ÁLGEBRAS DE LIE, ÁLGEBRAS DE HOPF E GRUPOS QUÂNTICOS

WALDECK SCHUTZER

Orientador: PROF. DR. PAULO AFONSO FARIA DA VEIGA

Dissertação apresentada ao Instituto de Ciências Matemáticas de São Carlos-USP, como parte dos requisitos para obtenção do título de "Mestre em Ciências - Área: Matemática".

USP - São Carlos

1996

Resumo

O objetivo deste trabalho é fornecer um resumo introdutório auto-consistente à Teoria dos Grupos Quânticos. Para realizar esta tarefa, as Álgebras de Lie e Álgebras de Hopf são estudadas num passo intermediário. Nossa discussão tem como meta final classificar as representações do análogo quântico da álgebra universal envolvente da álgebra de Lie $\mathfrak{sl}(2)$.

Abstract

This work aims at giving a self-contained and introductory review of the Theory of Quantum Groups. To accomplish this goal, Lie Algebras and Hopf Algebras are also discussed at an intermediate step. We focus at providing a study leading to the classification for the representations of the quantum analogue of the universal enveloping algebra of the $\mathfrak{sl}(2)$ Lie algebra.

para Lília, com todo meu amor...

Agradecimentos

À Santíssima Trindade, Fonte de toda Ciência e Sabedoria, pelo Dom da Vida.

À minha esposa, Lília, por sua paciência e dedicação, e por suportar minha ausência durante as longas horas de trabalho.

À minha mãe, Maria, pelo seu grande esforço, que permitiu realizar minha formação.

Ao meu amigo e orientador Prof. Dr. Paulo Afonso Faria da Veiga, pela valiosa inspiração e pelo incentivo que me permitiram decidir por esta excelente carreira.

À Profa. Dra. Ires Dias, pela assistência e pelos vários aconselhamentos.

À CAPES, pelo apoio financeiro integral a este trabalho.

À UFSCar, especialmente aos colegas e funcionários do DM, pela calorosa acolhida.

Aos meus amigos e companheiros, de modo especial a Marcelo Escudeiro Hernandes, a quem ainda devo um exemplar do Scott.

Aos professores e funcionários do ICMSC, pela acolhida, pelo apoio, e pelos serviços prestados.

Ao meu antigo chefe na ABC Bull, Sr. Aurélio Takeshi Iwasa, que me convenceu a retomar meus estudos, dando-me o apoio necessário, e a quem devo mais do que posso expressar.

Waldeck Schützer

Conteúdo

1 Introdução **1**

2 Álgebras de Lie **4**

2.1 Conceitos Básicos 4

2.1.1 Definição e primeiras propriedades 4

2.1.2 As famílias clássicas de álgebras de Lie 10

2.2 Álgebras de Lie Solúveis, Nilpotentes e Semisimples 12

2.2.1 A decomposição de Jordan-Chevalley 16

2.2.2 A forma de Killing 18

2.2.3 A decomposição de Jordan abstrata 21

2.3 Grupos e Álgebras de Lie 23

2.3.1 Definição e exemplos 24

2.3.2 A álgebra de Lie $\mathfrak{g}$ de um grupo de Lie G. 26

2.4 Módulos e o Teorema de Weyl 28

2.4.1 Definição e exemplos 28

2.4.2 O Elemento de Casimir de uma representação 33

2.4.3 O Teorema de Weyl 35

2.4.4 Conservação da decomposição de Jordan 38

2.5 Representações de dimensão finita de $\mathfrak{sl}(2, F)$ 39

2.5.1 Pletismo 43

2.5.2 Resumo 45

2.6 Classificação das Álgebras de Lie Semisimples de Dimensão Finita 46

2.6.1 Álgebras Torais Maximais . . . 46
2.6.2 Propriedades da decomposição do espaço por raízes . . . 49
2.6.3 Sistemas de raízes . . . 55
2.6.4 Raízes simples . . . 60
2.6.5 Teorema de Classificação . . . 63
2.7 A álgebra universal envolvente $U\mathfrak{g}$ de uma álgebra de Lie $\mathfrak{g}$ . . . 72
2.7.1 A construção de $U\mathfrak{g}$ . . . 73
2.7.2 O Teorema de Poincaré-Birkhoff-Witt . . . 74

3 Álgebras de Hopf 77

3.1 Álgebras Associativas com Unidade . . . 77
3.1.1 Definição e exemplos . . . 78
3.1.2 Teorema Fundamental do Isomorfismo . . . 82
3.2 Coálgebras . . . 84
3.2.1 Definição e exemplos . . . 84
3.2.2 Dualidade entre álgebras e coálgebras . . . 90
3.2.3 Subcoálgebras e coideais . . . 94
3.2.4 Teorema Fundamental do Isomorfismo para Coálgebras . . . 97
3.2.5 Conclusão . . . 99
3.3 Biálgebras . . . 100
3.3.1 Definição e exemplos . . . 100
3.3.2 Teorema Fundamental do Isomorfismo para Biálgebras . . . 102
3.4 Álgebras de Hopf . . . 103
3.4.1 Definição e exemplos . . . 104
3.4.2 Álgebra de Convolução . . . 106
3.4.3 Propriedades da Aplicação Antípoda . . . 107
3.4.4 Conclusão . . . 109

4 Grupos Quânticos 111

4.1 Álgebras de Hopf quasitriangulares . . . 111
4.1.1 Definição e exemplos . . . 111

4.1.2 Álgebras de Hopf quasitriangulares e a QYBE 116
4.2 As Álgebras de Hopf $\breve{A}(R)$ e $\breve{U}(R)$ 119
4.2.1 As biálgebras $A(R)$ e $\tilde{U}(R)$ 119
4.2.2 Representação fundamental de $A(R)$ e a biálgebra $\tilde{U}(R)$ 121
4.2.3 As álgebras de Hopf $\breve{A}(R)$ e $\breve{U}(R)$ 124
4.2.4 Famílias clássicas de Grupos Quânticos 125
4.2.5 Os grupos quânticos $SL_q(2, \mathbb{C})$ e $U_q\mathfrak{sl}(2, \mathbb{C})$ 127
4.3 O análogo quântico $U_t\mathfrak{g}$ da álgebra universal envolvente $U\mathfrak{g}$ de uma álgebra de Lie simples $\mathfrak{g}$ 129
4.3.1 Sobre a estrutura de $U_t\mathfrak{g}$ quando t não é raiz da unidade 133
4.3.2 Representações de dimensão finita de $U_t\mathfrak{g}$ 139
4.4 Observações Finais 145

A Álgebra Linear 146

A.1 Módulos 146
A.1.1 Preliminares algébricos 146
A.1.2 Definição e exemplos 149
A.1.3 Produto Direto 150
A.1.4 A aplicação transposição 152
A.1.5 Soma direta 153
A.1.6 Módulos livres 154
A.1.7 Produto Tensorial 155
A.1.8 Produtos Simétrico e Exterior 164
A.2 Dualidade de Espaços Vetoriais 169
A.2.1 Espaço Ortogonal 169

B Álgebra 173

B.1 Homomorfismos 173
B.2 Álgebras Filtradas e Álgebras Graduadas 175

C Representações de Grupos Finitos **177**

C.1 Definição e exemplos 177

C.2 Redutibilidade Completa 179

Capítulo 1

Introdução

Nos últimos anos, vários campos da Matemática têm se beneficiado de uma proveitosa interação com a Física Teórica, conforme testemunham, por exemplo, as atribuições mais recentes da Medalha Fields (cf. Casacuberta [CC] e Jaffe [FQ]).

Paralelamente à Teoria dos Nós, ao estudo das representações dos Grupos de Tranças, e à Geometria Não-Comutativa, um exemplo proeminente desta interação é o tópico dos Grupos Quânticos, lançado originalmente por Jimbo [Ji3] e Drinfeld [D] em 1985, e que hoje é objeto de estudo intensivo.

Embora tenha se originado nos estudos dos sistemas completamente integráveis da Mecânica Estatística e na Teoria Quântica dos Campos, apesar do nome, os grupos quânticos não apresentam estrutura de grupo e só tem a estrutura não-comutativa em comum com os sistemas quantizados da Física. Rigorosamente falando, estes correspondem a estruturas (bi-)algébricas denominadas Álgebras de Hopf Quasitriangulares, que aparecem como ingredientes básicos subjacentes nas chamadas equações de Yang-Baxter. Estas são as principais equações que governam a Física dos sistemas completamente integráveis.

