade (Q_r é o anel de Martindale à direita).

Proposição 1.3.6. *Seja R um anel primo. Então, existe um anel de quocientes de Martindale simétrico $Q = Q(R)$ de R. Mais especificamente, os seguintes anéis são anéis de quocientes de Martindale simétrico de R*

(i) $Q(R) = \{q \in Q_l(R) : \exists B \lhd R, B \neq 0, qB \subseteq R\}$.

(ii) $Q(R) = \{q \in Q_r(R) : \exists A \lhd R, A \neq 0, Aq \subseteq R\}$.

Demonstração: Vejamos que se $S = \{q \in Q_l(R) : \exists B \lhd R, B \neq 0, qB \subseteq R\}$, então S é um anel de quocientes de Martindale simétrico de R. É fácil perceber que S é um subanel de $Q_l(R)$, e, portanto, um anel.

1 Se $r \in R$, então $r \in Q_l(R)$ e $rR \subseteq R$, ou seja R é um subanel de S. Além disso, como a unidade de $Q_l(R)$ é a mesma de R, segue que a unidade de S também será, de modo que vale.

2 Por hipótese, também é válido.

3’ Por hipótese é válido, pois S é um subanel de $Q_l(R)$.

4 Sejam $A, B \lhd R$ ideais não nulos e $f : {}_RA \to {}_RR$, $g : B_R \to R_R$ morfismos de R-módulos à esquerda e à direita respectivamente balanceados. Por hipótese, existe $q \in Q_l(R)$ tal que $aq = f(a)$, para todo $a \in A$. Assim, dados $a \in A, b \in B$, temos $a(qb) = (aq)b = f(a)b = ag(b)$. Logo $A(qb - g(b)) = 0$. Como $qb - g(b) \in Q_l(R)$, segue que $g(b) = qb$. Para terminar, perceba que $q \in S$, pois $qb = g(b) \in R$, isto é $qB \subseteq R$.

De modo análogo, mostra-se que $\{q \in Q_r(R) : \exists A \lhd R, A \neq 0, Aq \subseteq R\}$ é um anel de quocientes de Martindale simétrico de R. □

Podemos então mostrar a seguinte propriedade.

Proposição 1.3.7. *Se R for um anel primo sem divisores de zero, então $Q(R)$ também não possui divisores de zero.*

Demonstração: Sejam $q_1, q_2 \in Q(R)$ tais que $q_1 q_2 = 0$. Sejam A_1, A_2 ideais de R tais que $A_1 q_1, q_2 A_2 \subseteq R$. Assim $(A_1 q_1)(q_2 A_2) = 0$. Como R não possui divisor de zero, e o produto de ideais (à esquerda, à direita, bilateral, podendo ser cada fator de tipos diferentes) é nulo, então um dos fatores é nulo, isto é, $A_1 q_1 = 0$ ou $q_2 A_2 = 0$, e, portanto $q_1 = 0$ ou $q_2 = 0$. □

Definição 1.3.8. Se R é um anel primo, dizemos que R é um *anel simetricamente fechado*, se $Q(R) = R$.

Mostraremos agora que uma álgebra livre é sempre simetricamente fechada. Vamos então precisar de alguns lemas e definições.

Definição 1.3.9. Dado X um conjunto não vazio, seja $S = \langle X \rangle$, o monoide (livre) gerado por X. Dado $a = \sum_{s \in S} \alpha_s s \in \Bbbk[S]$, definimos o *suporte* de a como sendo $\operatorname{supp}(a) = \{s \in S : \alpha_s \neq 0\}$. Sendo assim, iremos ver a álgebra $\Bbbk\langle X \rangle = \Bbbk[S]$, como uma álgebra de monóides. Dizemos que $A \subseteq S^{\times} = S \setminus \{1\}$ é *separado*, se, para todos $a, b \in S$ e $w \in S \setminus \{1\}$ tal que w é um segmento inicial de a e um segmento final de b, tem-se $a = w = b$. O *ideal de aumento* J é formado pelos elementos de $x \in \Bbbk[S]$ tal que $1 \notin \operatorname{supp}(x)$. Dado $a \in S$, denotamos por $|a|$ o comprimento de a.

Lema 1.3.10. *Seja $A \subseteq S^{\times}$ um conjunto separado e sejam $a, b \in A$ e $s, t \in S$.*

(i) Se $as = bt$, então $a = b$ e $s = t$.

(ii) Se $sa = tb$, então $a = b$ e $s = t$.

(iii) Se $as = tb$ e $s \neq 1$ ou $t \neq 1$, entao existe $r \in S$ tal que $s = rb$ e $t = ar$.

Demonstração: (i) Suponha sem perda de generalidade que $|a| \leq |b|$. Assim, como $as = bt$, devemos ter que a é um segmento inicial de b. Logo, como $a = w \neq 1$ é um segmento final a, e segue que $a = w = b$.

(ii) Análogo ao anterior

(iii) Se $|t| \geq |a|$, então existe $r \in S$ tal que $t = ar$. Assim,

$$as = tb = arb \Rightarrow s = rb.$$

Suponha agora que $|t| < |a|$. Assim, existe $w \in S$ tal que $tw = a$, com $w \neq 1$. Portanto

$$tb = as = tws \Rightarrow b = ws.$$

Assim, $w \neq 1$ é um segmento inicial de b e final de a, logo $a = w = b$. Dessa forma, devemos ter $s = t = 1$.

□

Lema 1.3.11. *Sejam $S = \langle X \rangle$, com $|X| > 1$ e A um subconjunto finito de S. Então, existem $s, t \in S$ tal que sAt é um conjunto separado.*

Demonstração: Sejam $x, y \in X, x \neq y$ e seja $n = \max\{|a| + 2 : a \in A\}$. Vejamos que $x^n y A x y^n$ é um conjunto separado.

Sejam $a, b \in A$ tais que $w \neq 1$ é um segmento inicial de $x^n y a x y^n$ e um segmento final de $x^n y b x y^n$. Se $|w| \leq n$, então w será simultâneamente uma potência de x e de y, absurdo. Logo $|w| > n \geq |a| + 2$. Mas w termina em y^n e é um segmento inicial de $x^n y a x y^n$, no qual a única ocorrência de y^n é no final. Logo $w = x^n y a x y^n$. De modo análogo $w = x^n y b x y^n$. □

Lema 1.3.12. *Seja $0 \neq \alpha \in \Bbbk[S]$ um elemento com suporte separado. Sejam $\beta, \gamma \in \Bbbk[S]$ tais que $\alpha\beta = \gamma\alpha$. Então existem $\tau \in \Bbbk[S], \lambda \in \Bbbk$, tais que $\gamma = \alpha\tau + \lambda, \beta = \tau\alpha + \lambda$. Além disso, se $\beta \in J$ ou $\gamma \in J$, então $\lambda = 0$.*

Demonstração: Seja $A = \operatorname{supp}(\alpha)$. Suponha que $1 \notin \operatorname{supp}(\beta)$. Se $\beta = 0$, então $\gamma = 0$, e podemos tomar $k = 0 = \tau$.

Caso contrário, $\operatorname{supp}(\beta) \neq \emptyset$ e sejam $a \in A, s \in \operatorname{supp}(\beta)$. Assim, por 1.3.10, as é a única forma de escrevê-lo em $(\operatorname{supp}(\alpha))(\operatorname{supp}(\beta))$, e, portanto, $as \in \operatorname{supp}(\alpha\beta) = \operatorname{supp}(\gamma\alpha) \subseteq \operatorname{supp}(\gamma)\operatorname{supp}(\alpha)$. Assim, existem $t \in \operatorname{supp}(\gamma), b \in \operatorname{supp}(\alpha) = A$, tais que $as = tb$. Como $1 \notin \operatorname{supp}(\beta)$ e $s \in \operatorname{supp}(\beta)$, segue que $s \neq 1$. Assim, por 1.3.10, existe $r \in S$ tal que $s = rb$. Dessa forma, todo elemento de $\operatorname{supp}(\beta)$ possui como segmento final, um elemento de A.

Agrupando os elementos com mesmo segmento final, para cada $a \in A$, existe $\tau'_a \in \Bbbk[S]$, tal que $\beta = \sum_{a \in A} \tau'_a a$. Além disso, podemos escrever $\alpha = \sum_{a \in A} k_a a$. Perceba que como $A = \operatorname{supp}(\alpha)$ e $\alpha \neq 0$, então $k_a \neq 0$, para todo $a \in A$. Assim, para cada $a \in A$, seja $\tau_a = k_a^{-1}\tau'_a$, de modo que $\tau'_a = k_a\tau_a$, e, portanto $\beta = \sum_{a \in A} k_a\tau_a a$. Como $\alpha\beta = \gamma\alpha$, temos

$$\sum_{a \in A} k_a \alpha \tau_a a = \alpha\beta = \gamma\alpha = \sum_{a \in A} k_a \gamma a.$$

Como A é um conjunto separado, de 1.3.10, segue que dois elementos de S que tenham mesmo segmento final devem ser os mesmos. Assim, para todo $a \in A, \alpha\tau_a a = \gamma a$. Dessa forma, $\alpha\tau_a = \gamma$. Como $\Bbbk[S]$ não possui divisores de zero, $\tau_a = \tau_b$, para todos $a, b \in A$. Assim, sendo $\tau = \tau_b$, temos $\alpha\tau = \gamma$. Assim,

$$\beta = \sum_{a \in A} k_a\tau_a a = \sum_{a \in A} k_a \tau a = \tau \sum_{a \in A} k_a a = \tau\alpha.$$

Além disso, $\gamma\alpha = \alpha\beta = \alpha\tau\alpha$, de modo que $\gamma = \alpha\tau$.

Suponha agora que $1 \in \operatorname{supp}(\beta)$, e escreva $\beta = \lambda + \beta'$, com $1 \notin \operatorname{supp}(\beta')$ e $\lambda \in \Bbbk$. Nesse caso, seja $\gamma' = \gamma - \lambda$. Assim

$$\alpha\beta' = \alpha(\beta - \lambda) = \alpha\beta - \lambda\alpha = \gamma\alpha - \lambda\alpha = (\gamma - \lambda)\alpha = \gamma'\alpha.$$

Portanto, existe $\tau \in \Bbbk[S]$ tal que $\beta' = \tau\alpha$ e $\gamma' = \alpha\tau$. Dessa maneira, $\beta = \beta' + \lambda = \tau\alpha + \lambda$ e $\gamma = \gamma' + \lambda = \alpha\tau + \lambda$.

Por fim, se $\beta \in J$, como $\alpha \in J$, J é um ideal e $\beta = \tau\alpha + \lambda$, segue que $\lambda \in J$, ou seja $\lambda = 0$. De modo análogo, se $\gamma \in J$. □

Podemos agora chegar ao nosso resultado.

Teorema 1.3.13. *Sejam $\Bbbk$ um corpo, X um conjunto com $|X| > 1$ e $R = \Bbbk\langle X\rangle$. Então R é uma álgebra prima simetricamente fechada.*

Demonstração: Como R não possui divisores de zero, segue que R é uma álgebra prima. Seja $q \in Q = Q(R)$ e $I \lhd R$ tal que $qI, Iq \subseteq R$ (podemos pegar a interseção caso os ideais que satisfaçam essa inclusão sejam distintos). Assim, JIJ é um ideal não nulo de R e $(JIJ)q = J(IJ)q \subseteq JIq \subseteq JR \subseteq J$. De modo análogo, devemos ter $q(JIJ) \subseteq J$. Dessa forma, trocando se necessário I por JIJ, podemos supor que $qI, Iq \subseteq J$.

Seja $\alpha \in I \setminus 0$ e seja $A = \operatorname{supp}(\alpha)$. Como A é finito, pelo Lema 1.3.11, existem $s, t \in S$ tais que $sAt = \operatorname{supp}(s\alpha t)$ é separado. Como $s\alpha t \in I$, poderiamos ter suposto que o suporte de $\alpha \in I \setminus 0$ era separado. Logo, sendo $\beta = q\alpha \in J$ e $\gamma = \alpha q \in J$, temos $\alpha\beta = \alpha q\alpha = \gamma\alpha$. Assim, pelo Lema 1.3.12, $\beta = \tau\alpha$, para algum $\tau \in R$. Como $\tau\alpha = \beta = q\alpha$ e R não possui divisores de zero, pela Proposição 1.3.7, segue que $q = \tau \in R$. Assim, R é simetricamente fechado. □

1.4 Lema de Higman

Nesta seção será demonstrado o Lema de Higman. O resultado principal desta seção utilizado nesta dissertação é o corolário no final da seção, que nos diz que em uma sequência (infinita) $(e_n)_{n\in\mathbb{N}}$ de palavras em um alfabeto finito, existem i, j índices tais que $i < j$ e e_i é uma subpalavra de e_j. A principal referência para este resultado é (Nash-Williams, 1967).

Definição 1.4.1. Seja X um conjunto com uma ordem parcial $\leq$. Se $(x_n)_{n\in\mathbb{N}}$ é uma sequência em X, dizemos que essa sequência é *boa* se existem $i, j \in \mathbb{N}$ com $i < j$ e $x_i \leq x_j$. Caso a sequência não seja boa, dizemos que a sequência é *ruim*. Dizemos que $(X, \leq)$ é *quase bem ordenado* se toda sequência (infinita) em X for boa.

Observação 1.4.2. Se $x, y \in X$ não é necessariamente verdade que $x \leq y$ ou $y \leq x$.

Se $(X, \leq_X)$ e $(Y, \leq_Y)$ são conjuntos parcialmente ordenados, podemos colocar uma parcial em $X \times Y$, da seguinte forma: dados $x_1, x_2 \in X$ e $y_1, y_2 \in Y$, $(x_1, y_1) \leq_{X\times Y} (x_2, y_2)$ se e somente se $x_1 \leq_X x_2$ e $y_1 \leq_Y y_2$. Pode-se perguntar em quais casos $X \times Y$ é quase bem ordenado, para isso, precisamos do seguinte resultado.

Proposição 1.4.3. *Se $(X, \leq)$ é um conjunto parcialmente-ordenado, então X é quase bem ordenado se, e somente se, toda sequência (infinita) em X possui subsequência (infinita) crescente.*

Demonstração: Suponha que X é quase bem ordenado e seja $(x_n)_{n\in\mathbb{N}}$ uma sequência. Dizemos que $m \in \mathbb{N}$ é terminal se não existe $n > m$ tal que $x_m \leq x_n$. Caso exista um número infinito de naturais terminais, a subsequência de $(x_n)_{n\in\mathbb{N}}$ cujos índices são os tais naturais seria ruim. Mas X é quase bem ordenado, contradição.

Dessa forma, seja $N \in \mathbb{N}$ um índice grande o suficiente de modo que para todo $m \in \mathbb{N}$, $m \geq N$, m não é terminal. Considere a função definida indutivamente $f(1) = N$ e $f(s+1)$ é um inteiro tal que $f(s+1) > f(s) \geq N$ e $x_{f(s)} \leq x_{f(s+1)}$ (tal $f(s+1)$ existe pois $f(s)$ não é terminal). Dessa forma a subsequência $(x_{f(n)})_{n\in\mathbb{N}}$ é crescente.

Por outro lado, se toda sequência infinita em X possui subsequência decrescente, e $(x_n)_{n\in\mathbb{N}}$ é uma sequência infinita, com $(x_{f(n)})_{n\in\mathbb{N}}$ subsequência decrescente, então $f(1) < f(2)$ e $x_{f(1)} \leq x_{f(2)}$, logo a sequência $(x_n)_{n\in\mathbb{N}}$ é boa. Portanto X é quase bem ordenado. □

Assim, temos

Proposição 1.4.4. *Sejam $(X, \leq_X)$ e $(Y, \leq_Y)$ conjuntos não vazios parcialmente ordenados. Então $X \times Y$ é quase bem ordenado (com a ordem parcial mostrada acima) se, e somente se, X e Y são.*

Demonstração: Suponha que X e Y são quase bem ordenados e seja $(x_n, y_n)_{n\in\mathbb{N}}$ uma sequência em $X \times Y$. Vejamos que essa sequência é boa. Como X é quase bem ordenado, $(x_n)_{n\in\mathbb{N}}$ possui uma subsequência (infinita) crescente $(x_{n_k})_{k\in\mathbb{N}}$. Assim, temos que a sequência $(y_{n_k})_{k\in\mathbb{N}}$ é uma sequência (infinita) em Y. Como Y é quase bem ordenado, existe uma subsequência (infinita) crescente $(y_{n_{k_j}})_{j\in\mathbb{N}}$. Dessa forma, a sequência $(x_{n_{k_j}})_{j\in\mathbb{N}}$ é uma subsequência de uma sequência crescente, portanto crescente. Assim, $(x_{n_{k_j}}, y_{n_{k_j}})_{j\in\mathbb{N}}$ é uma sequência crescente em $X \times Y$.

Por outro lado, suponha que $X \times Y$ é quase bem ordenado. Como $Y \neq \emptyset$, tome $y \in Y$. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência em X. Então, $(x_n, y)_{n\in\mathbb{N}}$ é uma sequência em $X \times Y$, e, portanto, possui uma subsequência crescente. Essa subsequência vai designar a uma subsequência crescente em X, de modo que X é quase bem ordenado. Pode-se mostrar que Y é quase bem ordenado de maneira análoga. □

Se X é um conjunto (não vazio), uma palavra em X é uma sequência finita de elementos de X. O conjunto de palavras, denotado por $\langle X \rangle$ e os elementos serão representados por justaposição, como por exemplo $x_1 \cdots x_n$. Se além disso, X for parcialmente ordenado, $\langle X \rangle$ também possui uma ordem parcial, dada por

$$x_1 \cdots x_m \leq_{\langle X \rangle} x'_1 \cdots x'_n,$$

se existe $f : \{1, \ldots, m\} \to \{1, \ldots, n\}$ função (estritamente) crescente tal que $x_i \leq_X x'_{f(i)}$, para todo $i \in \{1, \ldots, m\}$.

Novamente, X ser quase bem ordenado, traz consequências para $\langle X \rangle$.

Lema 1.4.5 (Lema de Higman)**.** *Se X é quase bem ordenado, então $\langle X \rangle$ também é.*

Demonstração: Suponha que existam sequências ruins em $\langle X \rangle$. Construa indutivamente uma sequência ruim, da seguinte maneira, seja u_1 a palavra com menor comprimento que está em uma sequência ruim. Dentre todas as sequências ruins que começam com u_1, seja u_2 uma palavra que está em uma dessas sequências de menor tamanho. Faça isso indutivamente, e teremos uma sequência ruim $(u_n)_{n\in\mathbb{N}}$. Como a sequência $(u_n)_{n\in\mathbb{N}}$ é ruim, sabemos que as palavras dessa sequência são todas não vazias.

Para cada n, seja A_n a última letra de u_n e seja v_n a palavra tal que $u_n = v_n A_n$. Seja $V = \{v_n : n \in \mathbb{N}\}$.

Suponha que V não é quase bem ordenado. Toda sequência em V é da forma $v_{g(1)}, v_{g(2)}, \ldots$ para alguma função $g : \mathbb{N} \to \mathbb{N}$. Como V não é quase bem ordenado, existe alguma $g : \mathbb{N} \to \mathbb{N}$ tal que $v_{g(1)}, v_{g(2)}, \ldots$ é uma sequência ruim. Sejam $l = \min\{g(n) : n \in \mathbb{N}\}$, e $s \in \mathbb{N}$ tal que $g(s) = l$. Dessa forma, se $f : \mathbb{N} \to \mathbb{N}$ é a função dada por $f(n) = g(n + s)$, então $(v_{f(n)})_{n\in\mathbb{N}}$ é uma sequência ruim (por ser subsequência de sequência ruim) e $f(1) \leq f(n)$, para todo n.

Assim, a sequência $u_1, u_2, \ldots, u_{f(1)-1}, v_{f(1)}, v_{f(2)}, \ldots$ é ruim. De fato, basta verificar para u_i e v_j nessa sequência. Perceba que se $u_i \leq v_j$, onde $j = f(t)$, para algum t e $i < f(1)$, então $i < f(1) \leq f(t)$, e $u_i \leq v_j = v_{f(t)} \leq u_{f(t)}$, contradição, logo essa sequência é ruim. Mas o tamanho de $v_{f(1)}$ é um a menos do que $u_{f(1)}$ e isso contradiz o modo como $u_{f(1)}$ foi escolhido, portanto V é quase bem ordenado.

Seja $Q = \{A_n : n \in \mathbb{N}\}$. Como X é quase bem ordenado e Q é um subconjunto de X, segue que Q é quase bem ordenado. Dessa forma, pela Proposição 1.4.4, $V \times Q$ é quase bem ordenado, de modo que a sequência $(v_n, A_n)_{n\in\mathbb{N}}$ é tal que existem i, j naturais com $i < j$ e $(v_i, A_i) \leq (v_j, A_j)$. Isso quer dizer que $v_i \leq v_j$ e $A_i \leq A_j$. Pela definição de ordem em $\langle X \rangle$, é fácil ver que $u_i \leq u_j$, contradição. Logo $\langle X \rangle$ é quase bem ordenado. □

Assim, um caso particular do lema de Higman é o seguinte.

Corolário 1.4.6. *Seja X um conjunto finito de letras. Se $(e_n)_{n\in\mathbb{N}}$ é uma sequência de palavras em X. Então, existe um par de naturais i, j tais que $i < j$ e e_i é uma subsequência de e_j.*

Demonstração: Se X é um conjunto finito, então X com a ordem trivial (cada elemento só é comparável a si mesmo) é quase bem ordendado. Pelo lema de Higman, $\langle X \rangle$ é quase bem ordenado. Isso quer dizer que existe i, j naturais tais que $i < j$ e $e_i \leq e_j$. Mas como a ordem e X é trivial, temos que e_i é subsequência de e_j. □

Capítulo 2

Invariantes da álgebra livre

As álgebras tensoriais são isomorfas às álgebras livres, e, portanto, iremos utilizar um ou o outro dependendo do contexto. Dessa forma, se H é uma álgebra de Hopf e V é um H-módulo, veremos como a álgebra tensorial $T(V)$ possui uma estrutura natural de H-módulo álgebra, no qual, estudaremos os invariantes. Será visto que essa subálgebra quase nunca é finitamente gerada e sempre é livre. Este capítulo é o principal desta dissertação.

A partir de agora neste capítulo H será uma biálgebra sobre $\Bbbk$. Ao longo deste capítulo, também denotaremos $T(V)$ por R, onde usualmente V será um espaço vetorial de dimensão finita. Assim, R possui a $\mathbb{N}$- graduação natural. Se W é um subespaço homogêneo, ao omitirmos alguma das componentes homogêneas W_i, estamos dizendo que $W \cap R_i = 0$ (por exemplo se escrevermos $W = W_2 \oplus W_3 \oplus \dots$, isso quer dizer que $W_0 = W_1 = 0$).

2.1 A subálgebra de invariantes é livre

Para esta seção, iremos considerar que H é uma álgebra de Hopf e R é uma álgebra filtrada qualquer (não necessariamente a álgebra livre) com pseudo-valoração v. As principais referências para esta subseção são (Masuoka e Yanai, 2003) e (V. O. Ferreira *et al.*, 2004).

Definição 2.1.1. Relembre a definição de pseudo-valoração dada na página 27. Dizemos que a ação de H em R é *compatível* se

(i) $v(h \cdot a) \leq v(a)$, para todos $h \in H$ e $a \in R$.

(ii) Todo $a \in R$ possui decomposição $a = a^+ + a^-$, em que $v(a^+) = v(a) > v(a^-)$, e tal que para todo $h \in H$ com $h \cdot a^+ \neq \varepsilon(h)a^+$, temos $v(\varepsilon(h)a^+ - h \cdot a^+) = v(a^+)$.

Exemplo 2.1.2. *Seja V um H-módulo de dimensão finita, e considere $R = T(V)$ com a ação homogênea. Coloque em R a valoração do Exemplo 1.2.10, isto é, e dado $a \in R$, escreva $a = \sum_I a_I x^I$. Dessa forma, considere $a^+ = \sum_J a_J x^J$, em que $|J|$ é máximo (ou seja, a^+ é a soma dos monômios de grau máximo de a com seus respectivos coeficientes) e $a^- = a - a^+$. Com isso, podemos perceber que a ação de H é compatível em R.*

Teorema 2.1.3. *Seja R uma $\Bbbk$-álgebra (não necessariamente livre) com uma pseudo-valoração v de modo que $v(\Bbbk) = 0$. Seja H uma álgebra de Hopf que age em R de forma compatível com a pseudo-valoração. Seja C um coideal à direita de H. Se R possui o algoritmo fraco, então a subálgebra de invariantes $R^C = \{a \in R : h \cdot a = \varepsilon(h)a \ \forall h \in C\}$ também o possui.*

Demonstração: Seja $A = \{a_1, \dots, a_m\}$ um conjunto R^C-dependente à direita, ordenado de forma que $v(a_1) \leq v(a_2) \leq \cdots \leq v(a_m)$. Assim, A também é um conjunto R-dependente à direita.

Seja n o menor número tal que $\{a_1, \dots, a_n\}$ seja R-dependente à direita. Como R possui o algortimo fraco, algum a_i é R-dependente em $\{a_1, \dots, a_{i-1}\}$.

Então existem $b_1, \dots, b_i \in R$ tais que

$$v\left(a_i - \sum_{j<i} a_j b_j\right) < v(a_i)$$

e $\max_{j<i}\left\{v\left(a_j\right) + v\left(b_j\right)\right\} \leq v(a_i)$. Sejam $J = \left\{j : v\left(a_j\right) + v\left(b_j\right) < v(a_i)\right\}$ e $L = \{1, \dots, i-1\} \setminus J$. Defina

$$c_j = \begin{cases} 0, j \in J \\ b_j, j \in L. \end{cases}$$

Dessa forma, vale

$$\begin{aligned} v\left(a_i - \sum_{j<i} a_j c_j\right) &= v\left(a_i - \sum_{j<i} a_j b_j + \sum_{j\in J} a_j b_j\right) \\ &\leq \max\left\{v\left(a_i - \sum_{j<i} a_j b_j\right), v\left(\sum_{j\in J} a_j b_j\right)\right\} \\ &\leq \max\left\{v\left(a_i - \sum_{j<i} a_j b_j\right), \max_{j\in J}\left\{v\left(a_j b_j\right)\right\}\right\} \\ &\leq \max\left\{v\left(a_i - \sum_{j<i} a_j b_j\right), \max_{j\in J}\left\{v\left(a_j\right) + v\left(b_j\right)\right\}\right\} < v(a_i). \end{aligned}$$

Considerando, para cada j, a decomposição $c_j = c_j^+ + c_j^-$, temos $c_j^+ = c_j - c_j^-$, de modo que

$$\begin{aligned} v\left(a_i - \sum_{j<i} a_j c_j^+\right) = v\left(a_i - \sum_{j<i} a_j c_j + \sum_{j<i} a_j c_j^-\right) &\leq \max\left\{v\left(a_i - \sum_{j<i} a_j c_j\right), v\left(\sum_{j<i} a_j c_j^-\right)\right\} \\ &= \max\left\{v\left(a_i - \sum_{j<i} a_j c_j\right), \max_{j<i}\left\{v\left(a_j\right) + v\left(c_j^-\right)\right\}\right\} < v(a_i), \end{aligned}$$

pois $v\left(c_j^-\right) < v\left(c_j\right) \leq v\left(b_j\right)$, de modo que $v\left(a_j\right) + v\left(c_j^-\right) < v\left(a_j\right) + v\left(b_j\right) \leq v(a_i)$.