Motivados, quando da confecção inicial de nosso programa de mestrado, pela não-disponibilidade de um bom compêndio no assunto, e motivados também pela ainda pequena penetração deste tópico na comunidade de matemáticos do país, quando comparado a quase todo grande centro de Matemática no mundo, neste trabalho, propor-nos-emos a fazer um estudo introdutório e de revisão sobre os Grupos Quânticos, visando a elaborar um primeiro guia em português, em linguagem acessível, que eventualmente possibilite a motivação de outros colegas e a difusão do assunto em outros centros.

Obviamente, dados os limites da nossa experiência e da duração de nosso projeto, nosso estudo não pôde ser completo e estará certamente aquém, em detalhes e conteúdo, do que aparece no excelente tratado publicado recentemente por Chary & Pressley [CP], que acabou por constituir-se numa referência essencial.

Além deste, tomamos como base os trabalhos originais de Drinfeld [D], Jimbo [Ji3], Majid [Ma] e Smith [Sm], assim como as notas de aula do curso de verão que ministrou o Prof. Ph. Roche [Ro2] no ICMSC-USP, em 1994, e seus artigos [RA] e [Ro1]. O livro de Lustig [Lu], de leitura extremamente difícil, também serviu-nos de suporte.

Nosso estudo constituiu-se de três etapas principais. Sendo a Teoria das Álgebras de Lie e suas Álgebras Envolventes um importante pré-requisito para o estudo dos Grupos Quânticos, a primeira etapa foi consagrada a um estudo crítico e detalhado do livro clássico de Humphreys [Hu], sendo que também buscamos inspiração nas obras de Serre [Se] e Bourbaki [Bo], a fim de podermos compreender pontos mais delicados tais como o estudo axiomático e classificatório dos sistemas de raízes. As Álgebras de Lie são apresentadas no Capítulo 2 e, se quiser, um leitor experiente pode ir diretamente ao capítulo seguinte, sem prejuízos maiores para a continuidade.

A segunda etapa constituiu-se de um estudo sobre as Álgebras de Hopf, seja do ponto de vista mais clássico, como o apresentado nos livros de Sweedler [Sw] e Abe [A], seja do ponto mais dirigido à introdução dos Grupos Quânticos, conforme explorado no trabalho de revisão de Majid [Ma].

Na última etapa, tratamos do estudo dos Grupos Quânticos propriamente ditos, onde, baseados nas referências acima mencionadas, introduzimos a quantização ou deformação $U_t\mathfrak{g}$ correspondente à álgebra universal envolvente $U\mathfrak{g}$ de uma álgebra de Lie simples $\mathfrak{g}$ (sendo imediata a extensão ao caso de uma álgebra semisimples).

No decorrer dos estudos, vários conceitos e resultados elementares da Álgebra e da Álgebra Linear, que não foram abordados por nossa formação clássica, tiveram de ser aprimorados. Parte do resultado desse estudo encontra-se nos três apêndices que se encontram no final do texto. Esperamos que o leitor possa neles encontrar todos os ingredientes necessários à compreensão deste trabalho.

Concluindo, vale mencionar, por um lado, o papel central (e enigma!) que desempenha a fórmula de Reshetikhin-Turaeev [RT] na Matemática atual, descrevendo invariantes de nós e de 3-variedades, cuja obtenção se serve do Grupo Quântico $U_t\mathfrak{sl}(2)$ (cf. o Exemplo 111 tratado na seção 4.3.2) para tornar rigoroso um argumento de Witten [Wi].

Por outro lado, mencionamos que o assunto estudado nesta tese encontra-se longe de ser fechado e que existem ainda inúmeros problemas em aberto envolvendo os próprios grupos quânticos. Explora-se também sua relação com a Teoria de Galois, a qual parece bastante promissora.

Este trabalho teve um papel decisivo na nossa opção pela carreira acadêmica, especialmente pela Matemática Pura. Cremos estar investindo em uma área proeminente, que nos proporcionará conhecimentos sólidos e perenes, que nos auxiliarão na continuidade de nossa formação superior, assegurando uma futura atuação em pesquisas de modo muito proveitoso.

Capítulo 2

Álgebras de Lie

As Álgebras de Lie são estruturas algébricas de ocorrência muito freqüente em diversas áreas da Matemática, a ponto de haverem se tornado tema indispensável na formação de bons especialistas. Seu estudo serve de base para muitas teorias avançadas, por exemplo, a teoria que nos propomos a estudar nos capítulos subseqüentes. Além disso, consistem de objetos de interesse e de estudo per si, revelando ainda muitos problemas em aberto.

O objetivo deste capítulo é apresentar as principais idéias da Teoria das Álgebras de Lie, sobretudo o estudo dos Sistemas de Raízes e o Teorema de Classificação para as álgebras semisimples de dimensão finita. Embora não façamos nenhum estudo geral sobre representações dessas álgebras, discutimos detalhadamente o caso das representações de $\mathfrak{sl}(2)$. Além deste tópico a álgebra $\mathfrak{sl}(2)$ sempre estará presente nos exemplos específicos que discutiremos, já que este será também o exemplo construído em detalhes no caso quântico.

2.1 Conceitos Básicos

2.1.1 Definição e primeiras propriedades

Uma *Álgebra de Lie* é um espaço vetorial $\mathfrak{g}$ sobre um corpo F munido de uma aplicação $\mathfrak{g}\times\mathfrak{g} \to \mathfrak{g}$, denominada *operação colchete*. Sua avaliação sobre o par $(x, y) \in \mathfrak{g} \times \mathfrak{g}$ é denotada por $[xy]$ e satisfaz as seguintes condições:

(L1) A operação colchete é bilinear.

(L2) $[xx] = 0$, para todo $x \in \mathfrak{g}$.

(L3) $[x\,[yz]] + [y\,[zx]] + [z\,[xy]] = 0$, quaisquer que sejam $x, y, z \in \mathfrak{g}$.

Equivalentemente, podemos definir a operação colchete como uma aplicação linear

$$\begin{array}{rcl} [\ ,\ ] : \Lambda^2\mathfrak{g} & \to & \mathfrak{g} \\ x \wedge y & \mapsto & [xy] \end{array}$$

satisfazendo a condição (L3), onde $\Lambda^2\mathfrak{g}$ é a segunda potência exterior de $\mathfrak{g}$ (cf. pág. 168). A operação colchete também é conhecida como *produto de Lie*, e o elemento $[xy] \in \mathfrak{g}$ é chamado *comutador* de x por y. A condição (L3), chamada *Identidade de Jacobi*, tem papel fundamental nesta teoria pois distingue uma álgebra de Lie de uma álgebra associativa. Se F tiver característica distinta de 2, a condição (L2) é claramente equivalente à condição de anti-simetria $[xy] = -[yx]$. De fato, por um lado, (L1) e (L2) implicam

$$\begin{aligned} 0 &= [x+y, x+y] \\ &= [xx] + [xy] + [yx] + [yy] \\ &= [xy] + [yx] \end{aligned}$$

isto é, $[xy] = -[yx]$. Por outro lado, $[xy] = -[yx]$ implica

$$\begin{aligned} 0 &= [xx] + [xx] \\ &= 2[xx], \end{aligned}$$

que certamente resulta em $[xx] = 0$, se F tem característica distinta de 2 .

Dizemos que $\mathfrak{g}$ é *abeliana* quando a operação colchete é trivial, isto é, quando $[xy] = 0$, para todo $x, y \in \mathfrak{g}$.

Neste trabalho, estaremos interessados principalmente nas álgebras de Lie cujo espaço vetorial subjacente $\mathfrak{g}$ é de dimensão finita sobre F. *Isto será sempre assumido, salvo menção em contrário.* Além disso, os axiomas que definem uma álgebra de Lie continuam a fazer sentido se substituímos F por um anel comutativo, mas não iremos abordar essa (interessante) possibilidade aqui.

Vários conceitos da Álgebra e da Álgebra Linear podem ser transportados imediatamente para a Teoria das Álgebras de Lie. Vejamos alguns.

Definição 1 (Subálgebra) Um subespaço K de $\mathfrak{g}$ é denominado *subálgebra de Lie* de $\mathfrak{g}$, se K for fechado em relação ao comutador, ou seja, $[xy] \in K$, para todo $x, y \in K$. Isto significa que K é uma álgebra de Lie por si mesma. Particularmente, $0 = \{0\}$ e $\mathfrak{g}$ são subálgebras de Lie de $\mathfrak{g}$, chamadas subálgebras *triviais.* Qualquer outra subálgebra de $\mathfrak{g}$ distinta de 0 e de $\mathfrak{g}$ é chamada *própria.*

Um exemplo importante de subálgebra é a *álgebra derivada* de $\mathfrak{g}$, definida pelo conjunto $[\mathfrak{g}\mathfrak{g}] = \{\sum[x_i y_i] : x_i, y_i \in \mathfrak{g}\}$. Novamente, temos que $\mathfrak{g}$ é abeliana se, e só se, $[\mathfrak{g}\mathfrak{g}] = 0$.

Definição 2 (Ideal) Um subespaço I de $\mathfrak{g}$ é denominado *ideal* de $\mathfrak{g}$ se para todo $x \in \mathfrak{g}$ e todo $y \in I$ ocorrer $[xy] \in I$ (também poderíamos dizer que $[yx] \in I$, em vista da condição L2). Os ideais 0 e $\mathfrak{g}$ são ditos *triviais* e todo ideal de $\mathfrak{g}$ distinto destes é dito *próprio.*

Como primeiros exemplos de ideais temos o *centro* de $\mathfrak{g}$, definido pelo conjunto

$$Z(\mathfrak{g}) = \{z \in \mathfrak{g} : [zx] = 0, \text{ para todo } x \in \mathfrak{g}\},$$

e também a álgebra derivada $[\mathfrak{g}\mathfrak{g}]$. Uma vez mais, podemos notar que $\mathfrak{g}$ é abeliana se, e só se, $Z(\mathfrak{g}) = \mathfrak{g}$.

Se I e J são ideais de uma álgebra de Lie $\mathfrak{g}$, então também são ideais

$$I + J = \{x + y : x \in I \text{ e } y \in J\},$$

$$[IJ] = \{\sum[x_i y_i] : x_i \in I \text{ e } y_i \in J\}.$$

Se $\mathfrak{g}$ tem apenas os ideais triviais e $[\mathfrak{g}\mathfrak{g}] \neq 0$, dizemos que $\mathfrak{g}$ é *simples*. Neste caso, é fácil concluir também que $Z(\mathfrak{g}) = 0$ e $[\mathfrak{g}\mathfrak{g}] = \mathfrak{g}$.

Definição 3 (Homomorfismo) Um *homomorfismo de álgebras de Lie* é uma aplicação linear $\varphi : \mathfrak{g} \to \mathfrak{g}'$ entre álgebras de Lie $\mathfrak{g}$ e $\mathfrak{g}'$, satisfazendo a condição: $\varphi([xy]) = [\varphi(x)\varphi(y)], \forall\, x, y \in \mathfrak{g}$. O *núcleo* de um homomorfismo φ é o subconjunto $\operatorname{Ker}\varphi = \{x \in \mathfrak{g} : \varphi(x) = 0\}$. Dizemos que um homomorfismo de álgebras de Lie é *monomorfismo* se $\operatorname{Ker}\varphi = 0$, *epimorfismo* se $\operatorname{Im}\varphi = \mathfrak{g}'$, e *isomorfismo* se ambas as condições se verificarem. Um *endomorfismo* é um homomorfismo de $\mathfrak{g}$ *em* $\mathfrak{g}$.

O núcleo de um homomorfismo $\varphi : \mathfrak{g} \to \mathfrak{g}'$ é um ideal de $\mathfrak{g}$ e a imagem de φ é uma subálgebra de $\mathfrak{g}'$. De fato, se $\varphi(x) = 0$ e $y \in \mathfrak{g}$, temos $\varphi([xy]) = [\varphi(x)\varphi(y)] = 0$, donde $[xy] \in \operatorname{Ker}\varphi$. Similarmente, dados $\varphi(x), \varphi(y) \in \mathfrak{g}'$, temos $[\varphi(x)\varphi(y)] = \varphi([xy]) \in \mathfrak{g}'$.

Um homomorfismo de grande importância é a *representação adjunta* de $\mathfrak{g}$, definida pela aplicação $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, tal que $x \mapsto (y \mapsto \operatorname{ad} x(y) = [xy])$. Uma propriedade notável deste homomorfismo é que seu núcleo coincide exatamente com $Z(\mathfrak{g})$, o centro de $\mathfrak{g}$. Isto nos proporciona dois casos extremos: quando $\mathfrak{g}$ é abeliana, então $\operatorname{ad} = 0$, e quando $Z(\mathfrak{g}) = 0$, ad é injetora. Em vista da identidade de Jacobi temos ainda

$$\operatorname{ad} x([yz]) = [x\,[yz]] = -[y\,[zx]] - [z\,[xy]] = [y, \operatorname{ad} x(z)] + [\operatorname{ad} x(y), z].$$

Os endomorfismos que satisfazem uma igualdade como esta são denominados *derivações*. Ao conjunto de todas as derivações de $\mathfrak{g}$ denotamos por $\operatorname{Der}\mathfrak{g}$.

Na verdade, o conjunto das derivações está definido para qualquer F-álgebra $\mathfrak{U}$ (esta é um espaço vetorial sobre F, dotado de um produto) não necessariamente associativa. Este é o conjunto dos endomorfismos $\delta : \mathfrak{U} \to \mathfrak{U}$ tais que a Regra de Leibniz

$$\delta(xy) = x\delta(y) + \delta(x)y,$$

seja satisfeita para todo $x, y \in \mathfrak{U}$. Se $\operatorname{End}\mathfrak{U}$ é o espaço vetorial formado por todos os endomorfismos de $\mathfrak{U}$, pode-se verificar facilmente que $\operatorname{Der}\mathfrak{U}$ é um subespaço vetorial de $\operatorname{End}\mathfrak{U}$, e que $\operatorname{Der}\mathfrak{U}$ é fechada pelo comutador $[\delta\delta'] = \delta\delta' - \delta'\delta$ de duas derivações quaisquer. Conseqüentemente, $\operatorname{Der}\mathfrak{U}$ é uma subálgebra de Lie de $\mathfrak{gl}(\mathfrak{U})$ e a imagem da representação adjunta $x \mapsto \operatorname{ad} x$ é uma subálgebra de Lie de $\operatorname{Der}\mathfrak{g}$. Todas as derivações de $\mathfrak{g}$ contidas nesta imagem são denonimadas *internas* e as demais *externas*.

Para uso posterior, introduzimos também alguns conceitos provenientes da teoria de grupos. O *normalizador* de uma subálgebra (ou mesmo subespaço) K de $\mathfrak{g}$ é a subálgebra $N_{\mathfrak{g}}(K) = \{x \in \mathfrak{g} : [xK] \subset K\}$, que é a maior subálgebra de $\mathfrak{g}$ contendo K como um ideal. O *centralizador* de um subconjunto X de $\mathfrak{g}$ é a subálgebra $C_{\mathfrak{g}}(X) = \{y \in \mathfrak{g} : [yX] = 0\}$. Se X for um conjunto contendo um único elemento x, escrevemos simplesmente $C_{\mathfrak{g}}(x)$ para $C_{\mathfrak{g}}(\{x\})$. Por exemplo, $C_{\mathfrak{g}}(\mathfrak{g}) = Z(\mathfrak{g})$.

Para uma álgebra de Lie $\mathfrak{g}$, construímos a *álgebra quociente* $\mathfrak{g}/I$ de $\mathfrak{g}$ por um ideal I de maneira análoga à dos anéis quocientes. O espaço vetorial $\mathfrak{g}/I$ é simplesmente o quociente do espaço vetorial $\mathfrak{g}$ pelo subespaço I, munido da operação colchete, a qual é definida naturalmente em $\mathfrak{g}/I$ por

$$[x + I, y + I] = [xy] + I$$

para todo $x, y \in \mathfrak{g}$. A operação em $\mathfrak{g}/I$ está bem-definida pois se $x + I = x' + I$ e $y + I = y' + I$ então temos $x' = x + u$ e $y' = y + v$ para algum $u, v \in I$, donde $[x'y'] - [xy] = [uy] + [xv] + [uv] \in I$, já que I é um ideal. Isto significa também que a *projeção canônica* $\mathfrak{g} \to \mathfrak{g}/I$, tal que $x \mapsto x + I$, é um homomorfismo de álgebras de Lie.

As seguintes proposições introduzem os resultados clássicos sobre homomorfismos, cujas demonstrações são idênticas àquelas que aparecem em Álgebra Linear (cf. Brown [Br, I, 5]).