Dado $h \in C$, temos

$$\begin{aligned} h \cdot \left(a_i - \sum_j a_j c_j^+ \right) &= h \cdot a_i - \sum_j h \cdot \left(a_j c_j^+ \right) = h \cdot a_i - \sum_j \sum_{(h)} \left(h_{(1)} \cdot a_j \right) \left(h_{(2)} \cdot c_j^+ \right) \\ &= \varepsilon(h) a_i - \sum_j \sum_{(h)} \varepsilon\left(h_{(1)} \right) a_j \left(h_{(2)} \cdot c_j^+ \right) \\ &= \varepsilon(h) a_i - \sum_j a_j \left(\sum_{(h)} \varepsilon\left(h_{(1)} \right) h_{(2)} \cdot c_j^+ \right) = \varepsilon(h) a_i - \sum_j a_j \left(h \cdot c_j^+ \right). \end{aligned}$$

Assim, vale

$$\begin{aligned} v\left(\sum_j a_j \left(\varepsilon(h) c_j^+ - h \cdot c_j^+ \right) \right) &= v\left(\left(\varepsilon(h) a_i - \sum_j a_j \left(h \cdot c_j^+ \right) \right) - \varepsilon(h) \left(a_i - \sum_j a_j c_j^+ \right) \right) \\ &\leq \max \left\{ v\left(h \cdot \left(a_i - \sum_j a_j c_j^+ \right) \right), v\left(\varepsilon(h) \left(a_i - \sum_j a_j c_j^+ \right) \right) \right\} \\ &< v(a_i) = \max_{j<i} \left\{ v(a_j) + v(c_j) \right\} = \max_{j<i} \left\{ v(a_j) + v(c_j^+) \right\}. \end{aligned}$$

Vamos mostrar agora que $c_m^+ \in R^C$ para algum m. Se supusermos o contrário teríamos $\varepsilon(h) c_m^+ - h \cdot c_m^+ \neq 0$, para algum $h \in C$ e algum m, de modo que $v\left(\varepsilon(h) c_m^+ - h \cdot c_m^+ \right) = v\left(c_m^+ \right)$. Como para todo $j < i$ tal que $\varepsilon(h) c_j^+ - h \cdot c_j^+ \neq 0$, vale $v(\varepsilon(h) c_j^+ - h \cdot c_j^+) = v(a_i) = v(a_j) + v(c_j^+)$ e, caso contrário $v(\varepsilon(h) c_j^+ - h \cdot c_j^+) = -\infty$, temos

$$\begin{aligned} v\left(\sum_j a_j \left(\varepsilon(h) c_j^+ - h \cdot c_j^+ \right) \right) &< \max_{j<i} \left\{ v\left(a_j \right) + v\left(c_j^+ \right) \right\} \\ &= v(a_i) = \max_{j<i} \left\{ v\left(a_j \right) + v\left(\varepsilon(h) c_j^+ - h \cdot c_j^+ \right) \right\}. \end{aligned}$$

Isso criaria uma relação de R-dependência em $\{a_1, \ldots, a_{i-1}\}$, contradição com a escolha de n. Dessa forma, concluímos que R^C também possui o algoritmo fraco.

□

Com esse teorema, temos o seguinte corolário.

Corolário 2.1.4. *Seja H uma álgebra de Hopf que age na álgebra livre R, e seja C um coideal à direita. Então, R^C é uma álgebra livre. Em particular, R^H é uma álgebra livre.*

Demonstração: Utilize a valoração dada no Exemplo 2.1.2. Por 1.2.17, temos que a álgebra livre satisfaz o algoritmo fraco para qualquer valoração e que suas subálgebras que satisfazem o algoritmo fraco são livres. Dessa forma, R^C é livre. □

2.2 Teorema da correspondência

Nesta seção, iremos mostrar um resultado que será utilizado algumas vezes durante o texto. Na teoria de Galois, temos teoremas que fazem uma correspondências entre

subgrupos do grupo de Galois e subcorpos da estensão. O que vamos achar aqui é uma correspondência entre algumas subálgebras de invariantes (que são fixos por alguma coideal subálgebra) e os coideais subálgebras.

Antes de mostrarmos o teorema da correspondência, vamos precisar de algumas definições e conceitos.

Observação 2.2.1. Teremos algumas definições e notações que serão utilizadas abaixo

1. Seja U uma subálgebra de R, uma álgebra prima. Dizemos que U é *racionalmente completa*, se para dado I ideal de U e $r \in R$ são tais que $Ir \subseteq U$, então $r \in U$.
2. Por (S. Montgomery, 1993) Corolário 3.5(2), se R é uma H-módulo álgebra, então $Q(R)$ também será. Assim, podemos considerar o produto smash $Q\#H$.
3. Sejam V, W, subconjuntos de $Q\#H$ como no item anterior. Denotamos $V^W = \{v \in V \ : \ vw = wv, \forall w \in W\}$.
4. Nas condições dos itens anteriores, o *centroide estendido* de R, denotado por $K = Z(Q)$ é o centro de Q, dizemos que a ação de H em R é X-*exterior* se $(Q\#H)^R = K$, o centroide estendido de R.

Assim, temos o seguinte teorema.

Teorema. [(Masuoka e Yanai, 2003) (Teorema 3.5)] Sejam $\Bbbk$ um corpo e H uma álgebra de Hopf pontuada de dimensão finita sobre $\Bbbk$ agindo em uma $\Bbbk$-álgebra prima R tal que a ação seja X-exterior. Sejam Q o anel de quocientes de Martindale simétrico de R e $K = Z(Q)$, o seu centro. Considere S o conjunto de todos os H-comódulo subálgebras à direita Λ de $K\#H$ contendo K, e F as subálgebras racionalmente completas U de R que contenham R^H. Então a função

$$\begin{aligned} \Phi \ : \ F &\to S \\ U &\mapsto (K\#H)^U \end{aligned}$$

é bijetora, com inversa dada por

$$\begin{aligned} \Psi \ : \ S &\to F \\ \Lambda &\mapsto R^\Lambda. \end{aligned}$$

□

Para a demonstração deste resultado, estuda-se um pouco o comportamento da categoria dos módulos.

Queremos um resultado parecido para o caso em que $R = \Bbbk\langle X\rangle$, sendo assim, iremos precisar de alguns lemas. Aqui estamos usando v como no Exemplo 1.2.10.

Lema 2.2.2. *Sejam $f \in \Bbbk\langle X\rangle$ um elemento homogêneo de grau $n > 0$ $x \in X$. Se, existe $h \in \Bbbk X$, tal que $xf = fh$, então existe $f' \in \Bbbk\langle X\rangle$ de grau $n-1$ tal que $f = xf'$. Em particular,*

se $f \in \Bbbk\langle X\rangle$ (um elemento não necessariamente homogêneo) tal que $f_0 = 0$ e $x \in X$ são tais que $xf = fh$, então existe $f' \in \Bbbk\langle X\rangle$ com $v(f') = v(f) - 1$, tal que $f = xf'$.

Demonstração: Se $h = 0$, como $\Bbbk\langle X\rangle$ não possui divisores de zero, segue que $f = 0$, pois $xf = f0 = 0$. Suponha assim $h \neq 0$ e seja n o grau de f. Escreva $f = \sum_{I\in X^n} \alpha_I x_{i_1}\cdots x_{i_n}, h = \sum_{x_j\in X} \beta_j x_j$. Assim

$$\sum_{I\in X^n} \alpha_I x x_{i_1}\cdots x_{i_n} = xf = fh = \sum_{I\in X^n, x_j\in X} \alpha_I\beta_j x_{i_1}\cdots x_{i_n}x_j.$$

Seja $I \in X^n$ tal que $\alpha_I \neq 0$ e tome $x_j \in X$ tal que $\beta_j \neq 0$ (existe pois $h \neq 0$). Perceba que os monônios do primeiro lado da igualdade são todos distintos (assim como no segundo lado da igualdade). Assim, como $\alpha_I\beta_j \neq 0$, segue que $x_{i_1}\cdots x_{i_n}x_j$ está no suporte de $fh = xf$. Mas todo monômio que está no suporte de xf começa com x, ou seja $x_{i_1} = x$. Dessa forma, se $f' = \sum_{I\in X^n} \alpha_I x_{i_2}\cdots x_{i_n}$, então $f = xf'$. É claro que o grau de f' é $n-1$.

Se f é como na segunda parte do enunciado, escreva $f = f_1 + f_2 + \cdots + f_n$, onde f_i é homogêneo de grau i, para todo $i \leq n$. Assim, como $xf = fh$, temos que $xf_1 + xf_2 + \cdots + xf_n = f_1h + f_2h + \cdots + f_nh$. Como xf_i e f_ih são homogêneos de grau $i+1$, pela unicidade da decomposição segue que $xf_i = f_ih$, para todo i. Assim, para todo i, existe $f_i' \in \Bbbk\langle X\rangle$ tal que $f_i = xf_i'$. Se $f' = f_1' + f_2' + \cdots + f_n'$, então

$$xf' = x(f_1' + f_2' + \cdots + f_n') = xf_1' + xf_2' + \cdots + xf_n' = f_1 + f_2 + \cdots + f_n = f.$$

Como $f_n \neq 0$, segue que $f_n' \neq 0$. Assim, $v(f') = v(f) - 1$. □

Lema 2.2.3. *Sejam $f \in \Bbbk\langle X\rangle$ e $x \in X$. Se existir $h \in \Bbbk\langle X\rangle$ um elemento homogêneo de grau 1 tal que $xf = fh$. Então $f \in \Bbbk[x]$.*

Demonstração: Faremos por indução em $v(f)$. Se $v(f) = 0$, então $f \in \Bbbk \subseteq \Bbbk[x]$. Suponha que o resultado seja válido para $v(f) = n$, e, provaremos para $v(f) = n+1$. Escreva $f = \lambda + f'$, com $f_0' = 0$. Assim,

$$xf - fh = x(\lambda + f') - (\lambda + f')h = \lambda(x - h) + xf' - f'h.$$

Assim, como toda componente homogênea de $xf' - f'h$ tem grau pelo menos 2 (pois $f_0' = 0$) e $\lambda(x-h)$ é homogêneo de grau 1, segue que $xf' - f'h = 0$. Pelo Lema 2.2.2, existe $f'' \in \Bbbk\langle X\rangle$, com $v(f'') = v(f') - 1 = v(f) - 1$ tal que $f'' = xf$. Temos

$$xxf'' = xf' = f'h = xf''h \Rightarrow xf'' = f'h.$$

Pela hipótese de indução, $f'' \in \Bbbk[x]$, e, portanto $f = \lambda + xf'' \in \Bbbk[x]$. □

Lema 2.2.4. *Seja $f \in \Bbbk\langle X\rangle$. Se para todo $x \in X$, existe um elemento homogêneo $h_x \in \Bbbk\langle X\rangle$ de grau 1 tal que $v(xf - fh_x) \leq 1$, então $f \in \Bbbk$.*

Demonstração: Escreva $f = \lambda + f'$, com $f'_0 = 0$. Para todo $x \in X$

$$xf - fh_x = \lambda(x - h_x) + xf' - f'h_x.$$

Portanto, toda componente homogênea não nula de $xf' - f'h_x$ deverá ter grau pelo menos 2, como $v(xf - fh_x) \leq 1$ e $\lambda(x - h_x)$ é homogêneo de grau 1, segue que $xf' - f'h_x = 0$. Portanto, $f' \in \Bbbk[x]$. Assim $f \in \bigcap_{x\in X} \Bbbk[x] = \Bbbk$. □

Lema 2.2.5. *Sejam $\Bbbk$ um corpo e H uma álgebra de Hopf de dimensão finita. Então toda ação homogênea de H em $\Bbbk\langle X\rangle$ é X-exterior, isto é, $(\Bbbk\langle X\rangle \# H)^{\Bbbk\langle X\rangle} = \Bbbk$.*

Demonstração: Primeiramente, repare que pelo Teorema 1.3.13 $Q = \Bbbk\langle X\rangle$ e que $Z(Q) = \Bbbk$. Seja $\{H_n\}$ a filtração co-radical de H. Pelo teorema de Taft-Wilson ((V. O. Ferreira *et al.*, 2004)), para cada $m \in \mathbb{N}$, existe um subespaço W_m de H que possui uma base Y_m tal que $H_m = H_{m-1} \oplus W_m$ e para todo $h \in W_m$, existe $\tau_h \in Y_0 = G(H)$

$$\Delta(h) = \tau_h \otimes h + w,$$

onde $w \in H \otimes H_{m-1}$. Assim, dado $\xi \in \Bbbk\langle X\rangle \# H_n$, podemos escrever

$$\xi = \sum_{i=0}^{n} \sum_{h\in Y_i} f_h h,$$

onde $f_h \in \Bbbk\langle X\rangle$. Assim, perceba que, dado $x \in X$, temos

$$hx = (\tau_h \cdot x)h + (w_1 \cdot x)w_2$$

onde w_1 é a primeira perna de w e w_2 a segunda (aqui não estamos assumindo que w é um tensor elementar). Dessa forma, vamos ter que

$$x\xi - \xi x = \sum_{h\in Y_n} (xf_h - f_h(\tau_h \cdot x))h + y,$$

para algum $y \in \Bbbk\langle X\rangle \# H_{n-1}$.

Como podemos decompor $H = W_0 \oplus W_1 \oplus \dots$, também podemos decompor $\Bbbk\langle X\rangle \# H = \bigoplus_{n\in\mathbb{N}} \Bbbk\langle X\rangle \# W_n$. Dessa forma, a componente de $x\xi - \xi x$ no subespaço $\Bbbk\langle X\rangle \# W_n$ seja

$$\sum_{h\in Y_n} (xf_h - f_h(\tau_h \cdot x))h.$$

Suponha agora que $\xi \in (\Bbbk\langle X\rangle \# H)^{\Bbbk\langle X\rangle}$. Logo ξ comuta com todos os elementos de X. Assim, como $x\xi - \xi x = 0$, todas as suas componentes são nulas, em particular $\sum_{h\in Y_n} (xf_h - f_h(\tau_h \cdot x))h = 0$. Como Y_n é linearmente independente, pela Proposição 1.1.43, segue que, para todo $h \in H$, $xf_h - f_h(\tau_h \cdot x) = 0$. Como a ação é homogênea, temos que $\tau_h \cdot x$ é homogêneo de grau 1. Assim, pelo Lema 2.2.4, como $v(0) < 1$, temos que $f_h \in \Bbbk$.

Vejamos por indução, que se $0 \leq m < n$ e $h \in Y_m$, então $f_h \in \Bbbk$. Escreva $\xi = \xi' + \xi''$, com

$$\xi' = \sum_{j=0}^{m} \sum_{h \in Y_j} f_h h$$

e

$$\xi'' = \sum_{i=m+1}^{n} \sum_{h \in Y_i} f_h h.$$

Pela hipótese de indução, $\xi'' \in \Bbbk \# H = H$. Além disso, como a ação de H em $\Bbbk\langle X \rangle$ é homogênea, segue que $x\xi'', \xi'' x \in \Bbbk X \# H$, logo, $x\xi'' - \xi'' x \in \Bbbk X \# H$. Assim,

$$0 = x\xi - \xi x = x\xi' + x\xi'' - \xi' x - \xi'' x \Rightarrow x\xi' - \xi' x = \xi'' x - x\xi'' \in \Bbbk X \# H.$$

Perceba que $\xi' \in \Bbbk\langle X \rangle \# H_m$. Dessa forma, analogamente ao que foi feito anterior, temos que a componente de $x\xi' - \xi' x$ em $\Bbbk\langle X \rangle \# W_m$ será

$$\sum_{h \in Y_m} (x f_h - f_h(\tau_h \cdot x)) h \in \Bbbk X \# H.$$

Assim, para todo $h \in Y_m$, devemos ter que $v(x f_h - f_h(\tau_h \cdot x)) \leq 1$. Pelo Lema 2.2.4, segue que $f_h \in \Bbbk$. Logo $\xi \in H$.

Como H possui dimensão finita, existe $\Lambda \in H$ um integral à esquerda não nulo. Seja $h \in (\Bbbk\langle X \rangle \# H)^{\Bbbk\langle X \rangle}$. Então, para todo $f \in \Bbbk\langle X \rangle$

$$\varepsilon(h) f \Lambda = fh\Lambda = hf\Lambda = \sum_{(h)} (h_{(1)} \cdot f) h_{(2)} \Lambda = (h \cdot f)\Lambda.$$

Novamente usando a Proposição 1.1.43, temos que $\varepsilon(h) f = h \cdot f$. Como a ação é fiel, segue que $h = \varepsilon(h) 1 \in \Bbbk$. □

O teorema que iremos esboçar a demonstração se utiliza de resultados mais avançados.

Teorema 2.2.6. *Seja X um conjunto com $|X| > 1$, e seja $R = \Bbbk\langle X \rangle$. Seja H uma álgebra de Hopf pontuada de dimensão finita que age homogeneamente e fielmente em R. Seja S o conjunto de todos os coideais subálgebras Λ de H e F o conjunto de todos as subálgebras livres de R contendo R^H. Então, F e S estão em bijeção, dada por*

$$\begin{aligned} \Phi : F &\to S \\ U &\mapsto \{h \in H : hf = fh \text{ em } R \# H, \forall f \in U\} \end{aligned}$$

com inversa dada por

$$\begin{aligned} \Psi : S &\to F \\ \Lambda &\mapsto R^{\Lambda} \end{aligned}$$

que invertem inclusões.

Esboço da demonstração: Pelo Lema 2.2.5, sabemos que a ação de H em R é X-exterior. Assim, pelo Teorema 2.2, existem funções entre F as subálgebras racionalmente livres e S o conjunto dos H-comódulo subálgebras que são justamente os coideais à direita subálgebras de $\Bbbk\langle X\rangle\#H$ contendo $\Bbbk\langle X\rangle$ e F o conjunto das subálgebras de R racionalmente completas contendo R^H e F' o conjunto das subálgebras livres de R contendo R^H. Para concluir, precisamos mostrar que $F = F'$. Pelo Lema 2.2.5 e pelo Corolário 2.1.4, podemos concluir que $F \subseteq F'$. Para a outra inclusão, perceba que todas as subálgebras livres de R são simetricamente fechadas, de modo que $Q(A) = A$, para todo $A \in F'$. Portanto, $A = Q(A) \cap R$, e pelo comentário na página 313 de (S. Montgomery e Passman, 1984), segue a outra inclusão. É claro que essas funções invertem inclusões. □

Corolário 2.2.7. *Suponha que $H = \Bbbk G$ é uma álgebra de grupo de dimensão finita. Então, existe uma correspondência entre os subgrupos de G e as subálgebras livres de R contendo R^H.*

Demonstração: Basta ver que todo coideal à direita subálgebra é da forma $\Bbbk N$ com N subgrupo de G. É claro que para todo $N \leq G$, $\Bbbk N$ é um coideal à direita subálgebra. Por outro lado, seja L um coideal à direita subálgebra. Considere $\{f_g : g \in G\}$ a base dual de G em $\Bbbk G$. Dado $l = \sum_{g\in G} \alpha_g g$, temos

$$\alpha_g g = (\mathrm{id} \otimes f_g)(\Delta(l)) \in (\mathrm{id} \otimes f_g)(L \otimes H) \subseteq L.$$

Logo, se g está no suporte de algum $l \in L$, então $g \in L$. Dessa forma, temos que $L = \Bbbk N$, onde $N = G \cap L$. Por fim, vejamos que N é um subgrupo de G. Como G e L são fechados pelo produto, N também é. Assim, N é um subconjunto não vazio de um grupo finito fechado pelo produto. Logo N é um subgrupo de G. □

Observação 2.2.8. Os resultados mostrados nesta seção são uma generalização dos resultados provados em (Harčenko, 1978).

2.3 Quando a subálgebra de invariantes é finitamente gerada

2.3.1 Caracterização através do suporte da subálgebra de invariantes

Na primeira subseção deste capítulo, vimos que a subálgebra de invariantes é sempre livre. No entanto, ocorre que essa álgebra quase nunca é finitamente gerada, como veremos nesta seção. A principal referência para esta seção é (Koryukin, 1994).

Definição 2.3.1. Seja A um anel com unidade. Dizemos que A é *Dedekind finito*, se para todos $x, y \in A$, tivermos que $xy = 1 \Rightarrow yx = 1$. Em outras palavras, todo elemento que possui inverso de algum lado é inversível.

Com essa definição, temos alguns exemplos de anéis Dedekind finitos

Exemplo 2.3.2. *Seja A um anel com unidade. Então se A for comutativo ou um anel com divisão então A é Dedekind finito.*

Além disso, temos o seguinte fato sobre anéis Dedekind finitos.

Lema 2.3.3. *Seja A um anel Dedekind finito e seja F um subanel de $Z(A)$ (que contenha a unidade). Sejam X e Y F-submódulos de A tais que $XY = \{xy : x \in X, y \in Y\} = F$.*

Então, existe $x \in X$ e $y \in Y$ inversíveis tais que $X = Fx$, $Y = Fy$ com $x = y^{-1}$. Em particular, se F for um anel com divisão, então X e Y são unidimensionais sobre F.

Demonstração: Como $XY = \{xy : x \in X, y \in Y\} = F$, existem $x \in X$ e $y \in Y$ tais que $xy = 1$. Como A é Dedekind finito, segue que $y = x^{-1}$

Assim, temos

$$Y = yxY \subseteq yXY = yF \subseteq Y,$$

dessa forma, temos que $yF = Y$ (como F está contido no centro, não importa o lado em que o colocamos). De modo análogo, podemos mostrar que $Fx = X$. □

Temos também as seguintes definições e notações.

Definição 2.3.4. Denotamos por $G(H^*) \subseteq U(H^*)$, os elementos inversíveis da álgebra H^* (cuja unidade é ε) que são morfismo de álgebras.

Sejam M um H-módulo à esquerda, $m \in M$ e $\alpha \in H^*$ um morfismo de álgebras. Dizemos que m é um *H-semi-invariante de peso α* se, para todo $h \in \ker(\alpha)$, tivermos $h \cdot m = 0$. O conjunto dos H-semi-invariantes de peso α é denotado por $I_\alpha(M)$. Os invariantes são um caso particular em que $\alpha = \varepsilon$.

Proposição 2.3.5. *Sejam M um H-módulo à esquerda e $\alpha \in G(H^*)$. Então, temos que*

$$I_\alpha(M) = \{m \in M : h \cdot m = \alpha(h)m \ \forall h \in H\}.$$

Além disso, dado $\alpha \in H^*$ e $m \in M$ não nulo de modo que para todos $h \in H$ temos $h \cdot m = \alpha(h)m$, então α é um morfismo de álgebras e $m \in I_\alpha(M)$. Em particular, se M é um H-módulo unidimensional sobre $\Bbbk$, então existe $\alpha \in G(H^*)$ tal que $M = I_\alpha(M)$.

Demonstração: Seja $m \in I_\alpha(M)$. Assim, dado $h \in H$, temos que

$$\alpha(h - \alpha(h)1) = \alpha(h) - \alpha(h) = 0$$

ou seja $h - \alpha(h)1 \in \ker(\alpha)$. Dessa forma, temos

$$0 = (h - \alpha(h)1) \cdot m = h \cdot m - \alpha(h)m \Rightarrow h \cdot m = \alpha(h)m.$$

Por outro lado, se $h \cdot m = \alpha(h)m$, para todo $h \in H$, então, dado $h \in \ker(\alpha)$, temos

$$h \cdot m = \alpha(h)m = 0m = 0,$$

o que conclui a igualdade.

Agora, dado $m \in M$ e $\alpha \in H^*$ como na segunda parte do enunciado, temos

$$m = 1 \cdot m = \alpha(1)m \Rightarrow (1 - \alpha(1))m = 0 \Rightarrow \alpha(1) = 1$$

$$\alpha(h_1h_2)m = (h_1h_2) \cdot m = h_1 \cdot (h_2 \cdot m) = h_1 \cdot \alpha(h_2)m = \alpha(h_2)h_1 \cdot m = \alpha(h_1)\alpha(h_2)m$$
$$\Rightarrow \alpha(h_1h_2) = \alpha(h_1)\alpha(h_2).$$

Concluímos assim que α é um morfismo de álgebras. Pela caracterização anterior, é claro que $m \in I_\alpha(M)$. □

Sejam M, N H-módulos à esquerda. Lembre que temos uma estrutura de H-módulo em $M \otimes N$, colocando, para todos $m \in M$ e $n \in N$

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

Lema 2.3.6. *Sejam M_1, M_2 dois H-módulos à esquerda e $x_i \in M_i$ $(i = 1, 2)$, elementos não nulos. Se $\alpha_i \in H^*$ é um morfismo de álgebra tal que $x_i \in I_{\alpha_i}(M_i)$ $(i = 1, 2)$, então $x_1 \otimes x_2 \in I_{\alpha_1 * \alpha_2}(M_1 \otimes M_2)$. Além disso, se $x_1 \otimes x_2 \in (M_1 \otimes M_2)^H$, então x_1 e x_2 são H-semi-invariantes de pesos mutualmente inversos.*

Demonstração: Para a primeira parte, dado $h \in H$

$$\begin{aligned} h \cdot (x_1 \otimes x_2) &= \sum_{(h)} h_{(1)} \cdot x_1 \otimes h_{(2)} \cdot x_2 = \sum_{(h)} \alpha_1(h_{(1)})x_1 \otimes \alpha_2(h_{(2)})x_2 \\ &= \sum_{(h)} \alpha_1(h_{(1)})\alpha_2(h_{(2)})x_1 \otimes x_2 = (\alpha_1 * \alpha_2)(h)x_1 \otimes x_2, \end{aligned}$$

dessa forma $x_1 \otimes x_2 \in I_{\alpha_1 * \alpha_2}(M_1 \otimes M_2)$.

Para a segunda parte, dado $i = 1, 2$, denotamos por N_i o H-submódulo de M_i gerado por x_i, e $f_i : N_i^* \to H^*$, dada por

$$f_i(n_i^*)(h) = n_i^*(h \cdot x_i) \tag{2.1}$$

para todos $n_i^* \in N_i^*$ e $h \in H$. Assim f_i é injetor, pois, se $n_i^* \in \ker(f_i)$, então, para todo $h \in H$, temos que $n_i^*(h \cdot x_i) = 0$, mas N_i é H-submódulo de M_i gerado por x_i, de modo que n_i^* é a transformação nula.