Proposição 4 (1^o Teorema do Isomorfismo) *Seja $\varphi : \mathfrak{g} \to \mathfrak{g}'$ um homomorfismo de álgebras de Lie, e I um ideal de $\mathfrak{g}$ tal que $I \subset \operatorname{Ker} \varphi$. Então, existe um único homomorfismo de álgebras $\psi : \mathfrak{g}/I \to \mathfrak{g}'$ de Lie tornando comutativo o diagrama*

$$\begin{tikzcd} \mathfrak{g} \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & \mathfrak{g}' \\ & \mathfrak{g}/I \arrow[ur, "\psi"'] & \end{tikzcd}$$

i.é, tal que $\psi \circ \pi = \varphi$, onde $\pi : \mathfrak{g} \to \mathfrak{g}/I$ é a projeção canônica. Particularmente, temos

$$\frac{\mathfrak{g}}{\operatorname{Ker} \varphi} \cong \operatorname{Im} \varphi.$$

Proposição 5 (2^o Teorema do Isomofismo) *Se I e J são ideais de $\mathfrak{g}$ então*

$$\frac{I + J}{J} \cong \frac{I}{I \cap J}$$

onde o isomorfismo é natural.

Proposição 6 (3^o Teorema do Isomorfismo) *Se I e J são ideais de $\mathfrak{g}$ tais que $I \subset J$, então J/I é um ideal de $\mathfrak{g}/I$ e temos o isomorfismo natural*

$$\frac{\mathfrak{g}/I}{J/I} \cong \frac{\mathfrak{g}}{J}.$$

Exemplo 7 (Unidimensional) Se $\mathfrak{g}$ é uma álgebra de Lie unidimensional, então $\mathfrak{g} = Fx$ para algum vetor não-nulo $x \in \mathfrak{g}$. Desse modo, vê-se imediatamente que $\mathfrak{g}$ é abeliana, e tem-se, no máximo, uma álgebra de Lie de dimensão 1 (a menos de isomorfismos). □

Exemplo 8 (Bidimensional) Seja $\mathfrak{g}$ uma álgebra de Lie de dimensão 2, com base $\{x, y\}$. Como $\dim \Lambda^2\mathfrak{g} = 1$, o posto da aplicação colchete $[\ ,\ ]$ somente pode ser 0 ou 1 (recordamos que o posto de uma aplicação linear é a dimensão de sua imagem). Se o posto for nulo, então a operação colchete é trivial e $\mathfrak{g}$ é abeliana. Por outro lado, se o posto for 1, podemos construir uma nova base de $\mathfrak{g}$ substituindo x por um gerador da imagem de $[\ ,\ ]$ e substituindo y por qualquer vetor independente de x. Assim, obtemos uma base em que $[xy] = ax$ $(0 \neq a \in F)$. Ademais, podemos multiplicar y por a^{-1} obtendo finalmente $[xy] = x$. Com isto, determinamos $\mathfrak{g}$ completamente e, portanto, há no máximo uma álgebra de Lie não abeliana de dimensão 2 (a menos de isomorfismos). □

Exemplo 9 (Álgebras Lineares) Seja V um espaço vetorial de dimensão finita n sobre F. Sabemos que $\operatorname{End} V$, o conjunto das transformações lineares $V \to V$, é uma álgebra associativa com unidade de dimensão n^2 sobre F. $\operatorname{End} V$ admite a operação colchete usual dada por

$$[xy] = xy - yx,$$

para todo $x, y \in \operatorname{End} V$. É simples verificar que esta operação realmente satisfaz os axiomas (L1)-(L3), tornando $\operatorname{End} V$ numa álgebra de Lie. Com esta nova estrutura, $\operatorname{End} V$ é chamada *álgebra geral linear,* denotada por $\mathfrak{gl}(V)$ (devido à estreita relação com o grupo geral linear, $\mathrm{GL}(V)$, dos automorfismos de V).

Toda subálgebra de $\mathfrak{gl}(V)$ é chamada *álgebra de Lie linear.* Fixada uma base, $\mathfrak{gl}(V)$ se identifica ao conjunto de todas as matrizes $n \times n$ sobre F, denotado por $\mathfrak{gl}(n, F)$. Esta identificação é bastante útil para realizar cálculos explícitos. Para ilustrar, em relação à base canônica de $\mathfrak{gl}(n, F)$ consistindo das matrizes e_{ij} tendo 1 na posição (i, j) e 0 nas demais posições, escrevemos a tabela de multiplicação dada pela expressão

$$[e_{ij}e_{kl}] = \delta_{jk}e_{il} - \delta_{li}e_{kj},$$

onde δ_{ij} é o *Delta de Kronecker*. Observemos que $e_{ij}e_{kl} = \delta_{jk}e_{il}$. □

Um homomorfismo de $\mathfrak{g}$ em $\mathfrak{gl}(V)$, é dito ser uma*representação* e, neste caso, V é dito $\mathfrak{g}$-*módulo*. Toda representação injetora é dita ser *fiel*. Por abuso de linguagem, costuma-se dizer simplesmente que V é uma representação de $\mathfrak{g}$.

2.1.2 As famílias clássicas de álgebras de Lie

Apresentamos a seguir quatro famílias de álgebras de Lie que estão em estreita relação com os respectivos grupos de Lie clássicos e cujo estudo tornou-se consagrado. Por essa razão, estas são também denominadas *álgebras de Lie clássicas*.

Exemplo 10 (A_l) Seja V um espaço vetorial de dimensão $l + 1$ sobre F. Consideremos o subconjunto $\mathfrak{sl}(V)$ de $\mathfrak{gl}(V)$ consistindo dos endomorfismos x de V com traço nulo, também denotado $\mathfrak{sl}(l + 1, F)$. Como $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$, e $\mathrm{Tr}(xy) = \mathrm{Tr}(yx)$, temos $\mathrm{Tr}([xy]) = \mathrm{Tr}(xy - yx) = 0$, donde $\mathfrak{sl}(V)$ é uma subálgebra de $\mathfrak{gl}(V)$, chamada *álgebra especial linear.* A dimensão de $\mathfrak{sl}(V)$ pode ser facilmente calculada: por um lado, esta é no máximo $(l + 1)^2 - 1$. Por outro lado, as $(l + 1)^2 - 1$ matrizes e_{ij} $(i \neq j)$ e $h_i = e_{ii} - e_{i+1,i+1}$ $(1 \leq i \leq l)$ formam um conjunto linearmente independente, sendo, assim, uma base de $\mathfrak{sl}(V)$. Essa base é chamada *canônica.* □

Exemplo 11 (Álgebra $\mathfrak{s}l(2, F)$) Um caso particular e muito importante da família A_l de álgebras é o de $\mathfrak{sl}(2, F)$. O estudo das representações desta álgebra permitirá obter resultados gerais sobre a Teoria das Representações de Álgebras de Lie, e também a classificação das álgebras simples. A base canônica consiste das matrizes

$$x = e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad h = e_{11} - e_{22} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad y = e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Em relação a esta base temos as relações de comutação de $\mathfrak{sl}(2, F)$

$$[hx] = 2x, \qquad [xy] = h, \qquad [hy] = -2y, \tag{2.1}$$

e as respectivas relações opostas. Ainda na mesma base, estas relações permitem-nos ver claramente que as matrizes das representações adjuntas de x, h, y são respectivamente

$$\operatorname{ad} x = \begin{pmatrix} 0 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \operatorname{ad} h = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \operatorname{ad} y = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

Exemplo 12 (C_l) Seja V um espaço vetorial de dimensão $2l$ sobre F, com base $(v_1, \ldots, v_{2l})$. Definimos uma forma bilinear anti-simétrica f sobre V pela matriz $s = \begin{pmatrix} 0 & I_l \\ -I_l & 0 \end{pmatrix}$, onde I_l é a matriz identidade $l \times l$ e denotamos por $\mathfrak{sp}(V)$ ao conjunto dos endomorfismos de V satisfazendo

$$f(x(v), w) = -f(v, x(w)),$$

para todo $v, w \in V$. Para todo $x, y \in \mathfrak{sp}(V)$ e todo $v, w \in V$ temos

$$\begin{aligned} f([xy](v), w) &= f(x(y(v)) - y(x(v)), w) \\ &= f(x(y(v)), w) - f(y(x(v)), w) \\ &= -f(y(v), x(w)) + f(x(v), y(w)) \\ &= f(v, y(x(w))) - f(v, x(y(w))) \\ &= f(v, (yx - xy)(w)) = -f(v, [xy](w)), \end{aligned}$$

isto é $[xy] \in \mathfrak{sp}(V)$. Portanto, este subconjunto é uma subálgebra de $\mathfrak{gl}(V)$, chamada *álgebra simplética.* Escrevendo-se a equação que define $\mathfrak{sp}(V)$ em notação matricial, torna-se fácil determinar por um cálculo direto que esta álgebra tem dimensão $2l^2 + l$ sobre F. $\square$

Exemplo 13 (B_l) Seja $\dim V = 2l + 1$, e consideremos a forma bilinear simétrica f definida pela matriz $s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I_l \\ 0 & I_l & 0 \end{pmatrix}$. Consideremos também o subconjunto $\mathfrak{o}(V)$ de $\mathfrak{gl}(V)$ de todos os endomorfismos de V satisfazendo a condição $f(x(v), w) = -f(v, x(w))$, para todo $v, w \in V$. Assim como no exemplo anterior, verificamos facilmente que $\mathfrak{o}(V)$ é uma álgebra de Lie. Esta é denominada *álgebra ortogonal*, e tem dimensão $2l^2 + l$ sobre F. $\square$

Exemplo 14 (D_l) Seja $\dim V = 2l$. Obtemos outra álgebra ortogonal, cuja construção é idêntica à de B_l, tomando, porém, $s = \begin{pmatrix} 0 & I_l \\ I_l & 0 \end{pmatrix}$ pela matriz que define a forma bilinear f. Neste caso, verificamos que $\dim \mathfrak{o}(V) = 2l^2 - l$. $\square$

As álgebras dos exemplos $A_l - D_l$ são denominadas álgebras de Lie clássicas (devido à correspondência com os grupos de Lie clássicos). Há ainda outras subálgebras de $\mathfrak{gl}(n, F)$ que são igualmente importantes. Temos $\mathfrak{t}(n, F)$, a álgebra das matrizes triangulares superiores (i.é, das matrizes (a_{ij}) tais que $a_{ij} = 0$ se $i > j$), $\mathfrak{n}(n, F)$, das matrizes triangulares estritamente superiores ($a_{ij} = 0$, se $i \geq j$), e $\mathfrak{d}(n, F)$, das matrizes diagonais. Observemos que $\mathfrak{t}(n, F) = \mathfrak{n}(n, F) + \mathfrak{d}(n, F)$, e $[\mathfrak{d}(n, F), \mathfrak{n}(n, F)] = \mathfrak{n}(n, F)$, donde a álgebra derivada de $\mathfrak{t}(n, F)$ é $\mathfrak{n}(n, F)$.

2.2 Álgebras de Lie Solúveis, Nilpotentes e Semisimples

A definição de solubilidade para álgebras de Lie imita o conceito correspondente da teoria de grupos, enquanto que a de nilpotência de grupos foi introduzida posteriormente a partir do conceito existente para as álgebras de Lie.

Definição 15 (Série derivada) *Seja $\mathfrak{g}$ uma álgebra de Lie. A* série derivada *de $\mathfrak{g}$ é a seqüência de ideais*

$$\mathfrak{g}^{(0)} = \mathfrak{g},\ \mathfrak{g}^{(1)} = [\mathfrak{g}\mathfrak{g}],\ \mathfrak{g}^{(2)} = [\mathfrak{g}^{(1)}\mathfrak{g}^{(1)}], \ldots,\ \mathfrak{g}^{(i)} = [\mathfrak{g}^{(i-1)}\mathfrak{g}^{(i-1)}],\ \ldots$$

Definição 16 (Álgebra solúvel) *Uma álgebra de Lie* $\mathfrak{g}$ *é dita* solúvel *se* $\mathfrak{g}^{(n)} = 0$ *para algum* $n = 0, 1, \ldots$

Definição 17 (Série descendente central) *A* série descendente central *de uma álgebra de Lie* $\mathfrak{g}$ *é a seqüência de ideais*

$$\mathfrak{g}^0 = \mathfrak{g},\ \mathfrak{g}^1 = [\mathfrak{g}\mathfrak{g}],\ \mathfrak{g}^2 = [\mathfrak{g}\mathfrak{g}^1],\ \ldots,\ \mathfrak{g}^i = [\mathfrak{g}\mathfrak{g}^{i-1}],\ \ldots$$

Definição 18 (Álgebra nilpotente) *Uma álgebra de Lie* $\mathfrak{g}$ *é dita nilpotente se* $\mathfrak{g}^n = 0$ *para algum* $n = 0, 1, \ldots$

As álgebra abelianas são trivialmente solúveis e nilpotentes e as álgebras simples não são solúveis (a série derivada é constante e igual a $\mathfrak{g}$). Além disso, as álgebras nilpotentes são solúveis pois $\mathfrak{g}^{(i)} \subset \mathfrak{g}^i$. Contudo, a recíproca não é verdadeira: basta tomar $\mathfrak{g} = \mathfrak{t}(n, F)$ para obter $\mathfrak{g}^{(1)} = \mathfrak{g}^1 = \mathfrak{n}(n, F)$, $\mathfrak{g}^2 = [\mathfrak{g}\mathfrak{g}^1] = \mathfrak{g}^1$ e, assim por diante, $\mathfrak{g}^i = \mathfrak{g}^1$. Por outro lado, $\mathfrak{g}^{(1)}$ é nilpotente, donde $\mathfrak{g}$ é solúvel.

As álgebras solúveis e nilpotentes têm as seguintes propriedades imediatas, cuja prova pode ser encontrada em Humphreys[Hu, §3.1 e §3.2]:

Proposição 19 *Seja* $\mathfrak{g}$ *uma álgebra de Lie.*

(a) Se $\mathfrak{g}$ *é solúvel (nilpotente) então também o são todas as subálgebras e imagens homomórficas de* $\mathfrak{g}$.

(b) Se I *é um ideal solúvel de* $\mathfrak{g}$ *tal que* $\mathfrak{g}/I$ *seja solúvel, então* $\mathfrak{g}$ *é solúvel.* $\mathfrak{g}$ *é nilpotente se* $\mathfrak{g}/Z(\mathfrak{g})$ *for nilpotente.*

(c) Se $\mathfrak{g}$ *é nilpotente então* $Z(\mathfrak{g}) \neq 0$.

(d) Se I *e* J *são ideais solúveis de* $\mathfrak{g}$ *então* $I + J$ *também é solúvel e, portanto,* $\mathfrak{g}$ *admite um único ideal solúvel maximal* $\operatorname{Rad}\mathfrak{g}$.

Definição 20 (Radical de uma Álgebra de Lie) *O único ideal solúvel maximal* $\operatorname{Rad}\mathfrak{g}$ *de uma álgebra de Lie* $\mathfrak{g}$ *é denominado* radical *de* $\mathfrak{g}$.

Definição 21 (Álgebra semisimples) *Uma álgebra de Lie* $\mathfrak{g}$ *é dita* semisimples *se* $\operatorname{Rad}\mathfrak{g}$ *for nulo.*

Isto equivale a dizer que $\mathfrak{g}$ não tem ideais abelianos não-nulos. Com efeito, se I for um ideal abeliano, então I é solúvel assim como $I + \operatorname{Rad}\mathfrak{g}$, obrigando $I + \operatorname{Rad}\mathfrak{g} = \operatorname{Rad}\mathfrak{g}$, isto é $I \subset \operatorname{Rad}\mathfrak{g} = 0$. Por outro lado, se $\operatorname{Rad}\mathfrak{g} \neq 0$, então o último termo não-nulo da série derivada de $\operatorname{Rad}\mathfrak{g}$ é um ideal abeliano de $\mathfrak{g}$. Conseqüentemente, $\mathfrak{g}$ semisimples implica $Z(\mathfrak{g}) = 0$ e, portanto, a representação adjunta de $\mathfrak{g}$ é fiel.

Por exemplo, uma álgebra de Lie simples é trivialmente semisimples, $\mathfrak{g} = 0$ é semisimples e, para $\mathfrak{g}$ arbitrária, $\mathfrak{g}/\operatorname{Rad}\mathfrak{g}$ é semisimples (pela parte (b) da Proposição 19).

A condição de nilpotência para $\mathfrak{g}$ equivale a dizer que $\operatorname{ad}x_1 \operatorname{ad}x_2 \cdots \operatorname{ad}x_n(y) = 0$ para todo $x_1, \ldots, x_n, y \in \mathfrak{g}$. Em particular $(\operatorname{ad}x)^n = 0$, para todo $x \in \mathfrak{g}$, isto é $\operatorname{ad}x$ é um endomorfismo nilpotente de índice n. Quer dizer, se $\mathfrak{g}$ é uma álgebra de Lie nilpotente então todo elemento $x \in \mathfrak{g}$ é ad-*nilpotente*. A recíproca também é verdadeira como atesta o seguinte teorema.

Teorema 22 (Engel) *Se* $\mathfrak{g}$ *é uma álgebra de Lie constituída inteiramente de elementos* ad-*nilpotentes, então* $\mathfrak{g}$ *é nilpotente.*

Para provar este teorema, vamos necessitar dos seguintes lema e teorema.