Dado $h \in H$, do fato de $x_1 \otimes x_2$ ser um H-invariante, temos que

$$\sum_{(h)} h_{(1)} \cdot x_1 \otimes h_{(2)} \cdot x_2 = h \cdot (x_1 \otimes x_2) = \varepsilon(h)x_1 \otimes x_2.$$

Dados $n_i^* \in N_i^*$ $(i = 1, 2)$, aplicando $n_1^* \otimes n_2^*$ nos dois lados da equação, temos

$$\sum_{(h)} n_1^*(h_{(1)} \cdot x_1) \otimes n_2^*(h_{(2)} \cdot x_2) = \varepsilon(h)n_1^*(x_1) \otimes n_2^*(x_2),$$

pela Equação (2.1), obtemos

$$\sum_{(h)} f_1(n_1^*)(h_{(1)}) \otimes f_2(n_2^*)(h_{(2)}) = \varepsilon(h) n_1^*(x_1) \otimes n_2^*(x_2).$$

Aplicando a multiplicação em ambos os lados, temos

$$(f_1(n_1^*) * f_2(n_2^*))(h) = \sum_{(h)} f_1(n_1^*)(h_{(1)}) f_2(n_2^*)(h_{(2)}) = \varepsilon(h) n_1^*(x_1) n_2^*(x_2),$$

de modo que $f_1(n_1^*) * f_2(n_2^*) = n_1^*(x_1)n_2^*(x_2)\varepsilon$, ou seja, $f_1(N_1^*) * f_2(N_2^*) = N_1^*(x_1)N_2^*(x_2)\varepsilon$. Como $x_i \neq 0$, segue que $N_1^*(x_1)N_2^*(x_2) = \Bbbk$. Concluímos portanto que

$$f_1(N_1^*) * f_2(N_2^*) = \varepsilon\Bbbk \tag{2.2}$$

Como ε é a unidade de H^*, segue que $\varepsilon\Bbbk \subseteq Z(H^*)$ e é um subanel (isomorfo à $\Bbbk$). Assim, pelo Lema 2.3.3, podemos concluir que $f_i(N_i^*)$ possui dimensão 1 sobre $\varepsilon\Bbbk(\cong \Bbbk)$ $(i = 1, 2)$. Como f_i é injetora, segue que N_i^* é unidimensional sobre $\Bbbk$ $(i = 1, 2)$, de modo que N_i também seja unidimensional sobre $\Bbbk$ $(i = 1, 2)$.

Assim, temos que para todo $h \in H$, $h \cdot x_i$ é um múltiplo escalar de x_i com escalar em $\Bbbk$. Dessa maneira, seja $\alpha_i \in H^*$ tal que $h \cdot x_i = \alpha_i(h)x_i$. Pela Proposição 2.3.5, segue que α_i é um morfismo de álgebras e $x_i \in I_{\alpha_i}(M_i)$. Pela primeira parte desse lema, temos que $\alpha_1 * \alpha_2 = \varepsilon$. Como H^* é um anel Dedekind finito, segue que α_1 e α_2 são mutualmente inversos. □

Também temos um resultado parecido em que não temos a necessidade de que o anel seja Dedekind finito, mas contém o caso em que os elementos não sejam apenas tensores elementares pelo seguinte lema.

Lema 2.3.7. *Sejam M e N H-módulos e $\alpha \in G(H^*)$ e $\beta = \alpha^{-1}$. Então $(I_\alpha(M) \otimes N)^H = I_\alpha(M) \otimes I_\beta(N)$.*

Demonstração: Seja $T : H^* \to \mathrm{End}(H)$, dada por $T(\gamma)(h) = \sum_{(h)} \gamma(h_{(1)})h_{(2)}$, para todo $\gamma \in H^*$ e $h \in H$. É fácil ver que essa aplicação é linear, e, além disso, é um antimorfismo de álgebras pois

$$T(\varepsilon)(h) = \sum_{(h)} \varepsilon(h_{(1)})h_{(2)} = h \Rightarrow T(\varepsilon) = id_H;$$

$$\begin{aligned} T(\gamma_1 * \gamma_2)(h) &= \sum_{(h)} (\gamma_1 * \gamma_2)(h_{(1)})h_{(2)} = \sum_{(h)} \gamma_1(h_{(1)})\gamma_2(h_{(2)})h_{(3)} \\ &= \sum_{(h)} \gamma_2(\gamma_1(h_{(1)})h_{(2)})h_{(3)} = T(\gamma_2)(T(\gamma_1)(h)) = T(\gamma_2) \circ T(\gamma_1)(h). \end{aligned}$$

A penúltima igualdade vem da definição de T e da seguinte

$$\Delta(T(\gamma_1(h)) = \Delta\left(\sum_{(h)} \gamma_1(h_{(1)})h_{(2)}\right) = \sum_{(h)} \gamma_1(h_{(1)})\Delta(h_{(2)}) = \sum_{(h)} \gamma_1(h_{(1)})h_{(2)} \otimes h_{(3)}.$$

Além disso, para todo $\gamma \in H^*$, temos $\varepsilon \circ T(\gamma) = \gamma$, pois, dado $h \in H$, vale

$$\varepsilon \circ T(\gamma)(h) = \sum_{(h)} \varepsilon(\gamma(h_{(1)})h_{(2)}) = \gamma\left(\sum_{(h)} \varepsilon(h_{(2)})h_{(1)}\right) = \gamma(h).$$

Assim, se $v \in I_\alpha(M) \otimes I_\beta(N)$, então $v \in I_\alpha(M) \otimes N$ e é semi-invariante de peso $\alpha\beta = \varepsilon$, ou seja, $v \in (I_\alpha(M) \otimes N)^H$.

Por outro lado, se $v \in (I_\alpha(M) \otimes N)^H$ é não nulo, escreva

$$v = \sum_{i=1}^{n} a_i \otimes b_i,$$

onde os a_i's são linearmente independente em $I_\alpha(M)$.

Dessa forma, dado $h \in H$, temos

$$\begin{aligned}\sum_{i=1}^{n} a_i \otimes \varepsilon(h)b_i = \varepsilon(h)v = h \cdot v = h \cdot \left(\sum_{i=1}^{n} a_i \otimes b_i\right) &= \sum_{i=1}^{n}\sum_{(h)} (h_{(1)} \cdot a_i) \otimes (h_{(2)} \cdot b_i) \\ &= \sum_{i=1}^{n}\sum_{(h)} (\alpha(h_{(1)})a_i) \otimes (h_{(2)} \cdot b_i) = \sum_{i=1}^{n} a_i \otimes \left(\sum_{(h)} (\alpha(h_{(1)})h_{(2)} \cdot b_i)\right).\end{aligned}$$

de modo que, para todo $h \in H$, e todo $i = 1, \dots, n$,

$$\varepsilon(h)b_i = \sum_{(h)} (\alpha(h_{(1)})h_{(2)} \cdot b_i) = \left(\sum_{(h)} \alpha(h_{(1)})h_{(2)}\right) \cdot b_i = T(\alpha)(h) \cdot b_i.$$

Como α é inversível e T é um antimorfismo, para todo $h \in H$ e $i = 1, \dots, n$, temos

$$h \cdot b_i = (T(\alpha)(T(\alpha^{-1})(h))) \cdot b_i = \varepsilon(T(\alpha^{-1})(h))b_i = \alpha^{-1}(h)b_i = \beta(h)b_i.$$

Isso mostra que, para cada $i = 1, \dots, n$, $b_i \in I_\beta(N)$, de modo que $v \in I_\alpha(M) \otimes I_\beta(N)$.

□

Definição 2.3.8. Considere a álgebra tensorial $R = T(V)$, com a $\mathbb{N}$-graduação natural, onde V é um H-módulo (de modo que R possui uma estrutura de H-módulo álgebra). Um subespaço homogêneo $A = A_0 \oplus A_1 \oplus \dots$ é dito ser uma *álgebra com inserção*, se para todos m, n, p não negativos

$$\tau_{mnp}(A_{m+n} \otimes A_p) \subseteq A_{m+n+p},$$

onde $\tau_{mnp}(x \otimes y \otimes z) = x \otimes z \otimes y$, para todos $x \in R_m$, $y \in R_n$ e $z \in R_p$.

Observação 2.3.9. Se A é uma álgebra com inserção, então A é uma subálgebra de R.

Isso vem do fato de que $A_m \otimes A_p = \tau_{m0p}(A_m \otimes A_p) \subseteq A_{m+p}$.

Queremos mostrar que R^H é uma álgebra com inserção. Vamos precisar do próxima lema para isso.

Lema 2.3.10. *Sejam m, n, p inteiros não negativos e $a \in R_{m+n}$, $z \in R_p^H$ e $h \in H$. Então vale a igualdade*

$$h \cdot \tau_{mnp}(a \otimes z) = \tau_{mnp}(h \cdot a \otimes z).$$

Demonstração: Como τ_{mnp} é linear, basta mostrarmos esta igualdade para $a = x \otimes y$, com $x \in R_m$ e $y \in R_n$. Temos

$$\begin{aligned} h \cdot \tau_{mnp}(a \otimes z) = h \cdot (x \otimes z \otimes y) &= \sum_{(h)} h_{(1)} \cdot x \otimes h_{(2)} \cdot z \otimes h_{(3)} \cdot y \\ &= \sum_{(h)} h_{(1)} \cdot x \otimes \varepsilon(h_{(2)}) z \otimes h_{(3)} \cdot y = \sum_{(h)} h_{(1)} \cdot x \otimes z \otimes h_{(2)} \cdot y \\ &= \tau_{mnp}(h \cdot a \otimes z). \end{aligned}$$

□

Com a igualdade anterior, podemos provar que R^H é uma álgebra com inserção.

Lema 2.3.11. *O subespaço R^H é uma álgebra com inserção.*

Demonstração: Primeiramente, é fácil ver que R^H é um subespaço homogêneo (dado que a ação é linear). Além disso, vejamos que dados inteiros não negativos m, n, p, temos que $\tau_{mnp}(R_{m+n}^H \otimes R_p^H) \subseteq R_{m+n+p}^H$.

Sejam então $a \in R_{m+n}^H$, $z \in R_p^H$ e $h \in H$. Temos então pelo lema anterior

$$h \cdot \tau_{mnp}(a \otimes z) = \tau_{mnp}(h \cdot a \otimes z) = \tau_{mnp}(\varepsilon(h)a \otimes z) = \varepsilon(h)\tau_{mnp}(a \otimes z),$$

ou seja, $\tau_{mnp}(a \otimes z) \in R_{m+n+p}^H$, portanto, segue que R^H é uma álgebra com inserção. □

O seguinte subespaço será importante para construções futuras.

Definição 2.3.12. Sejam M e N $\Bbbk$-espaços e $K \subseteq M \otimes N$ um subespaço. Dizemos que um subespaço $l(K)$ de M é o *espaço-posto à esquerda* se $l(K)$ é o menor subespaço de M tal que $K \subseteq l(K) \otimes N$. Analogamente, definimos o *espaço-posto à direita* $r(K)$ de K como sendo o menor subespaço de N tal que $K \subseteq M \otimes r(K)$.

Proposição 2.3.13. *Se M e N são $\Bbbk$-espaços e $K \subseteq M \otimes N$ é um subespaço, então*

$$l(K) = \operatorname{span}\{(\mathrm{id}_M \otimes \varphi)(K) : \varphi \in N^*\} \quad e\ r(K) = \operatorname{span}\{(\varphi \otimes \mathrm{id}_N)(K) : \varphi \in M^*\},$$

onde estamos identificando $M = M \otimes \Bbbk$.

Demonstração: Seja $l_1 = \operatorname{span}\{(\mathrm{id}_M \otimes \varphi)(K) : \varphi \in N^*\}$. Vejamos que $K \subseteq l_1 \otimes N$ e que se l_2 é um subespaço de M tal que $K \subseteq l_2 \otimes N$, então $l_1 \subseteq l_2$.

Sejam $\{n_i : i \in I\}$ uma base de N, $\{f_i : i \in I\}$ seu conjunto dual e $x \in K$. Escreva $x = \sum_{i \in I} m_i \otimes n_i$. Assim, $m_i = (\mathrm{id}_M \otimes f_i)(x) \in l_1$. Logo $K \subseteq l_1 \otimes N$.

Por outro lado, sejam l_2 um subespaço de M tal que $K \subseteq l_2 \otimes N$, $x \in K$ e $\varphi \in N^*$. Assim $(\mathrm{id}_M \otimes \varphi)(x) \in l_2$. Como l_2 é um subespaço, segue que $l_1 \subseteq l_2$. □

Com essa definição, iremos considerar alguns subespaços da álgebra tensorial. Dado $n \in \mathbb{N}$, temos a projeção canôninca $P_n : R \to R_n$ e a inclusão $i_n : R_n \to R$. Assim, temos o operador $F_n : R \to R$, dado por $F_n = \mathrm{id}_R - i_0 \circ P_0 - \cdots - i_{n-1} \circ P_{n-1}$. O que esse operador com um elemento w de R é eliminar os termos de grau menor que n de w. Sendo assim, a imagem de F_n está contida em $R_n \otimes R$. Dessa maneira, dado K um subespaço de R, definimos $l_n(K)$ como sendo o espaço-posto de $F_n(K) \subseteq R_n \otimes R$.

Seja W um subespaço de R. Denotamos por $L(W)$ o subespaço homogêneo $L(W) = l_0(W) \oplus l_1(W) \oplus \cdots$.

Queremos mostrar que se A é uma álgebra com inserção, então, $L(A)$ é uma subálgebra. Isso será importante, pois R^H é uma álgebra com inserção, e iremos olhar para $L(R^H)$. Isso será feito em alguns lemas.

Lema 2.3.14. *Sejam $n, m, i, j \in \mathbb{N}$ e S e T subespaços de R_{n+i} e R_{m+j} respectivamente. Então $l_{n+m}(\tau_{n,i,m+j}(S \otimes T)) = l_n(S) \otimes l_m(T)$ em R_{n+m}.*

Demonstração: Sejam $l_1 = l_n(S)$, $l_2 = l_m(T)$ e $X = \tau_{n,i,m+j}(S \otimes T)$. Assim, como $S \subseteq l_1 \otimes R_i$ e $T \subseteq l_2 \otimes R_j$, temos que

$$S \otimes T \subseteq l_1 \otimes R_i \otimes l_2 \otimes R_j \Rightarrow$$

$$X = \tau_{n,i,m+j}(S \otimes T) \subseteq \tau_{n,i,m+j}(l_1 \otimes R_i \otimes l_2 \otimes R_j) = l_1 \otimes l_2 \otimes R_j \otimes R_i = l_1 \otimes l_2 \otimes R_{m+n}.$$

Dessa forma, temos que $l_{n+m}(X) \subseteq l_1 \otimes l_2$.

Por outro lado, sejam $\phi \in R_i^*, \psi \in R_j^*$. Considere $\alpha = (\mathrm{id}_{R_{n+m}} \otimes \psi \otimes \phi) \circ \tau_{n,i,m+j}$ e $\beta = \mathrm{id}_{R_n} \otimes \phi \otimes \mathrm{id}_{R_m} \otimes \psi$, aplicações lineares de domínio $R_{n+m+i+j}$ e contradomínio R_{n+m} (aqui estamos fazendo utilizando isomorfismos $\Bbbk \otimes V \cong V$, para todo V espaço vetorial).

Dados $x_n \in R_n, x_m \in R_m, x_i \in R_i$ e $x_j \in R_j$, então

$$\begin{aligned}\alpha(x_n \otimes x_i \otimes x_m \otimes x_j) &= (\mathrm{id}_{R_{n+m}} \otimes \psi \otimes \phi) \circ \tau_{n,i,m+j}(x_n \otimes x_i \otimes x_m \otimes x_j) \\ &= (\mathrm{id}_{R_{n+m}} \otimes \psi \otimes \phi)(x_n \otimes x_m \otimes x_j \otimes x_i) = x_n \otimes x_m \otimes \psi(x_j) \otimes \phi(x_i) \\ &= x_n\phi(x_i) \otimes x_m\psi(x_j) = (\mathrm{id}_{R_n} \otimes \phi \otimes \mathrm{id}_{R_m} \otimes \psi)(x_n \otimes x_i \otimes x_m \otimes x_j),\end{aligned}$$

de modo que $\alpha = \beta$. Assim, como $\psi \otimes \phi \in R_{i+j}^*$, temos que

$$\begin{aligned}\beta(S \otimes T) = \alpha(S \otimes T) &= ((\mathrm{id}_{R_{n+m}} \otimes \psi \otimes \phi) \circ \tau_{n,i,m+j})(S \otimes T) \\ &= (\mathrm{id}_{R_{n+m}} \otimes \psi \otimes \phi)(X) \subseteq l_{n+m}(X).\end{aligned}$$

Pela definição de l_1 e l_2, temos que $l_1 \otimes l_2 \subseteq l_{n+m}(X)$, portanto, vale a igualdade.

□

Lema 2.3.15. *Seja $A = A_0 \oplus A_1 \oplus \cdots$ uma álgebra com inserção. Então, $L(A)$ é uma subálgebra de R.*

Demonstração: Sejam $n, m, i, j \in \mathbb{N}$. Como A é uma álgebra com inserção, então, temos que $\tau_{n,i,m+j}(A_{n+i} \otimes A_{m+j}) \subseteq A_{n+m+i+j}$, dessa forma

$$l_{n+m}(\tau_{n,i,m+j}(A_{n+i} \otimes A_{m+j})) \subseteq l_{n+m}(A_{n+m+i+j}) \subseteq l_{n+m}(A).$$

Pelo lema anterior, podemos concluir que

$$l_n(A_{n+i}) \otimes l_m(A_{m+j}) \subseteq l_{n+m}(A).$$

Somando, para todo i, j, concluimos que $l_n(A) \otimes l_m(A) \subseteq l_{n+m}(A)$, concluindo que $L(A)$ é uma subálgebra. □

Seja I um ideal à direita de R homogêneo. Como V possui dimensão finita e ideais homogêneos são gerados por seus elementos homogêneos, então I é finitamente gerado se e somente se existir n tal que I é gerado pelos seus elementos de grau $\leq n$. Vamos provar mais alguns lemas que vão nos ajudar a dizer em quais casos R^H é finitamente gerado (considerando o ideal à direita $I = l_1(R^H)$).

Lema 2.3.16. *Seja $m \in \mathbb{N}$ e $\rho = \rho_0 \oplus \rho_1 \oplus \cdots$ um ideal homogêneo de R gerado por elementos homogêneos de grau no máximo m. Dado $n \geq m$, temos que $l_n(\rho) = \rho_n$.*

Demonstração: Vejamos que $F_n(\rho) \subseteq \rho_n \otimes R$. Seja $r \in \rho$ um dos geradores de ρ (de grau $t \leq m$) e seja x um elemento homogêneo de grau $n - t$. Então $xr \in \rho$ (pois ρ é um ideal) é um elemento homogêneo de grau n, ou seja, $xr \in \rho_n$, pois ρ é um subespaço homogêneo. Assim, para todo y homogêneo, temos que $xry \in \rho_n \otimes R$. Como todo elemento de $F_n(\rho)$ é soma de elementos dessa forma (pois ρ é gerado por elementos de grau no máximo m), segue que $F_n(\rho) \subseteq \rho_n \otimes R$, e, portanto, segue que $l_n(\rho) \subseteq \rho_n$.

Por outro lado, perceba que $\rho_n \subseteq l_n(\rho_n) \otimes R$. Assim, temos que $\rho_n = P_n(\rho_n) \subseteq P_n(l_n(\rho_n) \otimes R) = l_n(\rho_n) \subseteq l_n(\rho)$, pois $\rho_n \subseteq \rho$. □

Lema 2.3.17. *Se $T(V)^H$ for gerada por elementos de grau no máximo n (onde n é um inteiro positivo fixado), então todos os elementos de $l_1(R^H)$ são H-semi-invariantes de mesmo peso $\alpha \in G(H^*)$, cuja ordem é finita e menor ou igual a n.*

Demonstração: Para cada $m \in \mathbb{N}$, seja $\rho_m = \rho_{m0} \oplus \rho_{m1} \oplus \ldots$, o ideal (homogêneo) à direita de R gerado por elementos de $F_1(R^H)$ de grau no máximo m. Por hipótese, temos que $F_1(R^H) \subseteq \rho_n$. Além disso, o ideal homogêneo ρ_n é gerado por elementos de grau no máximo n, de modo que pelo Lema 2.3.16, vale $l_n(\rho_n) = \rho_{nn}$.

Seja $l = l_1(R^H) = l_1(F_1(R^H))$. Pelos Lemas 2.3.11 e 2.3.15, segue que $L(F_1(R^H))$ é uma subálgebra de R. Em particular

$$l^{\otimes n} \subseteq l_n(F_1(R^H)) \subseteq l_n(\rho_n) = \rho_{nn}.$$

Seja m o menor inteiro positivo tal que $l^{\otimes m} \subseteq \rho_{mm}$. É claro que $m \leq n$. Se $m = 1$, então $l \subseteq \rho_{11}$. Assim, como $\rho_1 = V^H \otimes R$, temos que $\rho_{11} = P_1(\rho_1) = P_1(V^H \otimes R) = V^H$. Isso nos diz que $l \subseteq V^H$, de modo que podemos tomar $\alpha = \varepsilon$ para tornar o lema válido.

Suponha então que $m \geq 2$. Seja $U = l^{\otimes m-1}$. Então, temos que $U \otimes l \subseteq R^H$, pela escolha de m. Assim pelo Lema 2.3.6, temos que todos os elementos de U são semi-invariantes de peso β e todos os elementos de l são semi-invariantes de peso α. De fato, pois se $x_1, x_2 \in U$ e $y_1, y_2 \in l$, então $x_1 \otimes y_1 \in U \otimes l \subseteq R^H$, portanto x_1 e y_1 possuem pesos mutualmente inversos. Com uma demonstração análoga, x_1 e y_2 são semi-invariantes de pesos mutualmente

inversos. Mas como o peso é único, segue que o peso de x_1 e x_2 é o mesmo, e isso também ocorre com y_1 e y_2, e podemos chamar o peso de l de α e de U de $\beta = \alpha^{-1}$.

Mas, como $U = l^{\otimes m-1}$, os elementos de U são invariantes de peso α^{m-1}. Pela unicidade do peso, segue que $\alpha^{m-1} = \beta = \alpha^{-1}$. Dessa forma, os elementos de l são semi-invariantes de um elemento de ordem finita $\leq m \leq n$, pela escolha de m. □

Definição 2.3.18. Seja $n > 1$ um inteiro e $T_n : R_n \to R_n$ a aplicação linear tal que, para todos $x \in V$ e $y \in R_{n-1}$ vale $T_n(x \otimes y) = y \otimes x$. Uma subálgebra homogênea A é dita *cíclica* se $T_n(A_n) \subseteq A_n$, para todo n.

As álgebras cíclicas e os invariantes estão relacionados.

Proposição 2.3.19. *Seja $n \in \mathbb{N}$. Se R^H for gerada por elementos de grau no máximo n, então R^H é uma álgebra cíclica.*

Demonstração: Seja $m \geq 2$ um inteiro e l e r os espaços de dimensão à esquerda e à direita respectivamente de $R^H_m \subseteq V \otimes R_{m-1}$.

Como $l = l_1(R^H_m) \subseteq l_1(R^H)$, pelo Lema 2.3.17 todos os elementos de l são semi-invariantes de mesmo peso α. De acordo com o Lema 2.3.7, todos os elementos de r são α^{-1} semi-invariantes. Assim, pelo Lema 1.1.1, $R^H_m \subseteq l \otimes R_{m-1} \cap V \otimes r = l \otimes r$.

Dessa forma, temos que $r \otimes l \subseteq R^H_m$, pois os elementos desse conjunto têm grau m e são semi-invariantes de peso $\alpha^{-1} * \alpha = \varepsilon$. Assim, $T_m(R^H_m) \subseteq T_m(l \otimes r) = r \otimes l \subseteq R^H_m$. Logo R^H é cíclica. [1] □

Definição 2.3.20. Seja X um subconjunto de $T(V)$. O *suporte* de X, denotado por $s(X)$ é o menor subespaço de V tal que $X \subseteq T(s(X))$.

O suporte sempre existe.

Proposição 2.3.21. *Seja V um $\Bbbk$-espaço vetorial e $\{W_i : i \in I\}$ uma família não-vazia de subespaços de V. Então $\Bbbk\langle \bigcap_i W_i \rangle = \bigcap_i \Bbbk\langle W_i \rangle$. Em particular, dado $X \subseteq T(V)$, existe um menor subespaço W de V tal que $X \subseteq \Bbbk\langle W \rangle$.*

Demonstração: Vamos denotar por W a interseção de todos esses subespaços, isto é $W = \bigcap_i W_i$. Como, para todo $j \in I$, temos $W \subseteq W_j$, segue que $\Bbbk\langle W \rangle \subseteq \Bbbk\langle W_j \rangle$, ou seja, $\Bbbk\langle W \rangle \subseteq \bigcap_i \Bbbk\langle W_i \rangle$. Provaremos por indução em m, que $\bigcap_i \Bbbk\langle W_i \rangle_m \subseteq \Bbbk\langle W \rangle_m$.

Seja $x \in \bigcap_i \Bbbk\langle W_i \rangle_m$. Se $m = 0$, então $x \in \Bbbk = \Bbbk\langle W \rangle_0$. Se $m > 0$, como I é não-vazio, seja $j \in I$. Assim, $x \in \Bbbk\langle W_j \rangle$, de modo que podemos escrever $x = \sum_{l=1}^{s} u_l \otimes v_l$, onde $u_l \in W_j^{\otimes(m-1)}$, $v_l \in W_j$ com $\{u_1, \dots, u_s\}$ e $\{v_1, \dots, v_s\}$ linearmente independentes. Assim, para cada $p = 1, \dots, s$ podemos tomar $f_p \in (T(V)_{m-1})^*$, $g_p \in V^*$ tal que $f_p(u_l) = \delta_{p,l} = g_p(v_l)$. Logo, para todo $i \in I$, temos

$$u_p = (\mathrm{id} \otimes g_p)(x) \in \Bbbk\langle W_i \rangle_{m-1};$$

$$v_p = (f_p \otimes \mathrm{id})(x) \in W_i,$$

[1] Nesta demonstração foi demonstrado que $R^H_m \subseteq l \otimes r$. Mas no segundo parágrafo, por algum argumento similar, poderiamos ter mostrado que $l \otimes r \subseteq R^H_m$, o que mostraria a igualdade.

pois $x \in \Bbbk\langle W_i\rangle$. Assim, pela hipótese de indução $u_p \in \bigcap_i \Bbbk\langle W_i\rangle_{m-1} \subseteq \Bbbk\langle W\rangle_{m-1}$. E também $v_p \in \bigcap_i W_i = W$, de modo que, para todo p, $u_p \otimes v_p \in \Bbbk\langle W\rangle_m$, ou seja $x \in \Bbbk\langle W\rangle_m$, provando o passo indutivo. Como $\Bbbk\langle W\rangle$ e $\bigcap_i \Bbbk\langle W_i\rangle$ são subespaços homogêneos, segue a igualdade.

Se $X \subseteq T(V)$ é um subconjunto, considere $B = \{W \leq V \ : \ X \subseteq \Bbbk\langle W\rangle\}$. Assim, B é não-vazio, pois $V \in B$, de modo que, se $W = \bigcap_{W_i \in B} W_i$, então W é o subespaço pedido. □

Além disso, o suporte possui algumas propriedades como veremos a seguir.