Lema 23 *Seja* $x \in \mathfrak{gl}(V)$ *um endomorfismo nilpotente. Então* $\operatorname{ad}x$ *é nilpotente.*

Prova. Associamos a x dois endomorfismos de $\operatorname{End}V$, as translações à esquerda e à direita respectivamente: $\lambda_x(y) = xy$ e $\rho_x(y) = yx$. Ambos são endomorfismos nilpotentes. Além disso, λ_x e ρ_x comutam como conseqüência da associatividade da multiplicação de $\operatorname{End}V$. Ademais, como para qualquer anel, a soma ou a diferença de dois endomorfismos nilpotentes que comutam é ainda nilpotente, então $\operatorname{ad}x = \lambda_x - \rho_x$ é nilpotente. ■

Teorema 24 *Seja* $\mathfrak{g}$ *uma subálgebra de* $\mathfrak{gl}(V)$*,* V *um espaço vetorial de dimensão finita sobre* F*. Se* $\mathfrak{g}$ *consiste inteiramente de endomorfismos nilpotentes e* $V \neq 0$*, então existe um vetor não-nulo* $v \in V$*, tal que,* $\mathfrak{g} \cdot v = 0$ *(i.é, um vetor que é anulado por todos os elementos de* $\mathfrak{g}$*).*

Prova. Usemos indução sobre $\dim\mathfrak{g}$, sendo $\dim\mathfrak{g} = 0$ um caso óbvio. Suponhamos que $K \neq \mathfrak{g}$ seja uma subálgebra qualquer de $\mathfrak{g}$. De acordo com o Lema 23, K age (via ad) como uma álgebra de Lie de endomorfismos nilpotentes sobre o espaço vetorial $\mathfrak{g}$, e também sobre o espaço $\mathfrak{g}/K$. Como $\dim K < \dim \mathfrak{g}$, a hipótese de indução nos proporciona um vetor $x + K \neq K$ em $\mathfrak{g}/K$ anulado pela imagem de K em $\mathfrak{gl}(\mathfrak{g}/K)$, isto é, $[yx] \in K$ para todo $y \in K$, enquanto que $x \notin K$. Em outras palavras, K está propriamente contido em $N_{\mathfrak{g}}(K)$.

Agora, se K for uma subálgebra própria maximal de $\mathfrak{g}$, o argumento precedente implica $N_{\mathfrak{g}}(K) = \mathfrak{g}$, ou seja, K é um ideal de $\mathfrak{g}$. Se $\dim \mathfrak{g}/K > 1$, então a imagem inversa em $\mathfrak{g}$ de uma subálgebra unidimensional de $\mathfrak{g}/K$ seria uma subálgebra própria contendo K propriamente, o que contradiz a hipótese da maximalidade de K; portanto K tem codimensão 1. Isto nos permite escrever $\mathfrak{g} = K + Fz$ para qualquer $z \in \mathfrak{g} - K$.

Por indução, $W = \{v \in V : K \cdot v = 0\}$ é não-nulo. Como K é um ideal, W é estável sob $\mathfrak{g}$. Com efeito, $x \in \mathfrak{g}$, $y \in K$, e $w \in W$ implica $yx \cdot w = xy \cdot w - [xy] \cdot w = 0$. Escolhamos $z \in \mathfrak{g} - K$, como acima, de modo que o endomorfismo z (agora agindo sobre o subespaço W) tenha um autovetor, i.é, tal que exista um vetor não nulo $v \in W$ para o qual $z \cdot v = 0$. Finalmente, $\mathfrak{g} \cdot v = 0$, como queríamos. ■

Prova do Teorema de Engel. Os elementos de $\mathfrak{g}$ são todos ad-nilpotentes, logo a álgebra $\operatorname{ad} \mathfrak{g} \subset \mathfrak{gl}(\mathfrak{g})$ satisfaz as hipóteses do Teorema 24. Assumindo $\mathfrak{g} \neq 0$, temos um vetor $x \neq 0$ em $\mathfrak{g}$ para o qual $[\mathfrak{g}x] = 0$ e, conseqüentemente, $Z(\mathfrak{g}) \neq 0$. Por sua vez, $\mathfrak{g}/Z(\mathfrak{g})$ também consiste de elementos ad-nilpotentes e tem dimensão menor que $\mathfrak{g}$. Novamente, a hipótese de indução sobre $\dim \mathfrak{g}$ garante-nos que $\mathfrak{g}/Z(\mathfrak{g})$ é nilpotente e, por conseqüência, $\mathfrak{g}$ é nilpotente. ■

Outra aplicação imediata do Teorema 24 é mostrar que existe uma base de V em relação à qual todas as matrizes de $\mathfrak{g}$ estão em $\mathfrak{n}(n, F)$, isto é são triangulares estritamente superiores (cf. Humphreys [Hu, Cor. 3.3]).

Para o caso em que $\mathfrak{g} \subset \mathfrak{gl}(V)$ é solúvel e F é algebricamente fechado, um resultado semelhante é garantido pelo seguinte teorema.

Teorema 25 (Teorema de Lie) *Seja $\mathfrak{g} \subset \mathfrak{gl}(V)$ uma álgebra de Lie solúvel onde V é um espaço vetorial de dimensão finita sobre um corpo F algebricamente fechado e de característica* 0. *Então existe uma base de V em relação a qual as matrizes de $\mathfrak{g}$ estão em $\mathfrak{t}(n, F)$, isto é, são triangulares superiores.*

O Teorema de Lie é um corolário do seguinte teorema, cuja prova é essencialmente análoga à do Teorema 24.

Teorema 26 *Seja* $\mathfrak{g}$ *uma subálgebra solúvel de* $\mathfrak{gl}(V)$, V *um espaço vetorial de dimensão finita sobre um corpo* F *algebricamente fechado e de característica* 0. *Se* $V \neq 0$, *então* V *contém um autovetor comum a todos os endomorfismos em* $\mathfrak{g}$.

Esboço da prova. Usemos indução sobre $\dim \mathfrak{g}$, sendo $\dim \mathfrak{g} = 0$ um caso óbvio. Devemos encontrar um ideal K de $\mathfrak{g}$ de codimensão 1 e mostrar, por indução, que existem autovetores comuns a todos os elementos de K. Verifiquemos que $\mathfrak{g}$ estabiliza o subespaço formado por tais autovetores e, finalmente, encontremos nesse espaço um autovetor $z \in \mathfrak{g}$ tal que $\mathfrak{g} = K + Fz$. ■

Temos ainda um importante colorário:

Corolário 27 *Se* $\mathfrak{g}$ *é uma álgebra de Lie solúvel então* $[\mathfrak{g}\mathfrak{g}]$ *é nilpotente (em particular, todo elemento de* $[\mathfrak{g}\mathfrak{g}]$ *é* ad-*nilpotente).*

Esboço da prova. Devemos mostrar que as matrizes de $\operatorname{ad} \mathfrak{g}$ estão em $\mathfrak{t}(n, F)$. Logo as matrizes de $[\operatorname{ad} \mathfrak{g}, \operatorname{ad} \mathfrak{g}] = \operatorname{ad}[\mathfrak{g}\mathfrak{g}]$ estão em $\mathfrak{n}(n, F)$, a álgebra derivada de $\mathfrak{t}(n, F)$. Em particular, $\operatorname{ad}_{\mathfrak{g}} x$ é nilpotente para todo $x \in [\mathfrak{g}\mathfrak{g}]$. A nilpotência segue do Teorema de Engel. ■

2.2.1 A decomposição de Jordan-Chevalley

Momentaneamente, permitiremos que F tenha característica arbitrária, mas exigiremos que F seja algebricamente fechado.

Recordamos da Álgebra Linear a Decomposição de Jordan: num espaço vetorial de dimensão finita sobre um corpo algebricamente fechado, todo endomorfismo se decompõe na soma de um endomorfismo diagonal com um endomorfismo nilpotente comutando entre si. No caso das álgebras de Lie, é útil tornar esta decomposição ainda mais precisa.

Um elemento $x \in \operatorname{End} V$ (V de dimensão finita) é dito *semisimples* se as raízes de seu polinômio minimal forem todas distintas. Equivalentemente, x é semisimples se, e só se, x é diagonalizável. Um resultado clássico da Álgebra Linear nos diz que dois endomorfismos diagonalizáveis comutando entre si são simultaneamente diagonalizáveis (numa base comum).

Portanto, sua soma ou diferença é ainda semisimples. Além disso, se x é semisimples e fixa um subespaço W de V, então a restrição de x a W é obviamente semisimples.

Proposição 28 *Sejam V um espaço vetorial de dimensão finita sobre F e $x \in \operatorname{End} V$.*

(a) Existem únicos x_s e $y_s \in \operatorname{End} V$ satisfazendo as condições $x = x_s + x_n$, x_s semisimples, x_n nilpotente, x_x e x_n comutam entre si.

(b) Existem polinômios $p(X)$ e $q(X)$ em uma indeterminada, sem termo constante, tais que $x_s = p(x)$ e $x_n = q(x)$. Em particular, x_s e x_n comutam com qualquer endomorfismo que comute com x.

(c) Se $A \subset B \subset V$ são subespaços, e x leva B em A, então x_s e x_n também levam B em A.

A decomposição $x = x_s + x_n$ é chamada *decomposição de Jordan-Chevalley* de x, ou simplesmente decomposição de Jordan. Os endomorfismos x_s e x_n são chamados respectivamente *parte semisimples* e *parte nilpotente* de x.

Prova. Sejam $a_1, \ldots, a_k$ os autovalores de x, $\prod_{i=1}^{k}(X - a_i)^{m_i}$ seu polinômio característico, e $V_i = \operatorname{Ker}(x - a_i 1)^{m_i}$. Então cada V_i é estável sob x, $V = \bigoplus V_i$, e a restrição de x a V_i tem polinômio característico $(X - a_i)^{m_i}$. Uma vez que os fatores $(X - a_i)^{m_i}$ são primos entre si, o Teorema Chinês do Resto garante-nos a existência de um polinômio $p(X)$ satisfazendo às congruências

$$\begin{aligned} p(X) &\equiv a_i \bmod (X - a_i)^{m_i}, \quad i = 1, \ldots, k \\ p(X) &\equiv 0 \bmod X. \end{aligned}$$

Esta última congruência é redundante quando algum dos autovalores de x for nulo, mas deve ser acrescentada para garantir que $p(X)$ tenha termo constante nulo. Sejam $q(X) = X - p(X)$, $x_s = p(x)$, e $x_n = q(x)$. Como $p(X)$ e $q(X)$ são polinômios em x, então x_s e x_n comutam entre si, e comutam também com qualquer endomorfismo que comute com x. Ademais, x_s e x_n estabilizam qualquer subespaço de V estável sob x, particularmente, os subespaços V_i, e x_s age diagonalmente sobre V_i com constante a_i. Por definição, $x_n = x - x_s$, deixando claro que x_n é nilpotente (os autovalores de $x - x_s$ são todos nulos). O item (c) deve estar claro, uma vez que $p(X)$ e $q(X)$ tem termo constante nulo.

Resta apenas provar a unicidade da decomposição (item (a)). Seja $x = s + n$ outra tal decomposição. Então temos $x_s - s = n - x_n$. Ora, o lado direito desta igualdade é nilpotente, enquanto que o lado esquerdo é semisimples (s, n, x_s, e x_n comutam entre si pois são polinômios em x), portanto deve ser identicamente nula, isto é, devemos ter $x_s = s$ e $x_n = n$. ∎

Vimos no Lema 23 que se $x \in \mathfrak{gl}(V)$ é nilpotente então x é ad-nilpotente. Usando a Proposição 28 podemos provar por um cálculo direto (cf. Humphreys [Hu, §4.2]) que se x é semisimples então x é ad-*semisimples*.

Lema 29 *Sejam* $x \in \operatorname{End} V$ *(*$\dim V$ *finita), e* $x = x_s + x_n$ *sua decomposição de Jordan. Então* $\operatorname{ad} x = \operatorname{ad} x_s + \operatorname{ad} x_n$ *é a decomposição de Jordan de* $\operatorname{ad} x$ *em* $\mathfrak{gl}(\operatorname{End} V)$*. Em outras palavras, a representação adjunta preserva a decomposição de Jordan.*

Prova. Claramente, $\operatorname{ad} x_s$ e $\operatorname{ad} x_n$ são respectivamente semisimples e nilpotente, e comutam entre si, pois $[\operatorname{ad} x_s, \operatorname{ad} x_n] = \operatorname{ad}[x_s x_n] = 0$. ∎

2.2.2 A forma de Killing

A definição de semisimplicidade para álgebras de Lie, apesar de não muito sofisticada, dificilmente é aplicada na prática, pois pode não ser fácil encontrar $\operatorname{Rad} \mathfrak{g}$ para uma particular álgebra $\mathfrak{g}$. Precisamos de um instrumento melhor, que nos permita investigar a semisimplicidade realizando uma verificação simples sobre alguns elementos de $\mathfrak{g}$. Como veremos, esse instrumento é a *Forma de Killing*, definida por $\kappa(x, y) = \operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y)$, com x e y varrendo $\mathfrak{g}$. Esta é claramente bilinear e associativa em relação ao comutador:

$$
\begin{aligned}
\kappa([xy], z) &= \operatorname{Tr}(\operatorname{ad}[xy] \operatorname{ad} z) \\
&= \operatorname{Tr}([\operatorname{ad} x \operatorname{ad} y] \operatorname{ad} z) \\
&= \operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y \operatorname{ad} z) - \operatorname{Tr}(\operatorname{ad} y \operatorname{ad} x \operatorname{ad} z) \\
&= \operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y \operatorname{ad} z) - \operatorname{Tr}(\operatorname{ad} x \operatorname{ad} z \operatorname{ad} y) \\
&= \operatorname{Tr}(\operatorname{ad} x [\operatorname{ad} y \operatorname{ad} z]) = \kappa(x, [yz]),
\end{aligned}
$$

para todo $x, y, z \in \mathfrak{g}$.

Iniciemos com uma propriedade functorial muito útil da forma de Killing.

Lema 30 *Se I é um ideal de $\mathfrak{g}$, κ é a forma de Killing de $\mathfrak{g}$, e κ_I é a forma de Killing de I (visto como álgebra de Lie), então $\kappa_I = \kappa|_{I\times I}$.*

Prova. Com efeito, se W é um subespaço de um espaço vetorial de dimensão finita V e φ é um endomorfismo de V levando V em W, então $\operatorname{Tr}\varphi = \operatorname{Tr}(\varphi|_W)$. Para todo $x, y \in I$, $\operatorname{ad} x \operatorname{ad} y$ é um endomorfismo de $\mathfrak{g}$ que leva $\mathfrak{g}$ em I, logo, seu traço $\kappa(x, y)$ coincide com o traço $\kappa_I(x, y)$ de $(\operatorname{ad} x \operatorname{ad} y)|_I = \operatorname{ad}_I x \operatorname{ad}_I y$. ∎

O *radical* de uma forma bilinear simétrica $\omega(x, y)$ é definido pelo conjunto

$$S = \{x \in \mathfrak{g} : \omega(x, y) = 0, \text{ para todo } y \in \mathfrak{g}\}.$$

Este é claramente um subespaço de $\mathfrak{g}$. Dizemos que ω é *não-degenerada* se $S = 0$. Para testar a não-degenerescência, basta calcular o determinante da matriz associada a ω em relação a uma base fixa de $\mathfrak{g}$. Temos que ω é não-degenerada se, e só se, esse determinante é não-nulo.

Devido à associatividade, o radical da forma de Killing é mais do que meramente um subespaço, é um ideal de $\mathfrak{g}$. Efetivamente, se R é o radical de κ, $x, z \in \mathfrak{g}$, e $y \in R$, então $\kappa([xy], z) = -\kappa(y, [xz]) = 0$ e, conseqüentemente, $[xy] \in R$.

Exemplo 31 Vamos calcular a forma de Killing para $\mathfrak{sl}(2, F)$, usando a base canônica $\{x, h, y\}$. Do Exemplo 11, temos que as matrizes das representações adjuntas de x, h, y, são respectivamente

$$\operatorname{ad} x = \begin{pmatrix} 0 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad \operatorname{ad} h = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad \operatorname{ad} y = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

Portanto, a matriz de κ é $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 8 & 0 \\ 4 & 0 & 0 \end{pmatrix}$, cujo determinante é -128, e κ é não-degenerada (desde que $\mathrm{Car}\, F \neq 2$). Para ilustrar, vamos calcular o elemento $\kappa(h,h)$:

$$\begin{aligned}\kappa(h,h) &= \mathrm{Tr}(\mathrm{ad}\, h \,\mathrm{ad}\, h)\\ &= \mathrm{Tr}\begin{pmatrix} 4 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 4\end{pmatrix} = 8.\end{aligned}$$

□

Teorema 32 (Critério de Semisimplicidade) *Seja $\mathfrak{g}$ uma álgebra de Lie. Então $\mathfrak{g}$ é semisimples se, e só se, sua forma de Killing for não-degenerada.*

Para provar este resultado necessitaremos de um critério de solubilidade que não estudaremos em detalhe aqui. Trata-se do Critério de Cartan (cf. Humphreys [Hu, §4.3]) cujo enunciado encontra-se expresso pelo seguinte teorema.