Lema 2.3.22. *Sejam W um subespaço de $T(V)$ e $x \in V$. Se existe $m > 0$ tal que $x^m \in W$ (isto é, $x \otimes \cdots \otimes x \in W$), então $x \in s(W)$.*

Demonstração: Se $x = 0$, então $x \in s(W)$. Caso contrário, seja $f \in (T(V)_{m-1})^*$ tal que $f(x^{m-1}) = 1$. Logo, se $U = s(W)$, então $x = (f \otimes \mathrm{id}_V)(x^m) \in (f \otimes \mathrm{id}_V)(W) \subseteq (f \otimes \mathrm{id}_V)(\Bbbk\langle U\rangle_m) \subseteq U$. □

Lema 2.3.23. *Sejam V um $\Bbbk$-espaço, U um subespaço de V, de dimensão finita com base $\{u_1, \dots, u_n\}$ e W um subespaço de $T(V)$. Seja $I = \{i = (i_1, \dots, i_m) \ : \ i_l \in \{1, \dots, n\} \forall l \text{ e } i_l = i_s \Rightarrow l = s\}$. Suponha que exista $x \in W$ um elemento homogêneo não-nulo de grau n que possa ser escrito da seguinte forma*

$$x = \sum_{i \in I} \alpha_i u_{i_1} \otimes \cdots \otimes u_{i_n}.$$

Então, $U \subseteq s(W)$. Em particular, se V possui dimensão finita com base $\{v_1, \dots, v_n\}$ e $\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) v_{\sigma(1)} \otimes \cdots v_{\sigma(n)} \in W$, então $s(W) = V$.

Demonstração: Sejam $f_1, \dots, f_n \in V^*$ tais que $f_l(u_s) = \delta_{l,s}$ e $V' = s(W)$. Como $x \neq 0$, existe $j \in I$ tal que $\alpha_j \neq 0$. Para cada $l = 1, \dots, n$, considere $g_l = f_{j_1} \otimes \cdots \otimes f_{j_{l-1}} \otimes \mathrm{id} \otimes f_{j_{l+1}} \otimes \cdots \otimes f_{j_n}$. Assim, dado $i \in I$ e $\alpha \in \Bbbk$, temos

$$g_l(\alpha u_{i_1} \otimes \cdots \otimes u_{i_n}) = \alpha \delta_{i_1, j_1} \cdots \delta_{i_{l-1}, j_{l-1}} \delta_{i_{l+1}, j_{l+1}} \cdots \delta_{i_n, j_n} u_{i_l} = \alpha \delta_{i,j} u_{j_l},$$

pois, se $i \neq j$, então $i_s \neq j_s$, para algum $s \neq l$ (pelo fato de que i e j são "permutações"que coincidem em pelo menos todos os elementos menos em l, então vão coincidir em todos), e se $i = j$, a igualdade é clara. Assim,

$$\alpha_j u_{j_l} = g_l(x) \in g_l(W) \subseteq g_l(\Bbbk\langle V'\rangle_n) \subseteq V'.$$

Como $\alpha_j \neq 0$, segue que $u_{j_l} \in V'$. Como para todo $s \in \{1, \dots, n\}$, existe $l \in \{1, ..., n\}$ tal que $s = j_l$, segue que $U \subseteq V' = s(W)$. Para a segunda parte, se pegarmos $U = V$, e $x = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) v_{\sigma(1)} \otimes \cdots v_{\sigma(n)}$, concluiremos que $V \subseteq s(W)$. A outra inclusão é óbvia. □

Lema 2.3.24. *Se A é uma álgebra cíclica, então $s(A) = l_1(A)$.*

Demonstração: Vamos começar mostrando que $s(A) \subseteq l_1(A)$. Para isso, vamos mostrar que para todo n, $A_n \subseteq l_1(A)^{\otimes n}$, de modo que $A \subseteq \Bbbk\langle l_1(A)\rangle$.

Seja $n \in \mathbb{N}$ qualquer e $i \leq n$ variando. Por definição de $l_1(A)$, temos que $A_{n+1} \subseteq l_1(A) \otimes R_n$. Como A é cíclica, segue que $T_{n+1}^{i+1}(A_{n+1}) = A_{n+1}$. Dessa forma, $A_{n+1} \subseteq T_{n+1}^{i+1}(l_1(A) \otimes R_n) = R_{n-i} \otimes l_1(A) \otimes R_i$. Assim, $A_{n+1} \subseteq \bigcap_{i=0}^{n} R_{n-i} \otimes l_1(A) \otimes R_i = l_1(A)^{\otimes(n+1)}$.

Para a outra inclusão, basta ver que $A \subseteq \Bbbk\langle s(A)\rangle$, de modo que $F_1(A) \subseteq F_1(\Bbbk\langle s(A)\rangle) \subseteq s(A) \otimes R$, e, portanto, $l_1(A) \subseteq s(A)$.

□

Com essas definições temos o seguinte teorema que classifica quando a álgebra de invariantes é finitamente gerada.

Teorema 2.3.25. *Sejam H uma biálgebra e V um H-módulo e n um inteiro positivo. São equivalentes:*

1. *A álgebra $T(V)^H$ é gerado por elementos de grau no máximo n.*
2. *O suporte de $T(V)^H$ é um submódulo de V consistindo de todos os elementos semi-invariantes de mesmo peso de ordem finita, cuja ordem é menor ou igual a n.*

Demonstração: Suponha que R^H seja gerada por elementos de grau no máximo n. Então, pela Proposição 2.3.19, R^H é cíclica, e, pela Proposição 2.3.24, $l_1(R^H)$ é o suporte de R^H. Então, pelo Lema 2.3.17, todos os elementos do suporte de R^H são semi-invariantes de mesmo peso α, cuja ordem é menor ou igual a n. Por outro lado, se $x \in I_\alpha(V)$, como α possui ordem finita m, temos que $x \otimes \ldots \otimes x \in R^H$ (com m termos). Segue do Lema 2.3.22 que $x \in s(R^H)$.

Reciprocamente, suponha que o suporte W de R^H seja um submódulo de V consistindo de todos os elementos semi-invariantes de mesmo peso α cuja ordem é finita é m que é menor ou igual a n. Vejamos que $W^{\otimes m}$ gera R^H (e é constituído por elementos de grau no máximo m e portanto, por elementos de grau no máximo n). Temos assim que R^H está na subálgebra gerada por W (pela definição de suporte), mas como $W = I_\alpha(V)$, apenas e exatamente os elementos de grau múltipo de m nessa subálgebra são os invariantes. Dessa forma, vale que $W^{\otimes m}$ gera R^H. □

Um corolário que segue facilmente desse teorema é o seguinte.

Corolário 2.3.26. *Sejam H uma biálgebra e V um H-módulo de dimensão finita. Então são equivalentes:*

1. *A álgebra $T(V)^H$ é finitamente gerada.*
2. *O suporte de $T(V)^H$ é um submódulo de V consistindo de todos os elementos semi-invariantes de mesmo peso, de ordem finita.*

2.3.2 Séries de Poincaré

O principal resultado dessa subseção nos diz que a álgebra de invariantes é finitamente gerada se, e só se sua série de Poincaré for inversível e a inversa for um polinômio. As referências desta subseção são (Dicks e Formanek, 1982/83) e (Vitor O. Ferreira e L. S. I. Murakami, 2014).

Definição 2.3.27. Seja V um espaço vetorial, e W um subespaço homogêneo da álgebra $T(V)$. A *série de Poincaré* de W é definida como

$$P(W) = \sum_{n\geq 0} \dim(W \cap V_n)t^n \in \mathbb{Z}[[t]].$$

As seguintes propriedades são satisfeitas pelas séries de Poincaré.

(i) Sejam U e W subespaços homogêneos de $T(V)$. Se $U \cap W = 0$, então $U \oplus W$ é um subespaço homogêneo de $T(V)$ e $P(U \oplus W) = P(U) + P(W)$.

(ii) Sejam U e W subespaços homogêneos de $T(V)$. Então $U \otimes W$ é homogêneo e $P(U \otimes W) = P(U)P(W)$.

Demonstração: (i) Sejam U e W subespaços homogêneos de $T(V)$ com $U \cap W = 0$. Então

$$\begin{aligned} U \oplus W &= (\bigoplus_{n\in\mathbb{N}} U \cap V_n) \oplus (\bigoplus_{n\in\mathbb{N}} W \cap V_n) \\ &= \bigoplus_{n\in\mathbb{N}} ((U \cap V_n) \oplus (W \cap V_n)) \\ &= \bigoplus_{n\in\mathbb{N}} ((U \oplus W) \cap V_n). \end{aligned}$$

Isso prova que $U \oplus W$ é homogêneo e $P(U \oplus W) = P(U) + P(W)$ segue da última igualdade.

(ii) Sejam U e W subespaços homogêneos de $T(V)$. Assim, temos

$$\begin{aligned} U \otimes W &= (\oplus_{n\in\mathbb{N}} U \cap V_n) \otimes (\oplus_{m\in\mathbb{N}} W \cap V_m) \\ &= \bigoplus_{n,m\in\mathbb{N}} ((U \cap V_n) \otimes (W \cap V_m)) \\ &= \bigoplus_{l\in\mathbb{N}} \bigoplus_{n+m=l} ((U \cap V_n) \otimes (W \cap V_m)) \\ &= \bigoplus_{l\in\mathbb{N}} (U \otimes W) \cap V_l. \end{aligned}$$

De maneira análoga ao anterior, isso mostra que $U \otimes W$ é homogêneo e a última igualdade mostra que $P(U \otimes W) = P(U)P(W)$.

□

Com essas definições e propriedades, conseguimos chegar no seguinte resultado.

Lema 2.3.28. *Sejam H uma álgebra de Hopf e V um H-módulo. Considere $T(V)$ com a estrutura de H-módulo álgebra usual. Então, $T(V)^H$ é finitamente gerada se e somente se $P(T(V)^H)$ é inversível com inversa polinomial.*

Demonstração: Pelo Corolário 2.1.4, sabemos que $T(V)^H$ é livre. Tome U um subespaço de $T(V)$ tal que $T(V)^H = \Bbbk\langle U\rangle$.

Assim, vale que $\Bbbk\langle U\rangle = \Bbbk \oplus (U \otimes \Bbbk\langle U\rangle)$, e, portanto

$$P(\Bbbk\langle U\rangle) = 1 + P(U)P(\Bbbk\langle U\rangle).$$

Logo,

$$P(\Bbbk\langle U\rangle)(1 - P(U)) = 1 \Rightarrow P(\Bbbk\langle U\rangle)^{-1} = 1 - P(U)$$

Então $T(V)^H$ é finitamente gerada se e somente se U tem dimensão finita se e somente se $1 - P(U)$ tem grau finito (ou seja, é um polinômio) se e somente se $P(T(V)^H)$ for inversível com inversa polinomial. □

Agora iremos ver um exemplo da aplicação das séries de Poincaré para determinar se a subálgebra de invariantes é finitamente gerada. Seja G um grupo finito e seja $H = (\Bbbk G)^*$. Lembre que uma álgebra A é uma H-módulo álgebra se e somente se A é G-graduada com $A^H = A_e$, como visto no Exemplo 1.1.37. Suponha que H aja linearmente em $T(V)$, isto é, V é um H-módulo, cuja ação induz em $T(V)$ uma estrutura de módulo álgebra. Assim, temos uma decomposição de V em soma direta de subespaços

$$V = \bigoplus_{x\in G} V_x.$$

Dessa forma, temos a decomposição de $T(V) = \bigoplus_{x\in G} T(V)_x$, em que se $x \neq e$,

$$T(V)_x = \bigoplus_{y_1\dots y_n = x} V_{y_1} \otimes \cdots \otimes V_{y_n}$$

e

$$T(V)_e = \Bbbk \oplus \bigoplus_{y_1\dots y_n = e} V_{y_1} \otimes \cdots \otimes V_{y_n}.$$

Para cada $n \geq 1$, temos a seguinte igualdade

$$V^{\otimes n} = \bigoplus_{x\in G} \left(\bigoplus_{y_1\dots y_n = x} V_{y_1} \otimes \dots \otimes V_{y_n} \right),$$

onde para cada $x \in G$, temos $(V^{\otimes n})_x = \bigoplus_{y_1\dots y_n = x} V_{y_1} \otimes \dots \otimes V_{y_n}$. Assim, para n natural qualquer, denote por $a_n^{(x)} = \dim(V^{\otimes n})_x$ e $d_x = a_1^{(x)}$.

Antes de obter a série de Poincaré de $T(V)_e$, vamos precisar do seguinte lema.

Lema 2.3.29. *Os números $a_n^{(x)}$ definidos acima satisfazem à seguinte relação recursiva, para $n \geq 1$*

$$a_n^{(x)} = \sum_{y\in G} d_{xy^{-1}} a_{n-1}^{(y)}.$$

Demonstração: Dado $n \geq 1$ e $x \in G$, temos

$$(V^{\otimes n})_x = \bigoplus_{y\in G} V_{xy^{-1}} \otimes \left(\bigoplus_{z_1\dots z_{n-1} = y} V_{z_1} \otimes \dots \otimes V_{z_{n-1}} \right) = \bigoplus_{y\in G} V_{xy^{-1}} \otimes (V^{\otimes(n-1)})_y.$$

Assim, o resultado segue. □

Vamos precisar de um lema antes de achar a série de Poincaré deste caso

Lema 2.3.30. *Sejam $r(t) \in \mathbb{Z}[t]$ um polinômio e $d \in \mathbb{Z}$, $d \neq 0$, tais que $r\left(\frac{1}{d}\right) = 0$. Então, existe um polinômio $q(t) \in \mathbb{Z}[t]$ tal que r(t) = (1-dt)q(t).*

Demonstração: Podemos considerar $l(t) \in \mathbb{Q}[t]$ tal que $r(t) = (t - \frac{1}{d})l(t)$. Escreva $l(t) = a_m t^m + \cdots + a_1 t + a_0$. Então

$$a_m t^{m+1} + \left(a_{m-1} - \frac{a_m}{d}\right) t^m + \cdots + \left(a_{i-1} - \frac{a_i}{d}\right) t_i + \cdots + \left(a_0 - \frac{a_1}{d}\right) t - \frac{a_0}{d} = \left(t - \frac{1}{d}\right) l(t) = r(t) \in \mathbb{Z}[t].$$

Logo, $-\frac{a_0}{d} \in \mathbb{Z} \Rightarrow a_0 \in d\mathbb{Z}$. Indutivamente, se $i \geq 1$, então $-\frac{a_i}{d} = a_{i-1} - \frac{a_i}{d} \Rightarrow a_{i-1} \in \mathbb{Z}$, portanto $a_i \in d\mathbb{Z}$. Assim, $l(t) \in (d\mathbb{Z})[t]$. Assim, basta tomar $q(t) = -\frac{l(t)}{d}$. □

Teorema 2.3.31. *Seja G um grupo finito e V um espaço vetorial de dimensão finita G-graduado. Então $P(T(V)_e)$ é uma função racional da forma*

$$P(T(V)_e) = \frac{p(t)}{(1 - dt)q(t)},$$

em que $p(t)$ e $q(t)$ são polinômios com coeficientes inteiros ambos com grau menor ou igual a $|G| - 1$.

Demonstração: Para cada $x \in G$, seja $F_x(t) = \sum_{n \geq 0} a_n^{(x)} t^n = P(T(V)_x)$. Pelo Lema 2.3.29, temos que

$$\begin{aligned} F_x(t) &= \sum_{n \geq 0} a_n^{(x)} t^n = \sum_{n \geq 1} \left(\sum_{y \in G} d_{xy^{-1}} a_{n-1}^{(y)} \right) t^n = \sum_{y \in G} \left(\sum_{n \geq 1} d_{xy^{-1}} a_{n-1}^{(y)} t^n \right) \\ &= \sum_{y \in G} d_{xy^{-1}} t \sum_{n \geq 1} a_{n-1}^{(y)} t^{n-1} = \sum_{y \in G} d_{xy^{-1}} t F_y(t), \end{aligned}$$

se $x \neq e$, e

$$\begin{aligned} F_e(t) &= \sum_{n \geq 0} a_n^{(e)} t^n = 1 + \sum_{n \geq 1} \left(\sum_{y \in G} d_{y^{-1}} a_{n-1}^{(y)} \right) t^n = 1 + \sum_{y \in G} \left(\sum_{n \geq 1} d_{y^{-1}} a_{n-1}^{(y)} t^n \right) \\ &= 1 + \sum_{y \in G} d_{y^{-1}} t \sum_{n \geq 1} a_{n-1}^{(y)} t^{n-1} = 1 + \sum_{y \in G} d_{y^{-1}} t F_y(t). \end{aligned}$$

Assim, tirando as parcelas correspondentes, chegamos no seguinte sistema

$$\begin{cases} (d_e t - 1) F_e(t) + \sum_{y \neq e} d_{y^{-1}} F_y(t) = -1 \\ (d_e t - 1) F_x(t) + \sum_{y \neq x} d_{xy^{-1}} F_y(t) = 0 (x \neq e) \end{cases}, \tag{2.3}$$

em $\mathbb{Q}(t)$. Enumere os elementos de G, $G = \{x_1 = e, x_2, \dots, x_s\}$. Podemos então utilizar a regra de Kramer, para concluir que $F_e(t) = \frac{p(t)}{r(t)}$, onde $p(t)$ e $r(t)$ são os polinômios dados por

$$p(t) = \det \begin{pmatrix} -1 & d_{x_2}t & \dots & d_{x_s}t \\ 0 & d_e t - 1 & \dots & d_{x_s x_2^{-1}}t \\ \dots & & & \\ 0 & d_{x_2 x_s^{-1}}t & \dots & d_e t - 1 \end{pmatrix}$$

e

$$r(t) = \det \begin{pmatrix} d_e t - 1 & d_{x_2}t & d_{x_3}t & \dots & d_{x_s}t \\ d_{x_2^{-1}}t & d_e t - 1 & d_{x_3 x_2^{-1}}t & \dots & d_{x_s x_2^{-1}}t \\ d_{x_3^{-1}}t & d_{x_2 x_3^{-1}}t & d_e t - 1 & \dots & d_{x_s x_3^{-1}}t \\ \dots & & & & \\ d_{x_s^{-1}}t & d_{x_2 x_s^{-1}}t & d_{x_3 x_s^{-1}}t & \dots & d_e t - 1 \end{pmatrix}.$$

O sistema de fato possui solução, pois, o termo de grau 0 de $r(t)$ é $(-1)^s$ que é diferente de zero.

Por fim, vejamos que $\frac{1}{d}$ é raiz de $r(t)$. Temos

$$r\left(\frac{1}{d}\right) = \frac{1}{d^s} \det \begin{pmatrix} d_e - d & d_{x_2} & d_{x_3} & \dots & d_{x_s} \\ d_{x_2^{-1}} & d_e - d & d_{x_3 x_2^{-1}} & \dots & d_{x_s x_2^{-1}} \\ d_{x_3^{-1}} & d_{x_2 x_3^{-1}} & d_e - d & \dots & d_{x_s x_3^{-1}} \\ \dots & & & & \\ d_{x_s^{-1}} & d_{x_2 x_s^{-1}} & d_{x_3 x_s^{-1}} & \dots & d_e - d \end{pmatrix}.$$

Dessa forma, ao colocarmos o vetor $(1, \dots, 1)$ na transformação linear da matriz acima, obtemos o vetor nulo, ou seja, essa matriz não é inversível, e, portanto possui determinante nulo. Assim $r\left(\frac{1}{d}\right) = 0$. O resultado segue do Lema 2.3.30. □

Uma graduação é dita ser trivial se existe $x \in G$ tal que $V_x = V$. Sendo assim, graduações triviais geram invariantes finitamente gerados. Temos também uma certa recíproca.

Teorema 2.3.32. *Seja G um grupo finito ($H = (kG)^*$)e V um espaço vetorial com alguma G-graduação. Se essa graduação for trivial, $T(V)^H$ é finitamente gerado. Por outro lado, se V for um espaço G-graduado não trivialmente tal que $V_e \neq 0$, então $T(V)^H$ não é finitamente gerado.*

Demonstração: Suponha que V seja trivialmente graduado, e seja $x \in G$ tal que $V = V_x$. Como G é finito, x possui ordem finita r. Assim, vamos ter que $T(V)_e = \Bbbk \oplus V^{\otimes r} \oplus V^{\otimes 2r} \oplus \cdots$. Portanto, qualquer base do espaço de dimensão finita $V^{\otimes r}$ gera $T(V)_e$.

Por outro lado, suponha que existe $x \neq e$ tal que $V_x \neq 0 \neq V_e$. Vamos supor inicialmente que $V = V_x \oplus V_e$. Sabemos que $P(T(V)_e) = \frac{p(t)}{r(t)}$, como no teorema anterior. É fácil perceber que $\frac{1}{d_e}$ é raiz de $p(t)$, mas não de $r(t)$, de modo que $P(T(V)_e)^{-1}$ não seja polinômial. Pelo Lema 2.3.28, segue que $T(V)_e$ não pode ser finitamente gerado.

Por fim, se existir $y \neq x, e$ tal que $V_y \neq 0$, seja $W = V_x \oplus V_e$. Seja $f : V \to W$ a projeção de V em W associada à graduação. Assim, f é um morfismo de álgebras. Se $T(V)_e$

fosse finitamente gerada então $\Bbbk\langle W\rangle_e$ seria finitamente gerada. Mas $W = W_x \oplus W_e$, o que contradiria o parágrafo anterior. Logo $T(V)_e$ não pode ser finitamente gerada. □

2.3.3 Caracterização pela descrição da ação para ações de grupos

Através das séries de Poincaré, iremos caracterizar quando as ações das álgebras de grupo são finitamente geradas. As referências para esta subseção são (Koryukin, 1994), (Dicks e Formanek, 1982/83) , (Green, 1962) e (Canesin, 2020).

Sejam G um grupo finito e $\Bbbk$ um corpo. Um *semianel* é um anel que não necessariamente possui inverso aditivo. Assim, podemos considerar o semianel formado pelas classses de isomorfismos de $\Bbbk G$-módulos finitamente gerados, denotado por $\mathrm{Rep} = \mathrm{Rep}(\Bbbk, G)$. Suas operações são dadas por $[U] + [U'] = [U \oplus U']$ e $[U][U'] = [U \otimes U']$, pela ação diagonal. Perceba que poderiamos formar tal semianel se tivessemos uma álgebra de Hopf, cuja ação no produto tensorial é dada como no início desse capítulo.

Se K é um corpo qualquer, podemos considerar o conjunto dos homomorfismos de semianéis $\mathrm{Char}(\Bbbk, G, K) = \{\mathrm{Rep} \to K, \text{morfismo de semianéis}\}$. Um elemento de $\mathrm{Char}(\Bbbk, G, K)$ é chamado de *caracter*.

Se $\mathrm{char}(K) = 0$, a seguinte função pode ser útil para calcular a série de Poincaré dos invariantes

$$\psi([U]) = \dim_{\Bbbk}(U^g).$$

Proposição 2.3.33. *Seja G um subgrupo finito de $\mathrm{GL}(V)$. Se K é um corpo de caracteristica 0, e ψ é uma K-combinação linear de elementos de $\mathrm{Char}(\Bbbk, G, K)$, com*

$$\psi = \sum_{\chi \in \mathrm{Char}} \langle \chi, \psi \rangle \chi,$$

então $P(T(V)^G) = \sum_{\chi \in \mathrm{Char}} \frac{\langle \chi, \psi \rangle}{1 - \chi[V]t}$ (igualdade válida em $K[[t]]$).

Demonstração: Dado $n \geq 0$, temos

$$\dim_{\Bbbk}(V^{\otimes n})^G = \psi([V^{\otimes n}]) = \sum_{\chi \in \mathrm{Char}} \langle \chi, \psi \rangle \chi([V^{\otimes n}]) = \sum_{\chi \in \mathrm{Char}} \langle \chi, \psi \rangle \chi([V])^n.$$

Dessa forma, vale

$$\begin{aligned} P(T(V)^G) &= \sum_{n \geq 0} \dim_{\Bbbk}(V^{\otimes n})^G t^n = \sum_{n \geq 0} \sum_{\chi \in \mathrm{Char}} \langle \chi, \psi \rangle \chi([V])^n t^n \\ &= \sum_{\chi \in \mathrm{Char}} \langle \chi, \psi \rangle \sum_{n \geq 0} \chi([V])^n t^n = \sum_{\chi \in \mathrm{Char}} \frac{\langle \chi, \psi \rangle}{1 - \chi[V]t}. \end{aligned}$$

□

Assim podemos calcular a série de Poincaré no caso em que $\Bbbk$ é um corpo de caracterís-

tica $p > 0$ e $H = \Bbbk C_p$, para caracterizar quando a subálgebra de invariantes é finitamente gerada.

Exemplo 2.3.34. *Vamos olhar para as classes de indecomponíveis de $\Bbbk G$-módulos em que G é um grupo cíclico gerado por g de ordem n e $\Bbbk$ um corpo de característica $p > 0$ algebricamente fechado. Escreva $n = p^a m$, em que m é um inteiro não divisível por p.*

Seja V um $\Bbbk C_n$ módulo qualquer, e g o gerador de C_n. Sendo assim, olhar para a ação de g em V dirá a ação de $\Bbbk C_n$. A ação de g em V é um automorfismo em V que possui dimensão finita. Sendo assim, a ação de g em V possui uma forma de Jordan, $V = V_1 \oplus \cdots \oplus V_n$, e essa decomposição é uma decomposição de $\Bbbk G$-módulos.

Além disso, cada V_i é um $\Bbbk G$-módulo indecomponível, pois se V_i é um bloco de Jordan associado ao autovalor λ, então, a ação de g em um submódulo não nulo deverá conter um autovetor associado à λ, logo, não existem dois submódulos com interseção trivial. Além disso, como $g^n = 1$, temos que λ é uma raiz n-ésima da unidade. Como a característica de $\Bbbk$ é p, temos que

$$0 = \lambda^n - 1 = (\lambda^m - 1)^{p^a} \Rightarrow \lambda^m - 1 = 0,$$

ou seja, λ é uma raiz p-ésima da unidade.

Portanto, os módulos indecomponíveis são aqueles cuja ação de g é um bloco de Jordan associado a uma raiz p-ésima da unidade. Suponha que V seja um módulo indecomponível, e que a ação de g em V é um bloco de Jordan associado a λ. Seja $T : V \to V$ a ação de g em V.. Como a característica de $\Bbbk$ não divide m, o polinômio $x^m - 1 = 0$ tem exatamente m raízes distintas $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_m$. Como λ_i não é autovetor de T para $i \geq 2$, $T - \lambda_i I$ é inversível, e, portanto $S = (T - \lambda_2) \cdots (T - \lambda_m)$ é inversível. Assim

$$0 = T^n - I = (T^m - I)^{p^a} = (T - \lambda I)^{p^a} S^{p^a} \Rightarrow (T^m - I)^{p^a},$$

totalizando então $n = p^a m$ módulos indecomponiveis (é claro que dois desses módulos são sempre não isomorfos).

Vamos agora analisar o caso em que $G = C_p$ e $\Bbbk$ é um corpo de caracteristica p. Nesse caso, iremos denotar por $U_1, \ldots, U_p$ os $\Bbbk G$-módulos indecomponíveis tais que a matriz ação de g em U_i é o bloco de Jordan associado a 1, e $\dim(U_i) = i$. Assim, iremos assumir o seguinte resultado.

Teorema. [(Green, 1962) (Teorema 2)] Seja $\omega \in \mathbb{C}$ uma raiz $2p$-ésima da unidade. Para cada $0 \leq k \leq p - 1$, seja $f_k \in \mathbb{Z}[t, t^{-1}]$, definido por

$$f_j(t) = t^{j-1} + t^{j-3} + \cdots + t^{-j+3} + t^{-j+1} = \frac{t^j - t^{-j}}{t - t^{-1}}.$$

Então, a função tal que $\chi_k(U_j) = f_j(\omega^k)$ se estende para um caracter. □

A ideia da demonstração desse resultado é mostrar que existem p estenções dos caracteres do grupo trivial e através de relações álgebricas, mostrar que essas são as estensões. Agora que já sabemos alguns caracteres iremos mostrar que $\psi : \mathrm{Rep} \to \mathbb{C}$ é combinação linear desses caracteres, de modo que podemos usar a Proposição 2.3.33.

Lema 2.3.35. *Vale a igualdade*

$$\psi = \frac{1}{p}\chi_0 + \frac{1}{2p}\sum_{k=1}^{p-1}(\omega^k + 2 + \omega^{-k})\chi_k.$$

Demonstração: Para essa demonstração iremos denotar $\sum_{k=l,s}^{m} f(k)$ para denotar $\sum_{k=0}^{\frac{s-l}{m}} f(l + km)$, se l e s são congruentes modulo m (i.e., os temos vão indo de m em m).

Para cada $1 \leq j \leq p-1$, temos $\omega^j - 1 \neq 0$, e portanto

$$\begin{aligned}\left(\sum_{k=1}^{p-1}(\omega^{kj} + \omega^{-kj})\right)(\omega^j - 1) &= (\omega^j)^p - \omega^j + 1 - (\omega^j)^{-p+1} \\ &= (-1)^j - \omega^j + 1 - (-1)^j\omega^j = (\omega^j - 1)(-1 - (-1)^j) \\ &\Rightarrow \sum_{k=1}^{p-1}(\omega^{kj} + \omega^{-kj}) = -1 - (-1)^j.\end{aligned}$$

E também, para cada $1 \leq j, k \leq p-1$, $\omega^k - \omega^{-k} \neq 0$, e, portanto

$$\begin{aligned}&\left(\omega^{kj} + 2\sum_{s=-(j-1),2}^{j-1}\omega^{ks} + \omega^{-kj}\right)(\omega^k - \omega^{-k}) \\ &= \omega^{k(j+1)} - \omega^{k(j-1)} + 2\sum_{s=-(j-1),2}^{j-1}(\omega^{k(s+1)} - \omega^{k(s-1)}) + \omega^{-k(j-1)} - \omega^{-k(j+1)} \\ &= \omega^{k(j+1)} - \omega^{k(j-1)} + 2(\omega^{kj} + \omega^{k(j-1)} - \omega^{-k(j-1)} - \omega^{-kj}) + \omega^{-k(j-1)} - \omega^{-k(j+1)} \\ &= \omega^{k(j+1)} + 2\omega^{kj} + \omega^{k(j-1)} - \omega^{-k(j-1)} - 2\omega^{kj} - \omega^{-k(j+1)} \\ &= (\omega^k + 2 + \omega^{-k})(\omega^{-kj} - \omega^{-kj}).\end{aligned}$$

Dessa maneira, temos

$$(\omega^k + 2 + \omega^{-k})\frac{(\omega^{kj} - \omega^{-kj})}{(\omega^k - \omega^{-k})} = \omega^{kj} + 2\sum_{s=-(j-1),2}^{j-1}\omega^{ks} + \omega^{-kj} = 2 + \sum_{s=1}^{j-1}2(\omega^{ks} + \omega^{-ks}) + \omega^{kj} + \omega^{-kj}$$

Assim,

$$\begin{aligned}
\sum_{k=1}^{p-1}(\omega^k+2+\omega^{-k})\chi_k(U_j) &= \sum_{k=1}^{p-1}(\omega^k+2+\omega^{-k})\frac{(\omega^{kj}-\omega^{-kj})}{(\omega^k-\omega^{-k})}\\
&= \sum_{k=1}^{p-1}(\omega^k+2+\omega^{-k})\frac{(\omega^{kj}-\omega^{-kj})}{(\omega^k-\omega^{-k})}\\
&= \sum_{k=1}^{p-1}\left[2+\sum_{s=1}^{j-1}2(\omega^{ks}+\omega^{-ks})+\omega^{kj}+\omega^{-kj}\right]\\
&= 2(p-1)+2\sum_{s=1}^{j-1}[(-1)-(-1)^s]+(-1)-(-1)^j\\
&= 2(p-1-(j-1))-1-2\sum_{s=1}^{j-1}(-1)^s-(-1)^j\\
&= 2(p-j)-1-(-1-(-1)^j)-(-1)^j = 2(p-j)\\
&= 2p-2j = 2p\psi(U_j)-2\chi_0(U_j),
\end{aligned}$$

pois $\psi(U_j)=1$ e $\chi_0(U_j)=j$, para todo $1\leq j\leq p$.

Portanto, $\psi=\frac{1}{p}\chi_0+\frac{1}{2p}\sum_{k=1}^{p-1}(\omega^k+2+\omega^{-k})\chi_k$. □

Agora, podemos calcular as Séries de Poincaré.

Proposição 2.3.36. *Se V é um H-módulo, então* $P(T(V)^G)=\frac{1}{2p}\left[\frac{2}{1-\dim(V)t}+\sum_{k=1}^{p-1}\frac{\omega^k+2+\omega^{-k}}{1-\chi_k(V)t}\right]$.

(i) $P(T(U_1)^G)=\frac{1}{1-t}$.

(ii) Se j é par e $1<j<p-1$, então $P(T(U_j)^G)=\frac{1}{2p}\left[\frac{2}{1-jt}+\sum_{k=1}^{p-1}\frac{\omega^k+2+\omega^{-k}}{1-f_j(\omega^k)t}\right]$, *e os denominadores são todos distintos.*

(iii) Se j é ímpar e $1<j<p-1$, então $P(T(U_j)^G)=\frac{1}{p}\left[\frac{1}{1-jt}+\sum_{k=1}^{\frac{p-1}{2}}\frac{2}{1-f_j(\omega^k)t}\right]$, *e os denominadores são todos distintos.*

(iv) $P(T(U_{p-1})^G)=\frac{1-(p-2)t-t^2}{(1-t)(1+t)(1-(p-1)t)}$.

(v) $P(T(U_p)^G)=\frac{1-(p-1)t}{1-pt}$.

Demonstração: A primeira igualdade segue da Proposição 2.3.33, observando que $\chi_0(V)=\dim(V)$. Antes de vermos as séries de Poincaré dos indecomponíveis, vamos precisar das seguintes igualdades.

Se α é uma raíz m-ésima da unidade, então $\sum_{k=1}^{m-1} \alpha^k = -1$ (segue da fórmula da PG) e $\sum_{k=1}^{p-1}(\omega^k + \omega^{-k}) = \sum_{k=1}^{p-1}(\omega^k + \omega^{2p-k}) = \sum_{k=1}^{2p-1} \omega^k - \omega^p = (-1) - (-1) = 0$.

(i) Perceba que $f_1(t) = 1$, portanto

$$\begin{aligned} P(T(U_1)^G) &= \frac{1}{2p}\left[\frac{2}{1-t} + \sum_{k=1}^{p-1}\frac{\omega^k + 2 + \omega^{-k}}{1 - f_1(\omega^k)t}\right] = \frac{1}{2p}\left[\frac{2}{1-t} + \sum_{k=1}^{p-1}\frac{\omega^k + 2 + \omega^{-k}}{1-t}\right] \\ &= \frac{1}{2p(1-t)}\left[2 + \sum_{k=1}^{p-1} 2 + \sum_{k=1}^{p-1}(\omega^k + \omega^{-k})\right] = \frac{1}{1-t}. \end{aligned}$$

(ii) A igualdade segue da igualdade inicial. A verificação de que os denominadores são todos distintos será feito abaixo.

(iii) Para $1 \leq k \leq \frac{p-1}{2}$, temos que $\omega^{-k} = \overline{\omega^k}$ e $\omega^{-(p-k)} = \overline{\omega^{p-k}}$, portanto

$$\begin{aligned} \omega^k + 2 + \omega^{-k} + \omega^{p-k} + 2 + \omega^{-(p-k)} &= 4 + 2(\mathfrak{R}(\omega^k) + \mathfrak{R}(\omega^{p-k})) \\ &= 4 + 2\left(\cos\left(\frac{k\pi}{2p}\right) + \cos\left(\frac{(p-k)\pi}{2p}\right)\right) \\ &= 4. \end{aligned}$$

Além disso, temos

$$f_j(\omega^{p-k}) = \frac{\omega^{(p-k)j} - \omega^{-(p-k)j}}{\omega^{p-k} - \omega^{-(p-k)}} = \frac{-\omega^{-kj} - (-\omega^{kj})}{-\omega^{-k} - (-\omega^{-k})} = \frac{\omega^{kj} - \omega^{-kj}}{\omega^k - \omega^{-k}} = f_j(\omega^k),$$

onde usamos o fato de que j é ímpar para mostrar que $\omega^{(p-k)j} = -\omega^{-kj}$. Portanto, segue a igualdade. O fato de que os denominadores são diferentes será mostrado abaixo.

(iv) Para cada $1 \leq k \leq p-1$, temos que

$$f_j(\omega^k) = \frac{\omega^{(p-1)k} - \omega^{-(p-1)k}}{\omega^k - \omega^{-k}} = \frac{(-1)^k(\omega^{-k} - \omega^k)}{\omega^k - \omega^{-k}} = (-1)^{k+1}.$$

Além disso, também temos que $\sum_{k=1}^{\frac{p-1}{2}} \omega^{2k} + \omega^{-2k} = \sum_{k=1}^{\frac{p-1}{2}} \omega^{2k} + \omega^{2p-2k} = -1$ pois é a soma das potências de ω^2 da primeira até a $(p-1)$-ésima. Como $\sum_{k=1}^{p-1} \omega^k + \omega^{-k} = 0$, segue

que $\sum_{k=1}^{\frac{p-1}{2}} \omega^{2k-1} + \omega^{-(2k-1)} = 1$. Assim

$$\begin{aligned} P(T(U_{p-1})^G) &= \frac{1}{2p}\left[\frac{2}{1-(p-1)t} + \sum_{k=1}^{\frac{p-1}{2}} \frac{\omega^{2k-1}+2+\omega^{-(2k-1)}}{1-t} + \sum_{k=1}^{\frac{p-1}{2}} \frac{\omega^{2k}+2+\omega^{-2k}}{1+t}\right] \\ &= \frac{1}{2p}\left[\frac{2}{1-(p-1)t} + \frac{2(p-1)+1}{1-t} + \frac{2(p-1)-1}{1+t}\right] \\ &= \frac{1-(p-2)t-t^2}{(1-t)(1+t)(1-(p-1)t)}. \end{aligned}$$

(v) Perceba que $f_p(\omega^k) = 0$, para todos $1 \leq k \leq p$, Assim

$$P(T(U_p)^G) = \frac{1}{2p}\left[\frac{2}{1-pt} + \sum_{k=1}^{p-1} \omega^k + 2 + \omega^{-k}\right] = \frac{1}{p}\left[\frac{1}{1-pt} + p - 1\right] = \frac{1-(p-1)t}{1-pt}.$$

Por fim, vamos verificar que os denominadores são todos distintos. Para isso, iremos precisar do seguinte fato de teoria de anéis, se ζ é uma raíz p-ésima da unidade, então, como $x^p - 1$ é um polinômio irredutível em $\mathbb{Q}[x]$, segue que $B = \{1 = \zeta^0, \zeta^1, \ldots, \zeta^{p-1}\}$ é um conjunto $\mathbb{Q}$ linearmente independente.

Sejam $1 < j < p-1$ e $1 \leq k_1 < k_2 \leq p-1$ tais que $f_j(\omega^{k_1}) = f_j(\omega^{k_2})$ e seja $\zeta = \omega^{p+1} = -\omega$ uma raíz p-ésima da unidade. Como, para todo k, $f_j(\omega^k) = (-1)^{k(j-1)} f_j(\zeta^k)$, temos que $(-1)^{k_1(j-1)} f_j(\zeta^{k_1}) = (-1)^{k_2(j-1)} f_j(\zeta^{k_2})$.

Se j é ímpar, então $f_j(\zeta^{k_1}) = f_j(\zeta^{k_2})$. Se j é par, então como B é $\mathbb{Q}$ linearmente independente, k_1 e k_2 não podem ter paridades distintas. Logo, nesse caso também vale que $f_j(\zeta^{k_1}) = f_j(\zeta^{k_2})$.

Seja $f \in \mathrm{Aut}(\mathbb{Q}(\zeta))$ em que $f(\zeta) = \zeta^{k_1}$ e seja $g = f^{-1}$. Assim, $g(\zeta^{k_1}) = \zeta$ e como $g(\zeta^{k_2})$ deve ser raíz de $x^p - 1$, segue que $g(\zeta^{k_2}) = \zeta^a$, para algum a. Assim $f(\zeta^a) = f(\zeta)^a = \zeta^{ak_1}$, ou seja $ak_1 \equiv k_2 \pmod{p}$. Como o inverso de ζ é uma potência em ζ, segue que $f_j(\zeta^{k_1})$ e $f_j(\zeta^{k_2})$ são polinômios em ζ. Assim,

$$f_j(\zeta) = f_j(g(\zeta^{k_1})) = g(f_j(\zeta^{k_1})) = g(f_j(\zeta^{k_2})) = f_j(g(\zeta^{k_2})) = f_j(\zeta^a).$$

Multiplicando os dois lados da igualdade por $(\zeta - \zeta^{-1})(\zeta^a - \zeta^{-a})$, obtemos

$$\zeta^{j+a} - \zeta^{j-a} - \zeta^{-j+a} + \zeta^{-a-j} = \zeta^{ja+1} - \zeta^{ja-1} - \zeta^{-ja+1} + \zeta^{-ja-1} \Rightarrow$$

$$\zeta^{j+a} + \zeta^{-j-a} + \zeta^{ja-1} + \zeta^{-ja+1} = \zeta^{j-a} + \zeta^{-j+a} + \zeta^{aj+1} + \zeta^{-ja-1}.$$

Usando novamente o fato de que B é linearmente independente sobre $\mathbb{Q}$, obtemos que $(j+a, -j-a, ja-1, -ja+1)$ é uma permutação de $(ja+1, -ja-1, -j+a, j-a)$. Logo a diferença dos seus produtos deve ser $0 \pmod{p}$. Sua diferença é $4aj(a^2-1)(j^2-1)$. Como $a \not\equiv 0, 1 \pmod{p}$ e $j \not\equiv 0, 1, -1 \pmod{p}$, segue que $a \equiv -1 \pmod{p}$. Dessa maneira, $k_2 = p - k_1$ de modo que k_1 e k_2 possuem paridades distintas. Portanto j é ímpar. □

Corolário 2.3.37. *Seja $2 \leq j \leq p$. Então $\Bbbk\langle U_j\rangle^G$ não é finitamente gerada.*

Demonstração: Para provar iremos usar a proposição anterior e o Lema 2.3.28. Escreva $P(T(U_j)^G) = \frac{Q_j(t)}{R_j(t)}$, onde Q_j e R_j são polinômios coprimos (podemos fazer isso pela proposição anterior). Assim, temos que $P(T(U_j)^G)R_j(t) = Q_j(t)$. Além disso, como cada elemento do denominador é um fator linear distinto, vejamos qual é o coeficiente de t em $R_j(t)$ em cada um dos casos.

(i) Se $1 < j < p-1$ e j é par, então tal coeficiente é $-j - \sum_{k=1}^{p-1} f_j(\omega^k)$. Vejamos que $\sum_{k=1}^{p-1} f_j(\omega^k) = 0$. Perceba que

$$\begin{aligned}\sum_{k=1}^{p-1} f_j(\omega^k) &= \sum_{k=1}^{p-1}(\omega^{k(j-1)} + \omega^{k(j-3)} + \cdots + \omega^{-k(j-3)} + \omega^{-k(j-1)}) \\ &= \sum_{k=1}^{p-1}\sum_{m=1}^{\frac{j}{2}} \omega^{k(2m-1)} + \omega^{-k(2m-1)} \\ &= \sum_{k=1}^{\frac{p-1}{2}}\sum_{m=1}^{\frac{j}{2}} \omega^{k(2m-1)} + \omega^{-(p-k)(2m-1)} + \omega^{-k(2m-1)} + \omega^{(p-k)(2m-1)} \\ &= 0,\end{aligned}$$

pois $\omega^{(p-k)(2m-1)} = \frac{\omega^{p(2m-1)}}{\omega^{k(2m-1)}} = \frac{(-1)^{2m-1}}{\omega^{k(2m-1)}} = -\omega^{-k(2m-1)}$ (e também $\omega^{-(p-k)(2m-1)} = \omega^{(p-k)*(-(2m-1))} = -\omega^{k*(--(2m-1))} = -\omega^{k(2m-1)}$). Portanto, tal coeficiente deve ser $-j$.

(ii) Se $1 < j < p-1$ e j é impar (p ímpar, se $p = 2$, então, não existem tais j), então o coeficiente é $-j - \sum_{k=1}^{\frac{p-1}{2}} f_j(\omega^k)$. Para chegar a alguma fórmula fechada, perceba que, dado $1 \leq m \leq \frac{j-1}{2}$, pela fórmula da soma da progressão geométrica, temos

$$s_m = \sum_{k=1}^{\frac{p-1}{2}} \omega^{2km} = \frac{\omega^{2m} - (-1)^m}{1-\omega^{2m}}.$$

Dessa forma, se m é par, então $s_m = -1$. Se m é impar, então $s_m = \frac{\alpha+1}{1-\alpha}$, com $\alpha = \omega^{2m}$. Portanto, se $\beta = \overline{\alpha}$, então

$$s_m = \frac{\alpha+1}{1-\alpha} = \frac{\alpha+1}{1-\alpha}\cdot\frac{1-\beta}{1-\beta} = \frac{1-\alpha\beta}{1-2\Re(\alpha)+|\alpha|^2} + \frac{2\,\mathrm{im}(\alpha)}{1-2\Re(\alpha)+|\alpha|^2}i.$$

Logo, como $|\alpha| = 1$, segue que $\alpha\beta = 1$, de modo que $\Re(s_m) = \frac{1-\alpha\beta}{1-2\Re(\alpha)+|\alpha|^2} = 0$.

Em qualquer caso, temos que $\mathfrak{R}(s_m) = \dfrac{(-1)-(-1)^m}{2}$. Assim

$$\begin{aligned}\sum_{k=1}^{\frac{p-1}{2}} f_j(\omega^k) &= \sum_{k=1}^{\frac{p-1}{2}}\left(1+\sum_{m=1}^{\frac{j-1}{2}}\omega^{2km}+\omega^{-2km}\right) = \frac{p-1}{2}+\sum_{m=1}^{\frac{j-1}{2}}\sum_{k=1}^{\frac{p-1}{2}} 2\mathfrak{R}(\omega^{2km}) \\ &= \frac{p-1}{2}+2\sum_{m=1}^{\frac{j-1}{2}}\mathfrak{R}(s_m) = \frac{p-1}{2}+2\sum_{m=1}^{\frac{j-1}{2}}\frac{(-1)-(-1)^m}{2} \\ &= \frac{p-1}{2}+\sum_{m=1}^{\frac{j-1}{2}}(-1)-(-1)^m = \frac{p-1}{2}-\frac{j-1}{2}-\sum_{m=1}^{\frac{j-1}{2}}(-1)^m \\ &= \frac{p-j+1+(-1)^{\frac{j+1}{2}}}{2} > 0.\end{aligned}$$

(iii) Se $j = p-1$, então o coeficiente é $-(p-1)$.

(iv) Se $j = p$, então o coeficiente é $-p$.

Em qualquer caso é diferente de -1. Como o coeficiente de grau 0 de $P(\Bbbk\langle U_j\rangle^G)$ é 1, o coeficiente de grau 1 de $Q_j(t)$ é diferente de 0, assim $P(\Bbbk\langle U_j\rangle^G)^{-1}$ não pode ser polinomial, e, portanto $\Bbbk\langle U_j\rangle^G$ não é finitamente gerada. □

Teorema 2.3.38. *Seja G um subgrupo finito de $\mathrm{GL}(V)$ com $|G| = \mathrm{char}(\Bbbk) > 0$. Então $T(V)^G$ não é finitamente gerada.*

Demonstração: Escreva $V \cong \oplus_{j=1}^{p} U_j^{m_j}$. Se $m_j = 0$, para todo $2 \leq j \leq p$, então G consistiria apenas da transformação identidade, ou seja $|G| = 1$. Assim $m_j > 0$, para algum $2 \leq j \leq p$. Assim, temos um morfismo de $\Bbbk G$-módulos $V \to U_j$ sobrejetor, o que induz um morfismo de álgebras $T(V)^G \to T(U_j)^G$ sobrejetor. Mas pelo corolário anterior, $T(U_j)^G$ não é finitamente gerada, de modo que $T(V)^G$ não pode ser finitamente gerada. □

Temos em constraste, o seguinte resultado para quando a caracteristica difere da ordem do grupo cíclico.

Teorema 2.3.39. *Seja G um subgrupo finito de $\mathrm{GL}(V)$ de ordem prima p e $\Bbbk$ um corpo de característica diferente de p. Se $T(V)^G$ for finitamente gerada então a ação de G é escalar.*

Demonstração: Podemos supor que $\Bbbk$ possui uma raiz p-ésima da unidade ω. Como visto anteriormente, os $\Bbbk G$-módulos indecomponíveis são $U_1, \ldots, U_p$ em que $\dim_{\Bbbk} U_i = 1$ e $g \cdot u = \omega^j u$, $u \in U_j$. Assim, podemos escolher uma base $x_1, \ldots, x_d$ de V tal que $g \cdot x_i = \omega^{j_i} x_i$. Dessa forma, todo monômio $x_{m_1} \cdots x_{m_s} (m_1, \ldots, m_s \in \{1, \ldots, d\})$ é um autovetor para g. Se existir um conjunto finito gerador de $T(V)^G$ como álgebra, então esse conjunto poderia ser tomado como um conjunto finito de monômios (dado que o conjunto de monômios é linearmente independente e que cada monômio é autovalor).

Suponha que a ação de G não é escalar. Assim, podemos assumir sem perda de generalidade que $j_1 \neq j_2$. Para cada m inteiro, construa indutivamente um monômio w_m de comprimento m tal que nenhum segmento inicial de w_m é invariante. Esse monômio

pode ser construído pois, dado w monômio, wx_1 ou wx_2 não é invariante. Assim, como $j_1 \neq j_2$, existe $n > 0$ tal que $w_m x_1^n$ ou $w_m x_2^n$ é invariante, (iremos chamar tal monômio de z_m). Suponha que exista um conjunto finito de monômios geradores dos invariantes, e seja m o comprimento do maior monômio. Assim, z_m seria um invariante não gerado por esse conjunto finito. Contradição. □

Lema 2.3.40. *Se G é um subgrupo finito de* $\mathrm{GL}(V)$ *tal que $T(V)^G$ é finitamente gerado, então $T(V)^H$ é finitamente gerado para todo H subgrupo de G.*

Demonstração: Sabemos que $T(V)^H$ é uma álgebra livre. Se $T(V)^H$ não for finitamente gerada, teríamos uma cadeia infinita de subálgebras livres de $T(V)^G$. Como $T(V)^G$ é finitamente gerada, por correspondência, teriamos uma cadeia infinita de subgrupos de G (que contém H), absurdo. □

Com isso, temos uma outra caracterização.

Teorema 2.3.41. *Seja G um grupo finito de* $\mathrm{GL}(V)$. *Então $T(V)^G$ é finitamente gerado se e somente se G é formado por matrizes escalares. Nesse caso, temos que G é gerado por ωI, onde ω é uma raiz $|G|$-ésima da unidade e $T(V)^G = \Bbbk\langle V^{\otimes |G|}\rangle$.*

Demonstração: Se G for escalar, então G é um subgrupo finito das matrizes da forma αI com $\alpha \in \Bbbk^*$ que é isomorfo a $\Bbbk^*$, portanto é um grupo cíclico da gerado por ωI, onde ω é uma raiz $|G|$-ésima da unidade. Além disso, $T(V)^G = \Bbbk\langle V^{\otimes n}\rangle$, e a subálgebra de invariantes é gerada por uma base de $V^{\otimes n}$ que é finita.

Suponha que $T(V)^G$ é finitamente gerada. Seja N o subgrupo de G formado pelas matrizes escalares. Assim, N é um subgrupo central. Assim, temos uma ação de $\frac{G}{N}$ em $T(V)^N = T(V^{\otimes |N|})$ induzida pela ação de G.

Assim, $T(V^{\otimes |N|})^{\frac{G}{N}} = T(V)^G$ é finitamente gerada. Pelo lema anterior, temos que para todo H subgrupo de $\frac{G}{N}$, $T(V^{\otimes |N|})^H$ é finitamente gerado. Seja p um primo que divide $\frac{G}{N}$ e tome H um subgrupo de ordem p. Se $\mathrm{char}(\Bbbk) = p$, então, sabemos que $T(\langle V^{\otimes |N|})^H$ não pode ser finitamente gerado. Logo, temos que $\mathrm{char}(\Bbbk) \neq p$. Nesse caso, como a ação de cada elemento não nulo de $\frac{G}{N}$ não é escalar, segue que a ação de H não é escalar, de modo que $T(V^{\otimes |N|})^H$ não pode ser finitamente gerada. Logo $\frac{G}{N}$ é trivial e a ação de G em V é escalar. □

Agora iremos olhar para outra caracterização desse caso.

Seja V um espaço vetorial de dimensão finita e $G \leq \mathrm{Aut}(V)$, um subgrupo finito. Dessa forma G age por automorfismos em R, via

$$g \cdot (v_1 \cdots v_n) = (g \cdot v_1) \cdots (g \cdots v_n).$$

Além disso, também existe a ação dos grupos simétricos nas componentes homogêneas de R, de modo que se $X = \{x_1, \ldots, x_n\}$ é uma base de V, então

$$(x_{i_1} \cdots x_{i_m}) \cdot \tau = x_{\tau^{-1}(i_1)} \cdots x_{\tau^{-1}(i_m)}$$

O suporte possui a seguinte propriedade

Lema 2.3.42. *Seja A um subconjunto de R. Se A for estável pela ação de G (isto é $g \cdot A = A$, para todo $g \in G$), então $s(A)$ é estável pela ação de G.*

Demonstração: Seja $g \in G$, temos que $A = g \cdot A \subseteq g \cdot T(s(A)) = T(g \cdot s(A))$. Assim, como $g \cdot s(A)$ é um subespaço de V, temos que $s(A) \subseteq g \cdot s(A)$. Como G age por automorfismos e $s(A)$ possui dimensão finita, temos a igualdade. □

Se X é uma base de V, então o semigrupo (multiplicativo) gerado por X em R é um semigrupo livre, e a álgebra R é livre em X. Com essa base X fixada, trataremos os elementos do semigrupo como monômios, e os elementos de X de letras. Um elemento arbitrário de R é uma combinação linear de monômios. Seja A um conjunto de elementos de R (respectivamente M um conjunto de monômios). Se y é uma letra, dizemos que y possui uma recorrência em A (resp. M), se y aparece em algum monômio de algum elemento de A (resp. algum monômio de M). Além disso, dizemos que uma sequência de letras $y_1, y_2, \ldots$ é compatível com A (resp. M), se algum elemento de A possuir algum monômio da forma $y_1 \cdots y_n$, para algum $n \in \mathbb{N}$ (resp. for um elemento de M). Com isso, temos

Lema 2.3.43. *Seja M um conjunto de monômios finito. Se o semigrupo gerado por M for fechado pela ação dos grupos simétricos, então toda sequência (infinita) de letras $y_1, y_2, \ldots$ que possui recorrência em M é compatível com M.*

Demonstração: Como M é finito, possui um monômio de maior comprimento, seja m o maior comprimento de tal monômio. Como cada letra y_i possui uma recorrência em M, tome e_i um monômio no qual y_i é uma letra. Considere o monômio $e = e_1 e_2 \cdots e_m$.

Dessa forma e está no semigrupo gerado por M que é fechado pela ação dos grupos simétricos, de modo que $y_1 y_2 \cdots y_m z$ também está nesse semigrupo, para algum monômio z. Isso quer dizer que existem monômios $v_1, \ldots, v_n \in M$ tal que $v_1 \cdots v_n = y_1 y_2 \cdots y_m z$. Como o tamanho de v_1 é menor ou igual a m, existe l natural (menor ou igual a m) tal que $y_1 \cdots y_l = v_1 \in M$. □

Lema 2.3.44. *Seja A um conjunto finito de elementos de R e seja B a álgebra gerada por A. Se B for fechada pela ação dos grupos simétricos e homogênea, então toda sequência de letras com ocorrência em A é compatível com A.*

Demonstração: Basta considerar M o conjunto dos monômios de A e aplicar o resultado anterior. □

Lema 2.3.45. *Seja $\mathfrak{G}$ um automorfismo de V (que possui dimensão pelo menos 2), e suponha que $\Bbbk$ seja algebricamente fechado. Se $\mathfrak{G}$ não for escalar (isto é, múltiplo da identidade), então existe uma base X de V e uma sequência infinita de letras de X que não é compatível com a álgebra dos invariantes não comutativos desse automorfismo.*

Demonstração: Suponha que $\mathfrak{G}$ não é diagonalizável. Então, existe $X = \{x_1, , \ldots, x_n\}$ uma base de V em que $\mathfrak{G}$ está na forma de Jordan. Como $\mathfrak{G}$ não é diagonalizável, podemos supor sem perda de generalidade que x_1 e x_2 estão no mesmo bloco, onde $\mathfrak{G}(x_1) = \rho x_1 + x_2$

e $\mathfrak{G}(x_2) = \rho x_2 + y$, onde $y \in \text{span}(x_3, \dots, x_n)$. Seja m um inteiro positivo qualquer, vejamos que x_1^m não pode ser invariante. Suponha que seja, então teriamos que

$$x_1^m = \mathfrak{G}(x_1^m) = \mathfrak{G}(x_1)^m = (\rho x_1 + x_2)^m.$$

A partir da comparação de coeficientes, o único jeito de isso acontecer é se $\rho^m = 1$ e $\rho = 0$ (comparando os coeficientes de x_1^m e $x_1 x_2^{m-1}$). Mas isso é impossível, logo x_1^m não pode ser invariante por $\mathfrak{G}$, para nenhum m. Dessa forma, a sequência $x_1, x_1, x_1, \dots$ satisfaz às condições do enunciado.

Suponha no entanto que $\mathfrak{G}$ seja diagonalizável e seja $X = \{x_1, \dots, x_n\}$ uma base de autovetores, em que x_i é associado ao autovalor ρ_i, e suponha sem perda de generalidade que $\rho_1 \neq \rho_2$ (caso todos fossem iguais, o automorfismo seria linear). Seja $y \in R$ não nulo qualquer. Vejamos que pelo menos um dos dois entre yx_1 e yx_2 não é invariante por $\mathfrak{G}$. Se yx_1 for invariante por $\mathfrak{G}$, então

$$yx_1 = \mathfrak{G}(yx_1) = \mathfrak{G}(y)\mathfrak{G}(x_1) = \rho_1 \mathfrak{G}(y) x_1$$

$$\Rightarrow (\rho_1 y - \mathfrak{G}(y))x_1 = 0 \Rightarrow \rho_1 y - \mathfrak{G}(y) = 0 \Rightarrow \rho_1 y = \mathfrak{G}(y).$$

De modo análogo, se yx_2 fosse invariante por $\mathfrak{G}$, teriamos que $\mathfrak{G}(y) = \rho_2 y$. Mas $\rho_1 \neq \rho_2$ e $y \neq 0$, chegando em uma contradição. Então pelo menos um dos dois não é invariante. Sendo assim, construa indutivamente a sequência $y_1, y_2, \dots$, de modo que $y_1 \cdots y_s$ não é invariante para nenhum s (para fazer isso, basta começar com $y = 1$ para $s = 1$ e para $s > 1$, tome $y = y_1 \cdots y_{s-1}$). Dessa forma, essa sequência construída satisfaz às propriedades pedidas. □

Podemos assumir que o corpo é algebricamente fechado. Para isso, perceba que suponha que $\mathbb{l}/\Bbbk$ é uma extensão de corpos e V um $\Bbbk$-espaço e G é um grupo de automorfismos de V (em que V é um $\Bbbk$-espaço de dimensão finita). Seja $W = V \otimes_{\Bbbk} \mathbb{l}$ visto como $\mathbb{l}$-espaço e seja $G' = \{g' = g \otimes \text{id} : g \in G\}$. Dessa forma, G' age por automorfismos em W. Então, $T(V)^G$ é finitamente gerado (como $\Bbbk$-álgebra) se e somente se $l\langle W\rangle^{G'}$ é finitamente gerado (como l-álgebra). Agora iremos juntar todos os lemas, para chegar no resultado principal dessa seção.

Teorema 2.3.46. *Seja G um grupo (não necessariamente finito) de automorfismos de V. Se a álgebra de invariantes for finitamente gerada, então G age no suporte da álgebra de invariantes como um grupo finito cíclico de matrizes escalares.*

Demonstração: Como citado anteriormente, podemos supor que $\Bbbk$ é álgebricamente fechado, e seja U o suporte de $T(V)^G$. Como R^G é estável relativo a ação de G, pelo Lema 2.3.42, temos que U é estável relativo a ação de G. Seja H o grupo dos automorfismos de G restritos a U. Se a dimensão de U for menor do que 2, o resultado é trivial.

Seja $\mathfrak{G} \in H$ qualquer. Perceba que vale $T(V)^G \subseteq T(U)^{\mathfrak{G}}$, pois dado $f \in R^G$, pela definição de U, temos que $f \in T(U)$. Além disso, existe $g \in G$ tal que sua restrição à H é $\mathfrak{G}$, de modo que tenhamos, $\mathfrak{G} \cdot f = g \cdot f = f$, e assim $f \in T(U)^{\mathfrak{G}}$.

Suponha que $\mathfrak{G}$ não é escalar, então, pelo Lema 2.3.45, existiria uma base de U e uma sequência de letras nessa base que não é compatível com $T(U)^H$. Mas $T(V)^G \subseteq \Bbbk\langle U\rangle^H$, o

que implicaria que existe uma sequência de letras em V que não é compatível com $T(V)^G$, contradição com o Lema 2.3.44, de modo que $\mathfrak{G}$ seja escalar.

Dessa forma H é um grupo de matrizes escalares. Suponha que H é infinito, e seja $f \in T(V)^G \subseteq T(U)$ homogêneo de grau s. Como existem no máximo s escalares α tais que $\alpha^s = 1$, e H é infinito, seja $\alpha \in H$ tal que o escalar associado não seja raiz s-ésima da unidade. Dessa forma, temos que

$$f = \alpha \cdot f = \alpha^s f \neq f,$$

pois $f \neq 0$. Logo, o único elemento de $T(V)^G$ é 0 (pois essa álgebra é homogênea). Mas isso, implicaria que $U = 0$, de modo que H teria que ser trivial, contradição. Logo H é finito.

Da mesma forma como fizemos anteriormente, temos que H é na verdade um subgrupo (finito) de $\Bbbk$ que é um corpo, de modo a ser um grupo cíclico. □

2.3.4 Caracterização pela descrição da ação para ações de álgebras de Hopf

Nessa seção iremos considerar o caso em que H é uma álgebra de Hopf gerada por elementos group-like e skew primitivos. Este caso é uma generalização da subseção anterior, pois a álgebra de grupo satisfaz essas propriedades. Assim, obteremos que a subálgebra de invariantes será finitamente gerada se e somente se a ação for escalar. Para esta seção, a referência é (Vitor O. Ferreira e L. S. I. Murakami, 2007).

Definição 2.3.47. Seja H uma álgebra de Hopf e A um H-módulo. Dizemos que a ação de H em A é *escalar* se para todo $h \in H$, existe $\lambda_h \in \Bbbk$ tal que $h \cdot a = \lambda_h a$, para todo $a \in A$.

Começaremos mostrando que qualquer ação escalar possui a subálgebra de invariantes finitamente gerada. Precisaremos do seguinte lema.

Lema 2.3.48. *Sejam H uma álgebra de Hopf e A uma H-módulo álgebra. Sejam $a, b \in A$ tais que $a, ab \in A^H$. Se a não for divisor de zero em A, então $b \in A^H$.*

Demonstração: Dado $h \in H$, temos

$$\begin{aligned}\varepsilon(h)ab = h \cdot (ab) &= \sum_{(h)} (h_{(1)} \cdot a)(h_{(2)} \cdot b) \\ &= \sum_{(h)} \varepsilon(h_{(1)})a(h_{(2)} \cdot b) = a \sum_{(h)} (\varepsilon(h_{(1)})h_{(2)}) \cdot b = a(h \cdot b).\end{aligned}$$

Como a não é divisor de zero, segue que $h \cdot b = \varepsilon(h)b$, ou seja, $b \in A^H$. □

Teorema 2.3.49. *Seja H uma álgebra de Hopf e A uma H-módulo álgebra que é um domínio de integridade. Suponha que exista um conjunto finito X gerador de A, tal que para todo $h \in H$, exista $\lambda_h \in \Bbbk$ de modo que $h \cdot x = \lambda_h x$, com $x \in X$. Então A^H é uma álgebra finitamente gerada. Em particular, se A for a álgebra livre e a ação de H for escalar, teremos que A^H será finitamente gerada.*

Demonstração: Sejam n um número natural, $n \geq 1$ e $h \in H$ e considere $x_1, \dots, x_n \in X$ (não necessariamente distintos). Assim

$$\begin{aligned} h \cdot (x_1 \cdots x_n) &= \sum_{(h)} (h_{(1)} \cdot x_1) \cdots (h_{(n)} \cdot x_n) \\ &= \sum_{(h)} (\lambda_{h_{(1)}} x_1) \cdots (\lambda_{h_{(n)}} x_n) \\ &= \sum_{(h)} (\lambda_{h_{(1)}} \cdots \lambda_{h_{(n)}}) x_1 \cdots x_n. \end{aligned}$$

Dessa forma, se $\lambda_{h,n} = \sum_{(h)} (\lambda_{h_{(1)}} \cdots \lambda_{h_{(n)}})$ e w for um produto de n elementos de X, então $h \cdot w = \lambda_{h,n} w$.

Como A é gerado por X, então, o conjunto $L = \{x_1 \cdots x_n : n \in \mathbb{N}, x_i \in X\}$ gera A como espaço vetorial. Seja B uma base de A formada por um subconjunto de L que contenha 1.

Considere uma função $d : B \to \mathbb{N}$, onde para cada $v \in B \setminus \{1\}$, v é um produto de $d(v)$ elementos de X e $d(1) = 0$ (como todo elemento de B é um elemento de L, sabemos que necessariamente todo elemento de B é um produto de alguns elementos de X, de modo que basta apenas escolher alguma delas).

Suponha que exista $v \in B \cap A^H$ e $d(v) = n$. Então, se w for um produto de n elementos de X, então $\lambda_{h,n} v = h \cdot v = \varepsilon(h) v$.

Seja $a \in A^H$. Para cada $v \in B$, tome $\alpha_v \in \Bbbk$ tal que $a = \sum_{v \in B} \alpha_v v$. Considere $\operatorname{supp}(a) = \{v \in B : \alpha_v \neq 0\}$. Vejamos que $\operatorname{supp}(a) \subseteq A^H$. Dado $h \in H$, temos

$$\sum_{v \in B} \varepsilon(h) \alpha_v v = \varepsilon(h) a = h \cdot a = h \cdot \left(\sum_{v \in B} \alpha_v v \right) = \sum_{v \in B} \alpha_v (h \cdot v) = \sum_{v \in B} \alpha_v \lambda_{h,d(v)} v$$

Como B é uma base, segue que, para todo $v \in B$, vale $\varepsilon(h)\alpha_v = \alpha_v \lambda_{h,d(v)}$. Se $v \in \operatorname{supp}(a)$, então $\varepsilon(h) = \lambda_{h,d(v)}$. Dessa forma, $v \in A^H$. Logo, todo elemento de A^H é combinação linear de elementos de $A^H \cap B$.

Se $A^H = \Bbbk 1$, então A^H é finitamente gerada. Caso contrário, sabemos pelo parágrafo anterior que algum produto de elementos de X é invariante. Seja t o menor inteiro positivo tal que existe um produto de t elementos de X que é invariante. Vejamos que A^H é gerado por todos os produtos de t elementos de X. Como X é finito, isso basta para provar que A^H é finitamente gerada.

Seja A' a subálgebra de A gerada por tais elementos. Sabemos que $A' \subseteq A^H$. Vejamos a outra inclusão. Seja $v \in A^H \cap B$. Então v é produto de n elementos de X. Utilize o algoritmo da divisão para achar q, r inteiros, com $0 \leq r < t$ tais que $n = qt + r$. Se $r > 0$, podemos escrever $v = uw$, onde u é o produto de qt elementos de X e w produto de r elementos de X. Assim, $u \in A'$. Como A é um domínio de integridade, não possui divisores de zero. Além disso, $u, v = uw \in A^H$, logo $w \in A^H$, pelo Lema 2.3.48. Mas w é o produto de r elementos de X e $r < t$, contradição. Logo $t = 0$. Portanto $A' = A^H$.

□

Vamos tentar ver uma certa recíproca. Para isso, demonstraremos alguns lemas. Iremos então considerar, H uma álgebra de Hopf e X um conjunto qualquer, em que $\Bbbk X$ é um H-módulo e $R = \Bbbk\langle X\rangle$ é o H-módulo álgebra induzido. Além disso, denotaremos por $\langle X\rangle$, o monoide (com 1) gerado por X (ou seja, o conjunto dos monômios). Dado $f \in \Bbbk\langle X\rangle$, onde $f = \sum_{w\in\langle X\rangle} \alpha_w w$, definimos o suporte de f, por $\{w \in \langle X\rangle : \alpha_w \neq 0\}$. Além disso, a ação sempre será fiel.

Em $\Bbbk[y,z]$, denotaremos por $c_n(y,z) = \sum_{i=0}^{n-1} y^{n-1-i}z^i$.

Lema 2.3.50. *Suponha que X é finito, digamos $X = \{x_1,\dots,x_n\}$ e $\sigma,\tau \in G(H)$ e $\delta \in P_{(\sigma,\tau)}(H)$. Suponha também que σ e τ agem escalarmente em R, baseados respectivamente em η e μ e $[\delta]_X$ esteja na forma de Jordan. Então, para cada $m > 0$ e cada $i = 1,\dots,r$, existe $f \in R$ homogênea de grau m satisfazendo.*

1. *Existe $g \in R$ tal que $\delta \cdot f = c_m(\eta,\mu)g$.*
2. $\operatorname{supp}(f) \cap x_i\langle X\rangle \neq \emptyset$.

Observação 2.3.51. Geralmente $c_n(\eta,\mu) \in \Bbbk$. Então a primeira condição do lema cobre o caso em que esse valor é 0.

Demonstração: Seja J o bloco de Jordan associada à i-ésima entrada da diagonal principal e s a última entrada do bloco J, e λ é o autovalor associado a J. Sobre essas condições, considere

$$f = \sum_{j_1+\cdots+j_n = i+(n-1)s,\, j_l \leq s} x_{j_1}\cdots x_{j_n}.$$

Vejamos que f sobre essas condições satisfaz às propriedades requeridas.

Primeiramente, é claro que f é homogênea de grau n. Também é claro que $x_i x_s \cdots x_s \in \operatorname{supp}(f)$, e portanto $\operatorname{supp}(f) \cap x_i\langle X\rangle \neq \emptyset$. Além disso, como $j_m \leq s$ para todo m, segue que

$$i + (n-1)s - j_m = j_1 + \cdots + j_n - j_m \leq (n-1)s \Rightarrow i \leq j_m \leq s$$

Ou seja, todas as variáveis estão no mesmo bloco de Jordan. Além disso, se $x_{j_1}\cdots x_{j_s}$ está no suporte de f, então

$$\delta\cdot(x_{j_1}\cdots x_{j_s}) = \lambda c_n(\eta,\mu)x_{j_1}\cdots x_{j_n} + \eta^{n-1}x_{j_1+1}x_{j_2}\cdots x_{j_n} + \cdots$$

$$+\eta\mu^{n-2}x_{j_1}x_{j_2}\cdots x_{j_{n-1}+1}x_{j_n} + \mu^{n-1}x_{j_1}\cdots x_{j_{n-1}}x_{j_n}$$

(onde vemos x_{s+1} como sendo 0). Portanto, podemos concluir que $\delta\cdot f = \lambda c_n(\eta,\mu)f + f'$, onde $\operatorname{supp}(f') \subseteq \{x_{l_1}\cdots x_{l_n} : l_1+\cdots+l_n = (i+1)+(n-1)s, l_q \leq s\ \forall q\}$. Por um raciocínio análogo ao feito anteriormente, temos que $i+1 \leq l_m$, para todo m. Dessa forma, temos que $x_{l_1}\cdots x_{l_n}$ ocorre no suporte da ação de δ em $x_{l_1-1}x_{l_2}\cdots x_{l_n},\dots,x_{l_1}\cdots x_{l_n-1}$ com coeficientes respectivamente $\eta^{n-1},\eta^{n-2}\mu,\dots,\mu^{n-1}$. Portanto, existe $f'' \in R$ tal que $f' = c_n(\eta,\mu)f''$. Concluimos assim que $\delta\cdot f = c_n(\eta,\mu)(\lambda f + f'')$.

□

Lema 2.3.52. *Seja $x \in X$. Se existe $f \in R^H$ com $\operatorname{supp}(f) \cap x\langle X\rangle \neq \emptyset$, então, para cada inteiro positivo n, existe $\tilde{f} \in R^H$, tal que $\operatorname{supp}(\tilde{f}) \cap x^n\langle X\rangle \neq \emptyset$.*

Demonstração: Vamos provar isso por indução em n. Podemos supor sem perda de generalidade que f é homogêneo.Seja m o grau de f e $w \in \langle X\rangle$ tal que $f = xw$.

A afirmação é válida para $k = 1$, e para $k > 1$ seja $\tilde{f} \in R^H$ homogêneo de grau t tal que $\operatorname{supp}(\tilde{f}) \cap x^{n-1}\langle X\rangle \neq \emptyset$, com $x^{n-1}\tilde{w} \in \operatorname{supp}(\tilde{f})$ para algum $\tilde{w} \in \langle X\rangle$. Pelo Lema 2.3.11, temos que $\bar{f} = \tau_{n-1,t-n,m}(\tilde{f}f) \in R^H$ e $x^n w\tilde{w} \in \operatorname{supp}(\bar{f})$. □

Teorema 2.3.53. *Suponha que H tenha dimensão finita e que H seja gerada por elementos group-like e skew-primitivos. Então R^H é finitamente gerada se e somente se a ação de H em R for escalar e X for finito.*

Demonstração: Se X for finito e a ação de H em R for escalar, então R^H é finitamente gerada pelo Teorema 2.3.49.

Vejamos o outro lado. Suponha que R^H seja finitamente gerada. Suponha por absurdo que X é infinito. Como R^H é finitamente gerada, existe n inteiro positivo e $x_1, \dots, x_n \in X$ tal que $R^H \subseteq \Bbbk\langle x_1, \dots, x_n\rangle$ (de fato, basta pegar as letras no monômios do suporte de um conjunto gerador).

Assim, como X é infinito, teriamos uma cadeia infinita de inclusões próprias

$$R^H \subseteq \Bbbk\langle x_1, \dots, x_n\rangle \subsetneq \Bbbk\langle x_1, \dots, x_n, x_{n+1}\rangle \subsetneq \dots$$

de subálgebras livres de R que contenham R^H. Pelo teorema da correspondência, teriamos uma cadeia infinita descendente de subespaços próprios de H. Mas H tem dimensão finita, de modo que não pode ter uma cadeia infinita de inclusões próprias de subespaços. Logo X é finito.

É claro que se $|X| = 1$, então a ação de H em R será escalar. Suponha então que $|X| > 1$, $X = \{x_1, \dots, x_r\}$. Seja H_0 o coradical de H. Como H é gerado por elementos group-like e skew-primitivos, $H_0 = \Bbbk G(H)$ pelo Corolário 1.1.54. Pelo teorema da correspondência R^{H_0} é uma subálgebra livre que contem R^H que é finitamente gerada (mesmo argumento do parágrafo anterior). Como H é finito, $G(H)$ é finito, logo a ação de $G(H)$ em H é escalar pelo Teorema 2.3.41.

Podemos supor que $\Bbbk$ é algebricamente fechado, pois podemos considerar o produto tensorial com $\bar{\Bbbk}$, de modo que tenhamos espaços sobre corpos algébricamente fechados.

Seja $\delta \in H$ um elemento (σ, τ)-primitivo, com $\sigma, \tau \in G(H)$. Seja $H(\delta)$ a subálgebra de H gerada por $\{\delta, \sigma, \tau\}$. Dessa forma, temos que $H(\delta)$ é uma subálgebra de Hopf de H, e pelo teorema da correspondência $R^{H(\delta)}$ é uma subálgebra livre de R.

Como $\Bbbk$ é algébricamente fechado, podemos supor que $[\delta]_X$ está na forma de Jordan (pois qualquer base de $\sum_{x\in X} \Bbbk x$ é uma base de R como álgebra). Vejamos que $[\delta]_X$ é na verdade uma matriz diagonal. Suponha que $[\delta]_X$ não seja diagonal, e, sem perda de generalidade, suponha que

$$\delta \cdot x_1 = \lambda x_1 + x_2$$

$$\delta \cdot x_2 = \lambda x_2 + \zeta x_3,$$

para algum $\lambda \in \Bbbk$ e $\zeta \in \{0, 1\}$. Além disso, $x_1, x_2 \notin \operatorname{supp}(\delta \cdot x_i)$, para $i \geq 3$. Seja C um conjunto finito que gera $R^{H(\delta)}$, e seja A o conjunto dos monômios diferente de 1 que aparecem em algum suporte de algum elemento de C.

Seja $f \in R^{H(\delta)}$ que satisfaça o Lema 2.3.50 com $i = 1$ e m a definir. Seja $n = |G(H)|$. Assim, existe $g \in R$ tal que $\delta \cdot f = c_m(\eta, \mu)g$ e $\operatorname{supp}(f) \cap x_1\langle X\rangle \neq \emptyset$. Por Lagrange, vale $\sigma^n = 1 = \tau^n$, portanto $\eta^n = 1 = \mu^n$.

- Se $\eta \neq \mu$, temos que $c_n(\eta, \mu) = 0$, e portanto $\delta \cdot f = 0 = \varepsilon(\delta)f$, ou seja f é invariante sobre δ. Como f é homogêneo de grau n, segue que f é invariante sobre σ e sobre τ. Dessa forma, $f \in R^{H(\delta)}$.

- Se $\eta = \mu$, como a ação é fiel, temos que $\sigma = \tau$. Nesse caso,

  $$\Delta(\sigma^{-1}\delta) = 1 \otimes \sigma^{-1}\delta + \sigma^{-1}\delta \otimes 1,$$

  ou seja $\sigma^{-1}\delta$ é um elemento primitivo. Assim, se a característica de $\Bbbk$ for 0, a subálgebra gerada por esse elemento possui dimensão infinita. Logo, $\Bbbk$ possui característica positiva. Tome f do Lema 2.3.50, igual feito no item anterior com $m = np$. Sendo assim, como $c_{np}(\eta, \eta) = np\eta^{np-1} = 0$. Dessa forma, $\delta \cdot f = 0 = \varepsilon(\delta)f$. Portanto, como f tem grau np, segue que $\phi = f \in R^{H(\delta)}$.

Sendo k inteiro maior que o maior elemento de A, e usando o fato de que $R^{H(\delta)}$ é uma álgebra com inserção, podemos achar um elemento $f \in R^{H(\delta)}$ tal que $\operatorname{supp}(f) \cap x_1^k\langle X\rangle \neq \emptyset$. Assim, existe $m \geq 1$ tal que $x_1^m \in A$. Em particular, existe um elemento homogêneo $d \in R^{H(\delta)}$ de grau m tal que $x_1^m \in \operatorname{supp}(d)$, sem perda de generalidade, podemos escrever $d = x_1^m + \alpha x_1^{m-1}x_2 + \bar{d}$, com $x_1^m, x_1^{m-1}x_2 \notin \operatorname{supp}(\bar{d})$. Assim

$$\delta \cdot d = \lambda c_m(\eta, \mu)x_1^m + \mu^{m-1}x_1^{m-1}x_2 + \alpha(\lambda\eta c_{m-1}(\eta, \mu) + \lambda\mu^{m-1})x_1^{m-1}x_2\bar{\bar{d}},$$

com $x_1^m, x_1^{m-1}x_2 \notin \operatorname{supp}\left(\bar{\bar{d}}\right)$. Como $d \in R^{H(\delta)}$, segue que $\lambda c_m(\eta, \mu) = 0$ e $\mu^{m-1} = \mu^{m-1} + \alpha\lambda c_m(\eta, \mu) = \mu^{m-1} + \alpha\lambda(\eta c_{m-1}(\eta, \mu) + \mu^{m-1}) = 0$, logo $\mu = 0$, absurdo, portanto $[\delta]_X$ é diagonal.

Assim, existem escalares $\lambda_i \in \Bbbk$ tal que $\delta \cdot x_i = \lambda_i x_i$, para todo i. Vamos mostrar que esses escalares são iguais. Como $H(\delta)$ é gerada por elementos de H cujas ações em $\sum \Bbbk x$ são diagonais, então para cada $x \in R^{H(\delta)}$, todo monômio do seu suporte estará em $R^{H(\delta)}$. Suponha que não existe monômio w tal que $wx_i \in A$ para todo i. Então, conseguiriamos achar um monômio $\tilde{w}$ de tamanho maior que o maior elemento de A, de modo que nenhum segmento inicial de $\tilde{w}$ esteja em A. Para cada $i = 1, \ldots, n$ existe $f_i \in R^{H(\delta)}$ tal que $\operatorname{supp}(f_i) \cap x_i\langle X\rangle \neq \emptyset$ (pode-se usar o Lema 2.3.50 para achar tal f_i). Usando novamente o fato de que $R^{H(\delta)}$ é uma álgebra com inserção, podemos encontrar $f \in R^{H(\delta)}$ com $\operatorname{supp}(f) \cap \tilde{w}\langle X\rangle \neq \emptyset$. Pela construção de A, algum segmento inicial de $\tilde{w}$ deve estar em A, absurdo. Logo, existe w monômio tal que $wx_i \in A$ para todo i.

Assim, seja $w = x_{i_1} \cdots x_{i_t}$ um monõmio que satisfaça essa propriedade. Dessa forma, temos que $\delta \cdot w = \xi w$, onde $\xi = \sum_{j=1}^{t} \lambda_{i_j}\eta^{t-j}\mu^{j-1}$. Logo, para cada i, wx_i é invariante por ser

um monômio do suporte de um elemento invariante, e, portanto

$$0 = \delta \cdot (wx_i) = \xi\eta wx_i + \mu^t \lambda_i wx_i \Rightarrow \lambda_i = -\frac{\eta\xi}{\mu^t}$$

Como esse resultado foi obtido independente de i, segue que todos os λ são iguais, e, portanto, a ação é escalar.

□

Capítulo 3

Ações de álgebras de Hopf cocomutativas

No caso em que H é cocomutativo, e V é um H-módulo, temos a ação dos grupos simétricos nas componentes homogêneas. Assim, apesar dos invariantes serem finitamente gerados apenas em condições específicas, com essas ações podemos achar uma outra condição de finitude que acontece mais frequentemente. Para este capítulo, a referência utilizada foi (Koryukin, 1994).

3.1 Caso cocomutativo

Se H é uma biálgebra, então, para cada $n \in \mathbb{N}$, temos uma ação do grupo S_n em V_n. Se além disso, H é cocomutativa, $V_1, \cdots, V_n$ são H-módulos e $\sigma \in S_n$, então

$$\begin{aligned} \tau(\sigma) \,:\, V_1 \otimes \cdots \otimes V_n &\to V_{\sigma(1)} \otimes \cdots \otimes V_{\sigma(n)} \\ x_1 \otimes \cdots \otimes x_n &\mapsto x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)} \end{aligned}$$

é um morfismo de H-módulos. Dessa forma, se $\phi_i \,:\, V_i \to U_i$ forem aplicações lineares (onde U_i e V_i são H-módulos), então $(\phi_1 \otimes \cdots \otimes \phi_n)((V_1 \otimes \cdots \otimes V_n)^H) = 0$ implica que para todo $\sigma \in S_n$, $(\phi_{\sigma(1)} \otimes \cdots \otimes \phi_{\sigma(n)})((V_{\sigma(1)} \otimes \cdots \otimes V_{\sigma(n)})^H) = 0$.

Sendo assim, se V possuir dimensão finita n, então podemos considerar a aplicação linear

$$s_n := \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\tau(\sigma) \,:\, V^{\otimes n} \to V^{\otimes n}$$

cuja imagem possui dimensão 1. Como H é cocomutativa, $\operatorname{im}(s_n)$ é um H-submódulo de $V^{\otimes n}$ (de dimensão 1).

Perceba que se H for uma álgebra de Hopf de dimensão finita, então $G(H^*)$ é finito. De fato, tal conjunto é constituido por elementos group-like de H^*, que é um conjunto linearmente independente. Mas como H^* possui dimensão finita, $G(H^*)$ é um grupo finito, e, em particular, todos os seus elementos possuem ordem finita.

Com essas observações, temos o seguinte lema.

Lema 3.1.1. *Seja H uma álgebra de Hopf cocomutativa de dimensão finita e V um H-módulo de dimensão finita. Então o suporte de $T(V)^H$ é igual a V.*

Demonstração: É claro que se $V = 0$, então isso é válido. Vamos supor então que $V \neq 0$, e seja $n = \dim V$. Assim, $U = \mathrm{im}(s_n)$ é um H-submódulo de $V^{\otimes n}$ unidimensional. Pela Proposição 2.3.5, existe $\alpha \in G(H^*)$ tal que $U = I_\alpha(U)$. Pelos comentários anteriores, segue que α possui ordem finita s. Segue do Lema 2.3.23, que $s(W) = V$. □

Assim, temos também o caso particular de quando a álgebra dos invariantes é finitamente gerada

Teorema 3.1.2. *Seja H uma álgebra de Hopf cocomutativa de dimensão finita e V um H-módulo de dimensão finita. Assim, os seguintes itens são equivalentes.*

1. *$T(V)^H$ é finitamente gerada.*
2. *V é a soma direta de submódulos isomorfos de dimensão* 1.

Demonstração: Se $T(V)^H$ for finitamente gerada, então seu suporte é um H-submódulo de V constituído de todos os elementos semi-invariantes de mesmo peso. Assim, se tivermos uma base de V, então, o subespaço gerado por cada elemento da base é um submódulo (pois V é o suporte), de modo que V seja soma direta de submódulos unidimensionais isomorfos.

Reciprocamente, assuma que V seja a soma direta de submódulos isomorfos unidimensionais. Então, como todo elemento de $G(H^*)$ possui ordem finita, e V é a soma direta de submódulos isomorfos, então todo elemento de V é semi-invariante de mesmo peso (faz sentido falar disso, pois todo elemento de $G(H^*)$ possui ordem finita), e isso segue do Teorema 2.3.25. □

3.2 Módulos redutivos

Definição 3.2.1. Seja M um H-módulo. Dizemos que M é um *H-módulo redutivo* se para todo $m \in M$, existe $h \in H$ tal que $h \cdot m \in M^H$ e $\varepsilon(h) \neq 0$ (ou equivalentemente, se $\varepsilon(\mathrm{Ann}_H\, x) \neq 0$, para todo $x \in \frac{M}{M^H}$).

Sejam M e N dois H-módulos e $\pi : M \to N$ um morfismo de H-módulos. É claro que elementos invariantes são preservados, isto é, que $\pi(M^H) \subseteq N^H$. Se M for um módulo redutível e π for um epimorfismo, então vale a outra inclusão, como iremos ver adiante. Vamos então olhar para um exemplo

Exemplo 3.2.2. *Seja $H = \Bbbk C_n$, a álgebra de grupo, C_n o grupo cíclico, e seja $V = \Bbbk^n$, com base $B = \{e_1, \dots, e_n\}$. Assim, V é um $\Bbbk G$-módulo em que $g(e_i) = e_{i+1(\mod n)}$. Assim, é fácil perceber que o elemento $h = 1 + g + \cdots + g^{n-1}$ é tal que $h \cdot e_i = e_i$, para todo $i = 1, \dots, n$. Perceba que esse elemento é um integral (à direita) de H e que $\varepsilon(h) = n$. Nesse caso, esse elemento é um integral e seu ε será não nulo se e somente característica de $\Bbbk$ não dividir $n = |G|$.*

Com isso, temos o seguinte resultado.

Proposição 3.2.3. *Seja H uma álgebra de Hopf. Então, todo H-módulo é redutivo se e somente se H for semissimples*

Demonstração: Seja $h \in H$ um integral à esquerda com $\varepsilon(h) \neq 0$. Então, para cada $m \in M$, dado $h' \in H$, temos

$$h' \cdot (h \cdot m) = (h'h) \cdot m = (\varepsilon(h')h) \cdot m = \varepsilon(h')h \cdot m.$$

Assim $h \cdot m \in M^H$.

Por outro lado, se todo H-módulo for redutível, então, H como módulo regular é redutível. Assim, existe $h \in H$, $\varepsilon(h) \neq 0$ tal que $h \cdot 1 \in M^H$. Isso quer dizer que, para todo $h' \in H$, temos

$$hh' = (h \cdot 1) \cdot h' = \varepsilon(h')h,$$

ou seja h é um integral à direita tal que $\varepsilon(h) \neq 0$. Logo H é semissimples. □

Assim, temos o seguinte lema

Lema 3.2.4. *Sejam M, N H-módulos, em que M é redutivo e $\pi : M \to N$ um epimorfismo. Então, vale que $\pi(M^H) = N^H$.*

Demonstração: Como dito na introdução desta seção, é sempre válido que $\pi(M^H) \subseteq N^H$, bastando apenas que π seja morfismo de H-módulos.

Seja agora $y \in N^H$. Como $y \in N$, existe $x \in M$ tal que $\pi(x) = y$ (dado que π é um epimorfismo). Como M é redutivo, podemos tomar $h \in H$ tal que $\varepsilon(h) = 1$ e $h \cdot x \in M^H$. Assim, temos que

$$y = \varepsilon(h)y = h \cdot y = h \cdot \pi(x) = \pi(h \cdot x) \in \pi(M^H).$$

□

Módulos redutivos também possuem uma certa relação com finitude.

Lema 3.2.5. *Seja M um módulo redutivo, então para todo subespaço W de $\frac{M}{M^H}$ de dimensão finita, vale que $\varepsilon(\mathrm{Ann}_H W) \neq 0$.*

Demonstração: Suponha inicialmente que $\dim W \leq 1$. Assim, temos que $W = \mathrm{span}\{\bar{m}\}$, com $m \in M$. Assim, como M é redutivo, temos que existe $h \in H$ tal que $\varepsilon(h) \neq 0$ e $h \cdot m \in \frac{M}{M^H}$, ou seja, $h \in \mathrm{Ann}_H W$ e $\varepsilon(h) \neq 0$.

Suponha que essa afirmação seja falsa, então, podemos tomar W de dimensão minimal que não satisfaz essa propriedade. Sejam então W_1 e W_2 subespaços próprios de W tais que $W = W_1 + W_2$. Assim, como W possui dimensão minimal, segue que existe $h_1 \in H$ tal que $h_1 \cdot W_1 = 0$ tal que $\varepsilon(h_1) \neq 0$.

Assim, vale que $\dim h_1 \cdot W_2 \leq \dim W_2 < \dim W$. Logo, existe $h_2 \in H$ tal que $\varepsilon(h_2) \neq 0$ e $(h_2h_1) \cdot W_2 = h_2 \cdot (h_1 \cdot W_2) = 0$. Temos, portanto que $\varepsilon(h_2h_1) \neq 0$ e

$$(h_2h_1) \cdot W = (h_2h_1) \cdot W_1 + (h_2h_1) \cdot W_2 = h_2 \cdot (h_1 \cdot W_1) + 0 = 0,$$

contradição. □

3.3 Ação dos grupos simétricos na álgebra dos invariantes

Quando H for álgebra cocomutativa, os grupos simétricos agem nas componentes homogêneas respectivas. Dessa forma, temos uma certa condição de finitude para a álgebra de invariantes que será feita através dessas ações.

Definição 3.3.1. Seja $R = T(V)$ e H uma álgebra de Hopf cocomutativa que age em R. Dessa forma, para cada $n \in \mathbb{N}$, o grupo S_n age em R_n. Se I (resp. A) é um ideal (subálgebra) homogêneo(a), dizemos que I (A) é um *S-ideal (S-subálgebra)*, se for fechada pela ação dos grupos simétricos.

Se D é uma S-subálgebra, e Y é um subconjunto de D, denotamos por $S_A(Y)$ a S-subálgebra gerada por Y e por $\mathrm{Sid}_D(Y)$ o S-ideal de D gerado por Y (perceba que a definição de $S_A(Y)$ independe da escolha de D).

Vamos precisar dos seguintes resultados.

Proposição 3.3.2. *Se V é um espaço de dimensão finita, então os S-ideais de $T(V)$ satisfazem a condição de cadeia ascendente.*

Demonstração: Seja $X = \{x_1, \dots, x_n\}$ uma base de V. Suponha por absurdo que $I_1, I_2, \dots$ uma cadeia ascendente de S-ideais de $T(V)$ que não se estabiliza. Seja $\alpha_{m+1} \in I_{m+1} \setminus I_m$ um elemento homogêneo com monômio líder e_{m+1} minimal (na ordem lexicográfica dos monômios). Podemos tomar elementos homogêneos, pois os ideais são homogêneos, de modo que as componentes homogêneas dos elementos pertençam ao ideal. Por simplicidade de notação, iremos considerar $I_0 = 0$ (e eventualmente deslocar a sequência caso $I_1 = 0$).

Temos portanto uma sequência $e_1, e_2, \dots$ de monômios que podem ser vistos como palavras em um conjunto finito de letras (base de V). Logo, pelo Corolário 1.4.6, existem i, j naturais, $i < j$ tal que e_i é uma subsequência de e_j. Isso quer dizer que podemos escrever

$$e_j = y_1 \cdots y_m, e_i = y_{r_1} \cdots y_{r_s},$$

em que $y_i \in X$, $s \leq m$ e $1 \leq r_1 < r_2 < \cdots < r_s \leq m$.

Seja $\sigma \in S_m$, a permutação que faz $\sigma(l) = r_l$ para $l = 1, \dots, s$ e para $l > s$, defina indutivamente $\sigma(l) = \min(\{1, \dots, m\} \setminus \{\sigma(1), \dots, \sigma(l-1)\})$, e seja $\tau = \sigma^{-1}$. Podemos supor, sem perda de generalidade, que o coeficiente de e_i (respectivamente e_j) em α_i (resp. α_j) é 1, e escreva $\alpha_i = e_i + \sum \beta_e e$, em que e são os outros monômios que aparecem em α_i.

Seja $h = y_{\sigma(s+1)} \cdots y_{\sigma(m)}$. Dessa forma, temos que

$$(\alpha_i h) \cdot \tau = (e_i h) \cdot \tau + \sum \beta_e (eh) \cdot \tau = y_1 \cdots y_m + \sum \beta_e (eh) \cdot \tau = e_j + \sum \beta_e (eh) \cdot \tau.$$

Assim, temos que $\sum \beta_e (eh) \cdot \tau = (\alpha_i h) \cdot \tau - e_j \in I_j \setminus I_{j-1}$. É claro que esse elemento é homogêneo. Vejamos que o monômio líder desse elemento é estritamente menor do que

α_j (chegando em uma contradição).

Seja $e < e_i$. Sabemos que $e_j = (e_i h) \cdot \tau$. Vejamos que $(eh) \cdot \tau < (e_i h) \cdot \tau = e_j$. Como nas posições diferentes de $r_1, \dots, r_s$ eles possuem a mesma letra, basta verificar nessas posições, e isso vem do fato de que $e < e_i$. Mostramos então que $(e_i h) \cdot \tau = e_j$ é o monômio líder. □

Proposição 3.3.3. *Seja D uma S-subálgebra e $f_1, \dots, f_m$ elementos homogêneos de D tais que $F_1(D) = \mathrm{Sid}_D(f_1, \dots, f_m)$. Então $D = S_A(f_1, \dots, f_m)$.*

Demonstração: Seja x um elemento homogêneo de D de grau no mínimo 1. Então,

$$x = \sum_{i=1}^{n} (f_i h_i) \cdot \tau_i,$$

em que $h_i \in \Bbbk$ ou é um elemento homogêneo de D. Além disso, temos que $\deg x = \deg f_i + \deg h_i$. Vejamos por indução no grau de x que $x \in S_A(f_1, \dots, f_m)$. É claro que todos os elementos de grau 0 estão em uma subálgebra. Por hipótese, $\deg(f_i) > 0$, para todo i (pois $F_1(D) = \mathrm{Sid}_D(f_1, \dots, f_m)$), dessa forma, $\deg h_i < \deg x$, e, por indução, temos que $h_i \in S_A(f_1, \dots, f_m)$. Portanto, $x \in S_A(f_1, \dots, f_m)$, concluindo o resultado. □

Proposição 3.3.4. *Sejam D uma S-álgebra e $\rho = \rho_0 \oplus \rho_1 \oplus \dots$ um ideal à direita de D. Então, o submódulo $P_n(\mathrm{Sid}_D(\rho))$ do $\Bbbk[S_n]$-módulo $V^{\otimes n}$ é gerado por elementos de ρ_n*

Demonstração: Perceba que

$$\mathrm{Sid}_D(\rho) = \mathrm{span}\left\{ \left(\left(\left(\left((v \otimes w_1) \cdot \sigma_1 \right) \otimes w_2 \right) \cdot \sigma_2 \right) \otimes \dots \otimes w_t \right) \cdot \sigma_t \ : \ v \in \rho_m, w_i \in D_{l_i}, \sigma_i \in S_{m + \sum_{j=1}^{i} l_j} \right\}.$$

Vejamos por indução que os elementos do conjunto gerador são da forma $\{v \cdot \sigma \ : \ v \in \rho_m, \sigma \in S_m\}$. Se $t = 0$, o resultado é claro e se $t = 1$, segue do fato de que ρ é um ideal à direita. Sejam $v \in \rho_m, w \in D_l, \sigma \in S_m, \tau \in S_{m+l}$. Considere $\psi \in S_{m+l}$ definida por

$$\psi(j) = \begin{cases} \sigma(j) & , j \leq m \\ j & , j > m. \end{cases}$$

Assim é claro que $\big((v \cdot \sigma) \otimes w\big) \cdot \tau = (v \otimes w) \cdot (\psi\tau)$. Portanto $P_n(\mathrm{Sid}_D(\rho)) = \{v \cdot \sigma \ : \ v \in \rho_n, \sigma \in S_n\} = \rho_n \cdot S_n$. □

Proposição 3.3.5. *Seja H uma biálgebra cocomutativa, e seja V um H-módulo de dimensão finita tal que $T(V)$ seja redutivo. Se $W = W_1 \oplus W_2 \oplus \dots$ é um espaço homogêneo de dimensão finita formada por elementos invariantes, então*

$$R^H \cap \mathrm{Sid}_R(W) = \mathrm{Sid}_{R^H}(W)$$

Demonstração: Sejam $A = R^H \cap \mathrm{Sid}_R(W)$ e $B = \mathrm{Sid}_{R^H}(W)$. Como H é cocomutativa, os invariantes são uma S-álgebra, de modo que a notação de B faça sentido. É claro que $B \subseteq A$.

Como A é interseção de subespaços homogêneos, A é homogêneo, de modo que basta mostrar que $P_n(A) \subseteq B$, para todo $n \geq 1$.

Seja $\rho = \rho_1 \oplus \rho_2 \oplus \dots$, o ideal à direita gerado por W. Temos

$$\rho_n \subseteq \sum_{i=1}^{n-1} W_i \otimes V^{\otimes(n-i)},$$

e, portanto ρ_n possui dimensão finita. Seja $U \subseteq R$ um subespaço de dimensão finita tal que $\rho_n \subseteq WU$. Como U é um subespaço de dimensão finita de R que é redutivo, pelo Lema 3.2.5, existe $h \in H$ tal que $\varepsilon(h) = 1$ e $h \cdot U \subseteq R^H$. Dessa forma, $h \cdot \rho_n \subseteq h \cdot (WU) \subseteq WR^H \Rightarrow h \cdot \rho_n \subseteq P_n(WR^H)$, pois a ação de H é homogênea. Dessa forma, pela Proposição 3.3.4 temos

$$\begin{aligned} P_n(R^H \cap \mathrm{Sid}_R(W)) &\subseteq R^H_n \cap P_n(\mathrm{Sid}_R(W)) = R^H_n \cap \rho_n \cdot \Bbbk[S_n] = h \cdot (R^H_n \cap \rho_n \cdot \Bbbk[S_n]) \\ &\subseteq h \cdot (\rho_n \cdot \Bbbk[S_n]) = (h \cdot \rho_n) \cdot \Bbbk[S_n] \subseteq P_n(WR^H) \cdot \Bbbk[S_n] \subseteq \mathrm{Sid}_{R^H}(W). \end{aligned}$$

□

Temos então, o resultado principal dessa seção.

Teorema 3.3.6. *Seja H uma biálgebra cocomutativa e seja V um H-módulo de dimensão finita, tal que $T(V)$ seja redutivo. Então existe X um conjunto finito de elementos invariantes de $T(V)$ como S-subálgebra.*

Demonstração: Através da Proposição 3.3.2, conseguimos achar um subespaço homogêneo W de $F_1(R^H)$ de dimensão finita tal que $\mathrm{Sid}_R(F_1(R^H)) \subseteq \mathrm{Sid}_R(W)$. Como $\mathrm{Sid}_R(W) \subseteq F_1(R)$, segue que $R^H \cap \mathrm{Sid}_R(W) \subseteq F_1(R^H)$. Por outro lado, é claro que $F_1(R^H) \subseteq R^H$ e $F_1(R^H) \subseteq \mathrm{Sid}_R(F_1(R^H)) \subseteq \mathrm{Sid}_R(W)$, de modo que $F_1(R^H) \subseteq R^H \cap \mathrm{Sid}_R(W)$. Assim, pela Proposição 3.3.5, temos que $F_1(R^H) = R^H \cap \mathrm{Sid}_R(W) = \mathrm{Sid}_{R^H}(W)$. Logo, da Proposição 3.3.3, segue que $R = S_A(W)$. Dessa forma, qualquer base homogênea de W será finita, composta de elementos invariantes e gerará $T(V)^H$ como S-subálgebra. □

Capítulo 4

Caso comutativo

Podemos considerar a ação em álgebras livres comutativas. Esse é o caso clássico e a demonstração de que a subálgebra de invariantes é finitamente gerada será feita de duas maneiras diferentes. Além disso, também será visto em quais casos essa subálgebra é livre. Ao longo desse capítulo G será um grupo finito que agirá por automorfismos em $\Bbbk$-álgebras comutativas A (em outras palavras, existe um homomorfismo $\rho : G \to \mathrm{Aut}(A)$), e dados $g \in G$ e $a \in A$, denotaremos por $g \cdot a$ a ação de g em a, i.e. $g \cdot a := \rho(g)(a)$. Iremos assumir que $\mathrm{char}(\Bbbk) = 0$. Para este capítulo, as principais referências são (Neusel, 2007) e (Springer, 1977).

4.1 A álgebra de invariantes comutativos é finitamente gerada

Definição 4.1.1. Se A for uma $\Bbbk$-álgebra comutativa, e G agir por automorfismos em A, então, *os invariantes*, denotados por A^G, são definidos como sendo os elementos de A que são fixos sobre a ação de G.

Temos ainda mais, mas primeiramente, vamos relembrar o conceito de extensão integral.

Definição 4.1.2. Sejam A, B aneis comutativos. Dizemos que B é uma *extensão* de A se A for um subanel de B. Dado $b \in B$, dizemos que b é *integral* sobre A se existe $p(x) \in A[x]$ polinômio mônico tal que $p(b) = 0$. Dizemos que a extensão é *integral* se todo elemento de B for integral sobre A.

Assim, o seguinte lema é válido.

Lema 4.1.3. *A álgebra A é integral sobre A^G.*

Demonstração: Seja $a \in A$. Como G é finito, podemos considerar o polinômio $p(x) = \prod_{g \in G}(x - g \cdot a)$ que é mônico, e seus coeficientes são polinômios simétricos em $\{g \cdot a : g \in G\}$ e , portanto, pertencem a A^G. Logo A é integral sobre A^G. □

O objetivo é achar alguma condição para que A^G seja finitamente gerada. Para isso, vamos precisar de outro lema.

Lema 4.1.4. *Sejam A, B, C anéis comutativos tais que A é subanel de B e B é subanel de C. Se B for uma A-álgebra finitamente gerada e C for uma B-álgebra finitamente gerada, então C é uma A-álgebra finitamente gerada (onde as estruturas de álgebra de um anel sobre um subanel são as naturais).*

Demonstração: Sejam $b_1, \dots, b_n \in B$ tais que $B = A[b_1, \dots, b_n]$ e $c_1, \dots, c_m \in C$ tais que $C = B[c_1, \dots, c_m]$. Vejamos que $C = A[b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m]$.

Seja $c \in C = B[c_1, \dots, c_m]$. Então, existe $p(x_1, \dots, x_m) = \sum_I \beta_I x^I \in B[x_1, \dots, x_m]$ tal que $c = p(c_1, \dots, c_m) = \sum_J \beta_J c^J$, onde $c^J = c_1^{j_1} \cdots c_m^{j_m}$, se $J = (j_1, \dots, j_m)$ e $\beta_J \in B = A[b_1, \dots, b_m]$.

Logo, para cada J, existe $q_J(y_1, \dots, y_n) \in A[y_1, \dots, y_n]$ tal que $\beta_J = q_J(b_1, \dots, b_m)$. Assim, podemos escrever $q_J(y_1, \dots, y_n) = \sum_I \alpha_{I,J} y^I$ (onde $y^I = y_1^{i_1} \cdots y_n^{i_n}$, se $I = (i_1, \dots, i_n)$ e $\alpha_{I,J} \in A$). Portanto, podemos concluir que

$$c = \sum_J \beta_J c^J = \sum_{I,J} \alpha_{I,J} b^I c^J.$$

Perceba que para todos I, J, temos que $b^I c^J$ é um produto de b_i e c_j, de modo que $c \in A[b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m]$. Logo vale a igualdade e, portanto, C é uma A-álgebra finitamente gerada. □

Com esses lemas, temos o seguinte teorema.

Teorema 4.1.5. *Se A é uma $\Bbbk$-álgebra (comutativa) finitamente gerada em que G age, então A^G é finitamente gerada. Em particular, se V é um $\Bbbk$-espaço de dimensão finita em que G age por automorfismos lineares, então, em $\Bbbk[V]$ com a ação induzida, vale que $\Bbbk[V]^G$ é finitamente gerada.*

Demonstração: Seja $a_1, \dots, a_n \in A$ tais que $A = \Bbbk[a_1, \dots, a_n]$. Como A é integral sobre A^G, para cada $i = 1, \dots, n$, seja $p_i(x) = x^{\alpha_i} + a_{i,\alpha_i - 1} x^{\alpha_i - 1} + \cdots + a_{i,1} x + a_{i,0} \in A^G[x]$ mônico tal que $p_i(a_i) = 0$. Tome $B = \Bbbk[a_{i,l} : 1 \leq i \leq n; 1 \leq l \leq \alpha_i - 1] \subseteq A^G$.

Como $\Bbbk$ é um corpo, segue que $\Bbbk$ é noetheriano, e como B é uma $\Bbbk$-álgebra finitamente gerada, segue que B é um anel noetheriano.

Além disso, A é um B-módulo finitamente gerado por $X = \{a^I : 0 \leq i_j < \alpha_j\}$, onde estamos denotando a^I por $a_1^{i_1} \cdots a_n^{i_n}$, se $I = (i_1, \dots, i_n)$. De fato, dado $a \in A$, existe um polinômio $p(x_1, \dots, x_n) = \sum_I \alpha_I x^I \in \Bbbk[x_1, \dots, x_n]$ tal que $a = p(a_1, \dots, a_n) = \sum_I \alpha_I a^I$. Perceba que, dado I, se algum $i_j \geq \alpha_j$, então esse termo pode ser escrito combinações linares sobre B de potências menores, de modo que a está nesse submódulo gerado por X.

Dessa forma, temos que A é um B-módulo noetheriano (módulo finitamente gerado sobre um anel noetheriano), e, portanto, A^G que é um B-submódulo também será finitamente gerado. Em particular, A^G é uma B-álgebra finitamente gerada. Como B é uma $\Bbbk$-álgebra

finitamente gerada, segue que A^G é uma $\Bbbk$-álgebra finitamente gerada, por causa do Lema 4.1.4.

Finalmente, note que V é um $\Bbbk$-espaço de dimensão finita, então $\Bbbk[V]$ é uma álgebra finitamente gerada (por uma base de V). □

4.2 Teorema de Chevalley-Shephard-Todd

Na seção anterior vimos que a álgebra de invariantes é sempre finitamente gerada, no caso em que o grupo age na álgebra livre comutativa. Isso é essencialmente o oposto do caso em que a ação ocorre na álgebra livre não comutativa. Então, iremos novamente ver o contraste com o caso não comutativo, em que a álgebra de invariantes sempre é livre, o que não ocorre no caso comutativo. Iremos precisar do seguinte lema. As principais referências para esta seção são (Neusel, 2007) e (Springer, 1977).

Lema 4.2.1. *Seja π_G, a seguinte aplicação*

$$\begin{aligned} \pi_G : \Bbbk[V] &\to \Bbbk[V] \\ f &\mapsto \frac{1}{|G|}\sum_{g\in G} g\cdot f. \end{aligned}$$

Então π_G é uma projeção em $\Bbbk[V]^G$ e é um morfismo de $\Bbbk[V]^G$-módulos.

Demonstração: É claro que π_G é uma transformação linear. Sejam $f \in \Bbbk[V]^G$ e $h \in \Bbbk[V]$. Então, para todo $g \in G$, $g \cdot f = f$, de modo que

$$\pi_G(f) = \frac{1}{|G|}\sum_{g\in G} g\cdot f = \frac{1}{|G|}\sum_{g\in G} f = \frac{|G|}{|G|}f = f.$$

Dessa forma, π_G é a identidade em $\Bbbk[V]^G$. Dado $g_1 \in G$, temos

$$\begin{aligned} g_1\cdot\pi_G(h) &= g_1\cdot\left(\frac{1}{|G|}\sum_{g\in G} g\cdot h\right) = \frac{1}{|G|}\sum_{g\in G} g_1\cdot(g\cdot h) \\ &= \frac{1}{|G|}\sum_{g\in G}(g_1 g)\cdot h = \frac{1}{|G|}\sum_{g\in G} g\cdot h = \pi_G(h). \end{aligned}$$

Assim, a imagem de π_G está contida em $\Bbbk[V]^G$, de modo a ser uma projeção. Por fim

$$\begin{aligned} \pi_G(fh) &= \frac{1}{|G|}\sum_{g\in G} g\cdot(fh) = \frac{1}{|G|}\sum_{g\in G}(g\cdot f)(g\cdot h) \\ &= \frac{1}{|G|}\sum_{g\in G} f(g\cdot h) = f\left(\frac{1}{|G|}\sum_{g\in G} g\cdot h\right) = f\pi_G(h). \end{aligned}$$

□

Definição 4.2.2. Seja V um espaço vetorial de dimensão finita. Uma transformação linear R é dita ser uma *pseudoreflexão* se

(i) $R \neq \mathrm{id}$.

(ii) Existe $m \in \mathbb{N}$ tal que $R^m = \mathrm{id}$.

(iii) Se W é o auto-espaço relacionado a 1 então a codimensão de W em V é 1.

Denotamos o subespaço W como V^R.

Dessa forma, se $R : V \to V$ for uma pseudoreflexão, então a imagem de $\mathrm{id} - R$ possui dimensão 1. Seja v_R um vetor não nulo que está nessa imagem. Assim, para todo $v \in V$, existe um escalar $\Delta_R(v) \in \Bbbk$ tal que $(\mathrm{id} - R)(v) = \Delta_R(v)v_R$. Podemos extender R para $\Bbbk[V]$, de forma que valha $R(x) = x - \Delta_R(x)v_R$, e que Δ_R seja uma derivação torcida.

Proposição 4.2.3. *Seja $R : V \to V$ uma pseudoreflexão e a considere como a sua extensão em $\Bbbk[V]$ como morfismo de álgebras. Seja v_R um vetor que gera* $\mathrm{im}(I - R)$*. Então, existe uma aplicação $\Delta_R : \Bbbk[V] \to \Bbbk[V]$, tal que $f - R(f) = \Delta_R(f)v_R$, para todo $f \in \Bbbk[V]$. Além disso, se f é um elemento homogêneo de grau m, então $\Delta_R(f)$ é um elemento homogêneo de grau $m - 1$ (de modo que se f é um elemento de grau m não necessariamente homogêneo, então $\Delta_R(f)$ é um elemento não necessariamente homogêneo de grau $m - 1$), e Δ_R é uma derivação torcida em $\Bbbk[V]$.*

Demonstração: Para encontrar tal aplicação, seja $f \in \Bbbk[V]$ um monômio. Vamos mostrar por indução no grau de f que $f - R(f)$ é múltiplo de v_R em $\Bbbk[V]$, de modo que todo elemento de $\Bbbk[V]$ também seja, fazendo com que exista a aplicação Δ_R. O caso do monômio de grau 1 segue do fato de que v_R gera $\mathrm{im}(\mathrm{id} - R)$.

Para o passo indutivo, seja $f = x_{i_1} \cdots x_{i_n} x_{i_{n+1}}$ um monômio. Pela hipótese de indução, se $h = x_{i_1} \cdots x_{i_n}$, então $h - R(h)$ é múltiplo de v_R. Assim, temos

$$\begin{aligned} f - R(f) &= hx_{i_{n+1}} - R(h)R(x_{i_{n+1}}) = hx_{i_{n+1}} - R(h)x_{i_{n+1}} + R(h)x_{i_{n+1}} - R(h)R(x_{i_{n+1}}) \\ &= (h - R(h))x_{i_{n+1}} + R(h)(x_{i_{n+1}} - R(x_{i_{n+1}})). \end{aligned}$$

Assim, $f - R(f)$ é múltiplo de v_R, e, portanto existe Δ_R e $\Delta_R(f)$ possui grau $m - 1$.

Para mostrar que Δ_R é uma derivação torcida, considere $f, h \in \Bbbk[V]$, e temos

$$\begin{aligned} fh - \Delta_R(fh)v_R = R(fh) = R(f)R(h) = R(f)(h - \Delta_R(h)hv_R) = R(f)h - R(f)\Delta_R(h)v_R \\ = fh - (\Delta_R(f)h + R(f)\Delta_R(h))v_R \Rightarrow \Delta_R(fh) = \Delta_R(f)h + R(f)\Delta_R(h). \end{aligned}$$

□

Definição 4.2.4. Seja G um grupo que age em um espaço de dimensão n. Dizemos que essa ação é de *pseudoreflexão* se $\rho(G)$ for gerada (como grupo) por pseudoreflexões.

Lema 4.2.5. *Seja $\rho : G \to \mathrm{GL}(n, \Bbbk)$ uma ação fiel. Então, $\Delta_R : \Bbbk[V] \to \Bbbk[V]$ é um morfismo de $\Bbbk[V]^G$-módulos.*

Demonstração: Dados $f \in \Bbbk[V]^G$ e $h \in \Bbbk[V]$, e R uma pseudoreflexão em $\rho(G)$, temos

$$\Delta_R(fh) = \Delta_R(f)h + R(f)\Delta_R(h) = R(f)\Delta_R(h) = f\Delta_R(h),$$

pois se f é invariante, então, $f = R(f) = f + \Delta_R(f)v_R \Rightarrow \Delta_R(f) = 0$. □

A partir de agora, iremos considerar I o ideal homogêneo de $\Bbbk[V]$ gerado pelos elementos homogêneos de $\Bbbk[V]^G$ de grau positivo. Temos então alguns lemas.

Lema 4.2.6. *O ideal I é G-invariante (isto é, para todo $g \in G$, $g \cdot I \subseteq I$).*

Demonstração: Para tal demonstração, seja $g \in G$, $f \in \Bbbk[V]^G$ homogêneo de grau positivo e $h \in \Bbbk[V]$. Então, $g \cdot (fh) = (g \cdot f)(g \cdot h) = f(g \cdot h) \in I$. Como I é composto por soma de elementos da forma fh, com f como anteriormente, segue que $g \cdot I \subseteq I$. □

Lema 4.2.7. *Seja $\mathfrak{B} = \{e_\alpha\}_{\alpha \in A}$ um conjunto de elementos homogêneos de $\Bbbk[V]$ tais que $\{e_\alpha + I\}_{\alpha \in A}$ gera $\dfrac{\Bbbk[V]}{I}$ como $\Bbbk$-espaço. Então o $\Bbbk[V]^G$-módulo gerado por $\mathfrak{B}$ é $\Bbbk[V]$.*

Demonstração: Seja M o $\Bbbk[V]^G$-módulo de $\Bbbk[V]$ gerado por $\mathfrak{B}$. Como $\mathfrak{B}$ é composto por elementos homogêneos, segue que M é um subespaço graduado. Mostraremos por indução que $M_d = \Bbbk[V]_d$, para todo $d \geq 0$. Como $\mathfrak{B} + I$ gera o quociente como $\Bbbk$-espaço, existem $c_\alpha \in \Bbbk$ quase todos nulos tais que

$$1 - \sum_\alpha c_\alpha e_\alpha \in I.$$

Mas I é gerado pelos elementos homogêneos de grau positivo, e como cada e_α é homogêneo, para algum $\beta \in A$, $e_\beta \in \Bbbk$, de modo que $1 \in M_0 \Rightarrow M_0 = \Bbbk[V]_0$.

Suponha agora que o resultado seja válido para todos os inteiros menores que d, e provaremos para d. Para isso, seja $f \in \Bbbk[V]_d$, novamente, existem $c_\alpha \in \Bbbk$ quase todos nulos tais que $h = f - \sum_\alpha c_\alpha e_\alpha \in I$. Como I é um ideal gerado pelos elementos homogêneos de $\Bbbk[V]^G$ de grau positivo, I é um ideal homogêneo, toda componente homogênea de h está em I. Do fato de f ser homogênea, podemos supor sem perda de generalidade que h é homogênea. Assim, existem $f_1, \ldots, f_t \in \Bbbk[V]^G$ homogêneos de grau positivo e $r_1, \ldots, r_t \in \Bbbk[V]$ de modo que

$$f = \sum_\alpha c_\alpha e_\alpha + \sum_{i=1}^{t} f_i r_i.$$

Podemos supor sem perda de generalidade que cada r_i é homogêneo (se r_i não for homogêneo, é soma de elementos homogêneos, sendo assim, basta colocar mais parcelas para garantir que r_i é homogêneo). Como f_i tem grau positivo, o grau de r_i é menor do que o grau de f, para todo i, e, portanto, pela hipótese de indução $r_i \in M$. Assim, $f \in M$. □

Lema 4.2.8. *Suponha que G seja um grupo de pseudo-reflexão. Sejam $y_1, \ldots, y_m \in \Bbbk[V]$ elementos homogêneos e $x_1, \ldots, x_m \in \Bbbk[V]^G$ tais que $\sum_{i=1}^{m} x_i y_i = 0$. Se x_1 não estiver no $\Bbbk[V]^G$-módulo gerado por $\{x_2, \ldots, x_m\}$, então $y_1 \in I$.*

Demonstração: Será feito por indução no grau de y_1. Se $y_1 = 0$, então $y_1 \in I$. Se $y_1 \neq 0$ e tem grau 0, dividindo por y_1, encontramos $z_2, \dots, z_m \in \Bbbk[V]$, tais que

$$x_1 = \sum_{i=2}^{m} x_i z_i.$$

Pelo Lema 4.2.1, obtemos

$$x_1 = \pi_G(x_1) = \sum_{i=2}^{m} \pi_G(x_i z_i) = \sum_{i=2}^{m} x_i \pi_G(z_i).$$

Dessa forma, podemos concluir que x_1 está no $\Bbbk[V]^G$-módulo gerado por $\{x_2, \dots, x_m\}$, contradição.

Para o passo indutivo, pelo Lema 4.2.5, para cada $R \in G$ pseudo-reflexão, temos

$$0 = \sum_{i=1}^{m} \Delta_R(x_i y_i) = \sum_{i=1}^{m} x_i \Delta_R(y_i).$$

Como o grau de $\Delta_R(y_1)$ é menor do que y_1, pela hipótese de indução, $\Delta_R(y_1) \in I$, para todo $R \in G$ pseudo-reflexão. Assim, se R é pseudo-reflexão, então $y_1 - R(y_1) = \Delta_R(y_1) v_R \in I$, pois I é um ideal. Vejamos por indução que $y_1 - R_m(R_{m-1}(\dots(R_1(y_1))\dots)) \in I$, com R_i pseudo-reflexão, para todo i. Para $m = 1$, é o que foi mostrado anteriormente. Por hipótese de indução, $y_1 - R_m(R_{m-1}(\dots(R_1(y_1))\dots)) \in I$. Como I é G-invariante, então

$$R_{m+1}(y_1) - R_{m+1}(R_m(\dots(R_1(y_1))\dots))) = R_{m+1}(y_1 - R_m(R_{m-1}(\dots(R_1(y_1))\dots))) \in I.$$

Assim

$$y_1 - R_{m+1}(R_m(\dots(R_1(y_1))\dots))) = (y_1 - R_{m+1}(y_1)) + (R_{m+1}(y_1) - R_{m+1}(R_m(\dots(R_1(y_1))\dots)))) \in I.$$

Como G é um grupo de pseudo-reflexão, segue que $y_1 - g \cdot y_1 \in I$, para todo $g \in$G. Assim,

$$y_1 - \pi_G(y_1) = \frac{1}{|G|} \sum_{g \in G} (y_1 - g \cdot y_1) \in I.$$

Dessa forma, do fato do grau de y_1 ser positivo, $\pi_G(y_1) \in I$, de modo que $y_1 \in I$.

□

Lema 4.2.9. *Seja G um grupo de pseudo-reflexão e sejam $\mathfrak{B} \subseteq \Bbbk[V]$ formado por elementos homogêneos tal que $\mathfrak{B} + I$ é linearmente independente sobre $\Bbbk$. Então $\mathfrak{B}$ é linearmente independente sobre $\Bbbk[V]^G$.*

Demonstração: Sejam $x_1, \dots, x_m \in \Bbbk[V]^G$ e $y_1, \dots, y_m \in \mathfrak{B}$ tais que $\sum_{i=1}^{m} x_i y_i = 0$. Provaremos por indução em m que $x_i = 0$, para todo i. Se $m = 1$, o resultado segue do fato que $\Bbbk[V]$ é um domínio de integridade. Para o passo indutivo, observe que $y_1 + I \neq 0 + I$, e portanto $y_1 \notin I$ (pois $\{y_1 + I, \dots, y_m + I\}$ é linearmente independente sobre $\Bbbk$). Através do Lema 4.2.8,

tome $z_2, \dots, z_m \in \Bbbk[V]^G$ tais que

$$x_1 = \sum_{i=2}^{m} x_i z_i.$$

Portanto

$$0 = x_1 y_1 + \sum_{i=2}^{m} x_i y_i = \left(\sum_{i=2}^{m} x_i z_i \right) y_1 + \sum_{i=2}^{m} x_i y_i = \sum_{i=2}^{m} x_i (z_i y_1 + y_i). \tag{4.1}$$

Para cada $i = 2, \dots, m$, escreva $z_i = \alpha_i + w_i$, onde $\alpha_i \in \Bbbk$ e o termo de grau 0 de w_i é 0. Dessa forma, como I é um ideal homogêneo e $\Bbbk[V]^G$ é uma subálgebra homogênea, $w_i \in I$, para todo i, pois $z_i \in \Bbbk[V]^G$ e w_i é a soma das componentes homogêneas de grau positivo de z_i, de modo que $z_i + I = \alpha_i + I$. Se $\beta_2, \dots, \beta_m \in \Bbbk$ são tais que $\sum_{i=2}^{m} \beta_i (z_i y_1 + y_i + I) = 0 + I$, então

$$\begin{aligned} 0 + I &= \sum_{i=2}^{m} \beta_i (z_i y_1 + y_i) + I = \sum_{i=2}^{m} \beta_i (\alpha_i y_1 + y_i) + I \\ &= \left(\sum_{i=2}^{m} \alpha_i \beta_i \right) (y_1 + I) + \sum_{i=2}^{m} \beta_i (y_i + I). \end{aligned}$$

Assim $\beta_i = 0$, para todo $i = 2, \dots, m$, isto é, $\{z_2 y_1 + y_2 + I, \dots, z_m y_1 + y_m + I\}$ é linearmente independente sobre $\Bbbk$. Podemos então aplicar o passo indutivo e concluir que $x_2 = \cdots = x_m = 0$. □

Proposição 4.2.10. *Seja $\rho : G \to \mathrm{GL}(n, \Bbbk)$ uma ação de pseudoreflexão. Então $\Bbbk[V]$ é um módulo livre sobre $\Bbbk[V]^G$.*

Demonstração: Segue da Proposição 1.2.6 e dos Lemas 4.2.7 e 4.2.9. □

Proposição 4.2.11. *Suponha que G seja um grupo finito que aja em V um espaço vetorial. Se $\Bbbk[V]$ é um $\Bbbk[V]^G$-módulo livre, então $\Bbbk[V]^G$ é uma álgebra de polinômios.*

Esboço da demonstração: A ideia é mostrar que $\Bbbk[V]^G$ é um anel noetheriano, e com isso, considerar um conjunto minimal de elementos homogêneos $\{f_1, \dots, f_m\}$ gerador do ideal gerado pelos elementos positivos J. Daí, usando uma indução, consegue-se mostrar que $\Bbbk[V] = \Bbbk[f_1, \dots, f_m]$. Para concluir, precisariamos mostrar que os elementos desse conjunto são algebricamente independentes.

Suponha por absurdo que existe um polinômio $h(X_1, \dots, X_m) \in \Bbbk[X_1, \dots, X_m]$ tal que $h(f_1, \dots, f_m) = 0$. Então pega-se as derivadas parciais em relação a cada uma dessas m variáveis e considera-se o ideal gerado por elas, considerando um conjunto minimal gerador.

Considerando as derivadas parciais em relação a uma base de V, podemos usar a regra da cadeia para encontrar algumas relações entre esses elementos. Agora, usando o fato de que $\Bbbk[V]$ é um $\Bbbk[V]^G$-módulo livre e comparando componente homogênea, conseguimos mostrar que o conjunto $\{f_1, \dots, f_m\}$ pode ser diminuido. Contradição. □

Proposição 4.2.12. *Seja V um $\Bbbk$-espaço de dimensão finita e seja $G \leq \mathrm{GL}(V)$ um subgrupo finito. Suponha que $\Bbbk[V]^G$ seja uma álgebra de polinômios. Então G é um grupo de pseudo-reflexões.*

Esboço da demonstração: Aqui serão utilizadas as séries de Poincaré. Mostra-se que se A é uma subálgebra finitamente gerada, $A = \Bbbk[a_1, \dots, a_n]$, com $a_1, \dots, a_n$ elementos homogêneos algebricamente independentes, então a série de Poincaré será o produto dos inversos de polinômios da forma $1 - t^{d_i}$ em que d_i são unicamente determinados pela álgebra. Sendo assim, se G' for o subgrupo gerado pelas pseudo-reflexões, já sabemos que $\Bbbk[V]^{G'}$ é uma álgebra de polinômios. Sendo assim, ao comparar as duas séries de Poincaré, concluimos que vale a igualdade entre os elementos unicamente determinados pela série de Poincaré. Dessa forma $G' = G$, e G é um grupo de pseudoreflexões. □

Juntando as três proposições, obtemos o seguinte teorema.

Teorema 4.2.13 (Teorema de Chevalley-Shephard-Todd)**.** *Seja V um $\Bbbk$-espaço de dimensão finita e seja $G \leq \mathrm{GL}(V)$ um subgrupo finito. Então os seguintes itens são equivalentes.*

(i) *G é um grupo de pseudo-reflexões.*

(ii) *$\Bbbk[V]$ é um $\Bbbk[V]^G$-módulo livre.*

(iii) *$\Bbbk[V]^G$ é uma álgebra de polinômios.*

Demonstração: Segue das Proposições 4.2.10, 4.2.11 e 4.2.12. □

Conclusão

Ao longo desta dissertação estudamos os invariantes da ação de uma álgebra de Hopf em uma álgebra livre (comutativa ou não). Vimos que no caso não-comutativo, a subálgebra é sempre livre e quase nunca finitamente gerada. Em contraste, temos o caso em que grupos agem nas álgebras livres comutativas e temos que os invariantes são sempre finitamente gerados e quase nunca livres.

Conseguimos achar um conjunto finito gerador se incluirmos a ação dos grupos simétricos. O que pedimos sobre a álgebra de Hopf é que ela seja cocomutativa, para que assim, a ação dos grupos simétricos comute com a ação de H, e também pedimos que a álgebra livre seja um H-módulo redutivo.

Similarmente aos grupos simétricos, os grupos de tranças também agem nas componentes homogêneas da álgebra livre. Se a álgebra de Hopf for quase triangular, então a ação de H comuta com a ação dos grupos de tranças. Portanto, como estudos futuros, iremos tentar encontrar alguma relação entre o grupo de tranças, a ação de álgebras de Hopf quase triangulares e um conjunto finito de geradores.

Uma outra possibilidade de estudos futuros é olhar para a ação da álgebras de Hopf em álgebras relativamente livres e tentar compreender quando essas propriedades (finitamente gerada, livre) acontecem.

Referências

[Canesin 2020] Ricardo Felipe Rosada Canesin. *Representaçoes Modulares de Grupos Finitos*. https://repositorio.usp.br/directbitstream/47849975-202a-4629-b38d-51db0c71c180/3063775.pdf. 2020 (citado na pg. 65).

[Cohn 1971] P. M. Cohn. *Free rings and their relations*. Vol. No. 2. London Mathematical Society Monographs. Academic Press, London-New York, 1971, pp. xvi+346 (citado nas pgs. 23, 28).

[Dăscălescu *et al.* 2001] Sorin Dăscălescu, Constantin Năstăsescu e Şerban Raianu. *Hopf algebras*. Vol. 235. Monographs and Textbooks in Pure and Applied Mathematics. An introduction. Marcel Dekker, Inc., New York, 2001, pp. x+401. isbn: 0-8247-0481-9 (citado na pg. 5).

[Dicks e Formanek 1982/83] Warren Dicks e Edward Formanek. "Poincaré series and a problem of S. Montgomery". *Linear and Multilinear Algebra* 12.1 (1982/83), pp. 21–30. issn: 0308-1087,1563-5139. doi: 10.1080/03081088208817467. url: https://doi.org/10.1080/03081088208817467 (citado nas pgs. 60, 65).

[V. O. Ferreira *et al.* 2004] V. O. Ferreira, L. S. I. Murakami e A. Paques. "A Hopf-Galois correspondence for free algebras". *J. Algebra* 276.1 (2004), pp. 407–416. issn: 0021-8693,1090-266X. doi: 10.1016/S0021-8693(03)00502-7. url: https://doi.org/10.1016/S0021-8693(03)00502-7 (citado nas pgs. 43, 48).

[Vitor O Ferreira e L. S. Murakami 2020] Vitor O Ferreira e Lucia SI Murakami. *Introdução às Álgebras de Hopf*. Vol. 5. TEXTUNIVERSITÁRIOS. Livraria da Física, 2020, pp. viii+293. isbn: 9788578616465 (citado nas pgs. 3, 6, 9, 10, 12).

[Vitor O. Ferreira e L. S. I. Murakami 2007] Vitor O. Ferreira e Lucia S. I. Murakami. "Finitely generated invariants of Hopf algebras on free associative algebras". *Linear Algebra Appl.* 420.1 (2007), pp. 70–78. issn: 0024-3795,1873-1856. doi: 10.1016/j.laa.2006.06.026. url: https://doi.org/10.1016/j.laa.2006.06.026 (citado na pg. 76).

[Vitor O. Ferreira e L. S. I. Murakami 2014] Vitor O. Ferreira e Lucia S. I. Murakami. "Rationality of the Hilbert series of Hopf-invariants of free algebras". *Proc. Amer. Math. Soc.* 142.3 (2014), pp. 821–826. ISSN: 0002-9939,1088-6826. DOI: 10.1090/S0002-9939-2013-11830-7. URL: https://doi.org/10.1090/S0002-9939-2013-11830-7 (citado na pg. 60).

[Green 1962] J. A. Green. "The modular representation algebra of a finite group". *Illinois J. Math.* 6 (1962), pp. 607–619. ISSN: 0019-2082. URL: http://projecteuclid.org/euclid.ijm/1255632708 (citado nas pgs. 65, 66).

[Harčenko 1978] V. K. Harčenko. "Algebras of invariants of free algebras". *Algebra i Logika* 17.4 (1978), pp. 478–487, 491. ISSN: 0373-9252 (citado na pg. 50).

[Koryukin 1994] A. N. Koryukin. "On noncommutative invariants of bialgebras". *Algebra i Logika* 33.6 (1994), pp. 654–680, 716. ISSN: 0373-9252. DOI: 10.1007/BF00756350. URL: https://doi.org/10.1007/BF00756350 (citado nas pgs. 50, 65, 83).

[Lam 2001] T. Y. Lam. *A first course in noncommutative rings*. Second. Vol. 131. Graduate Texts in Mathematics. Springer-Verlag, New York, 2001, pp. xx+385. ISBN: 0-387-95183-0. DOI: 10.1007/978-1-4419-8616-0. URL: https://doi.org/10.1007/978-1-4419-8616-0 (citado nas pgs. 3, 13, 20).

[Masuoka e Yanai 2003] Akira Masuoka e Tadashi Yanai. "Hopf module duality applied to X-outer Galois theory". *J. Algebra* 265.1 (2003), pp. 229–246. ISSN: 0021-8693,1090-266X. DOI: 10.1016/S0021-8693(03)00130-3. URL: https://doi.org/10.1016/S0021-8693(03)00130-3 (citado nas pgs. 43, 46).

[S. Montgomery 1993] S. Montgomery. "Bi-invertible actions of Hopf algebras". *Israel J. Math.* 83.1-2 (1993), pp. 45–71. ISSN: 0021-2172,1565-8511. DOI: 10.1007/BF02764636. URL: https://doi.org/10.1007/BF02764636 (citado na pg. 46).

[S. Montgomery e Passman 1984] S. Montgomery e D. S. Passman. "Outer Galois theory of prime rings". *Rocky Mountain J. Math.* 14.2 (1984), pp. 305–318. ISSN: 0035-7596,1945-3795. DOI: 10.1216/RMJ-1984-14-2-305. URL: https://doi.org/10.1216/RMJ-1984-14-2-305 (citado na pg. 50).

[Susan Montgomery 1993] Susan Montgomery. *Hopf algebras and their actions on rings*. Vol. 82. CBMS Regional Conference Series in Mathematics. Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993, pp. xiv+238. ISBN: 0-8218-0738-2. DOI: 10.1090/cbms/082. URL: https://doi.org/10.1090/cbms/082 (citado na pg. 3).

[Nash-Williams 1967] C. St. J. A. Nash-Williams. "On well-quasi-ordering trees". In: *A Seminar on Graph Theory*. Holt, Rinehart e Winston, New York-Toronto, Ont.-London, 1967, pp. 79–82 (citado na pg. 39).

[Neusel 2007] Mara D. Neusel. *Invariant theory*. Vol. 36. Student Mathematical Library. American Mathematical Society, Providence, RI, 2007, pp. viii+314. ISBN: 978-0-8218-4132-7; 0-8218-4132-7. DOI: 10.1090/stml/036. URL: https://doi.org/10.1090/stml/036 (citado nas pgs. 89, 91).

[Passman 1987] D. S. Passman. "Computing the symmetric ring of quotients". *J. Algebra* 105.1 (1987), pp. 207–235. ISSN: 0021-8693. DOI: 10.1016/0021-8693(87)90187-6. URL: https://doi.org/10.1016/0021-8693(87)90187-6 (citado na pg. 32).

[Springer 1977] T. A. Springer. *Invariant theory*. Vol. Vol. 585. Lecture Notes in Mathematics. Springer-Verlag, Berlin-New York, 1977, pp. iv+112 (citado nas pgs. 89, 91).

Índice remissivo