Teorema 33 (Critério de Cartan) *Seja $\mathfrak{g}$ uma subálgebra de $\mathfrak{gl}(V)$, para V um espaço vetorial de dimensão finita sobre F. Definimos em $\mathfrak{g}$ uma forma bilinear $\omega(x,y) = \mathrm{Tr}(xy)$, com radical S. Se $[\mathfrak{g}\mathfrak{g}] \subset S$ então $\mathfrak{g}$ é solúvel.*

Corolário 34 *Seja $\mathfrak{g}$ uma álgebra de Lie e κ sua forma de Killing. Se $[\mathfrak{g}\mathfrak{g}]$ está contida no radical de κ então $\mathfrak{g}$ é solúvel.*

Prova. Pelo teorema, $\mathrm{ad}\,\mathfrak{g}$ é solúvel. Como $\mathrm{Ker}\,\mathrm{ad} = Z(\mathfrak{g})$ também é solúvel, e $\mathrm{ad}\,\mathfrak{g} \cong \mathfrak{g}/Z(\mathfrak{g})$ então $\mathfrak{g}$ é solúvel. ■

Prova do Critério de Semisimplicidade. De acordo com o Critério de Cartan $\mathrm{ad}_{\mathfrak{g}} S$ é solúvel. Suponhamos que $\mathrm{Rad}\,\mathfrak{g} = 0$ (logo $Z(\mathfrak{g}) = 0$). Então $S \cong \mathrm{ad}_{\mathfrak{g}} S$ é solúvel, logo $S \subset \mathrm{Rad}\,\mathfrak{g} = 0$ e, conseqüentemete, κ é não-degenerada.

Por outro lado, se I é um ideal abeliano de $\mathfrak{g}$, $x \in I$, $y \in \mathfrak{g}$, então $\mathrm{ad}\, x \,\mathrm{ad}\, y$ leva $\mathfrak{g}$ em I, $(\mathrm{ad}\, x \,\mathrm{ad}\, y)^2$ leva $\mathfrak{g}$ em $[II] = 0$, ou seja, $\mathrm{ad}\, x \,\mathrm{ad}\, y$ é nilpotente. Conseqüentemente $\kappa(x,y) = \mathrm{Tr}(\mathrm{ad}\, x \,\mathrm{ad}\, y) = 0$, e $I \subset S$. Se κ é não-degenerada (i.é, $S = 0$), então $\mathfrak{g}$ não contém nenhum ideal abeliano não-nulo, logo $\mathfrak{g}$ é semisimples. ■

Vejamos agora um resultado que torna mais precisa a caracterização de uma álgebra de Lie semisimples e seus ideais.

Teorema 35 *Seja $\mathfrak{g}$ uma álgebra de Lie semisimples. Então existem (finitos) ideais simples $\mathfrak{g}_1, \ldots, \mathfrak{g}_t$ de $\mathfrak{g}$ tais que $\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_t$ e todo ideal simples de $\mathfrak{g}$ coincide com algum dos $\mathfrak{g}_i$.*

Prova. Inicialmente, consideramos I um ideal arbitrário de $\mathfrak{g}$ e definimos $I^\perp = \{x \in \mathfrak{g} : \kappa(x, y) = 0$, para todo $y \in I\}$. Como κ é associativa, $I^\perp$ é um ideal de $\mathfrak{g}$. O Critério de Cartan aplicado à álgebra de Lie I revela que o ideal $I \cap I^\perp$ é solúvel, logo 0. Portanto, devemos ter $\mathfrak{g} = I \oplus I^\perp$.

Em seguida, usamos indução sobre $\dim \mathfrak{g}$ para obter a decomposição desejada. Se $\mathfrak{g}$ não é simples, então $\mathfrak{g}$ contém um ideal minimal não-nulo $\mathfrak{g}_1$, de modo que $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_1^\perp$. Em particular, qualquer ideal de $\mathfrak{g}_1$ é também ideal de $\mathfrak{g}$, donde $\mathfrak{g}_1$ é simples (pela minimalidade). Pelo mesmo motivo, $\mathfrak{g}_1^\perp$ é semisimples e por hipótese de indução $\mathfrak{g}_1^\perp$ se decompõe numa soma direta de ideais simples, os quais são também ideais de $\mathfrak{g}$.

Resta-nos provar a unicidade dessa decomposição. Se I é qualquer ideal simples de $\mathfrak{g}$, então $[I\mathfrak{g}]$ é também ideal de $\mathfrak{g}$, e é não-nulo, já que $Z(\mathfrak{g}) = 0$. Isto obriga $[I\mathfrak{g}] = I$. Por outro lado, $[I\mathfrak{g}] = [I\mathfrak{g}_1] \oplus \cdots \oplus [I\mathfrak{g}_t]$, donde uma única destas parcelas deve ser não-nula, digamos $I = [I\mathfrak{g}_i]$. Então $0 \neq I \subset \mathfrak{g}_i$ e, portanto, $I = \mathfrak{g}_i$ (já que $\mathfrak{g}_i$ é simples). ∎

Corolário 36 *Se $\mathfrak{g}$ é semisimples, então $\mathfrak{g} = [\mathfrak{g}\mathfrak{g}]$ e todos os ideais e imagens homomórficas de $\mathfrak{g}$ são semisimples (ou 0). Além disso, cada ideal de $\mathfrak{g}$ é soma direta de ideais simples de $\mathfrak{g}$.*

Prova. O quociente $\mathfrak{g}/[\mathfrak{g}\mathfrak{g}]$ é simultaneamente abeliano e semisimples (como imagem homomórfica de $\mathfrak{g}$), logo, deve ser nulo, isto é $\mathfrak{g} = [\mathfrak{g}\mathfrak{g}]$. ∎

2.2.3 A decomposição de Jordan abstrata

Por construção, a decomposição de Jordan-Chevalley vista na subseção 2.2.1 aplica-se apenas ao caso $\mathfrak{g} \subset \mathfrak{gl}(V)$, para um espaço vetorial V de dimensão finita. Contudo, é útil estender este conceito para as álgebras de Lie abstratas. Como veremos a seguir, isto será possível quando $\mathfrak{g}$ for semisimples de dimensão finita. Primeiramente, necessitamos de um fato geral sobre F-álgebras associativas.

Proposição 37 *Seja $\mathfrak{U}$ uma F-álgebra de dimensão finita. Então* $\operatorname{Der}\mathfrak{U}$ *contém as partes semisimples e nilpotente de todos os seus elementos.*

Prova. Seja $\delta = \sigma + \nu \in \operatorname{Der}\mathfrak{U}$, onde $\sigma \in \operatorname{End}\mathfrak{U}$ é a parte semisimples e $\nu \in \operatorname{End}\mathfrak{U}$ é a parte nilpotente de δ. Basta mostrar que $\sigma \in \operatorname{Der}\mathfrak{U}$. Por um lado, $\mathfrak{U}$ é a soma direta dos subespaços $\mathfrak{U}_a = \{x \in \mathfrak{U} : (\delta - a)^k x = 0$, para algum k dependendo de $x\}$, $a \in F$, os quais são nulos quase sempre (a soma é finita), e δ age sobre $\mathfrak{U}_a$ como multiplicação pelo escalar a. Por outro lado, um simples argumento de indução nos permite verificar a fórmula

$$(\delta - (a+b)\cdot 1)^n(xy) = \sum_{i=0}^{n} \binom{n}{i} ((\delta - a\cdot 1)^{n-i}x)((\delta - b\cdot 1)^i y)$$

para todo $x, y \in \mathfrak{U}$. Por definição, se $x \in \mathfrak{U}_a$ temos que $(\delta - a\cdot 1)^k x = 0$ para algum k. Também, se $y \in \mathfrak{U}_b$ então $(\delta - b\cdot 1)^l y = 0$, para algum l. Assim sendo, tomando $n = k + l$ e aplicando a fórmula acima obtemos $(\delta - (a+b)\cdot 1)^n(xy) = 0$, isto é, $xy \in \mathfrak{U}_{a+b}$. Desse modo, $\sigma(xy) = (a+b)xy$. Por outro lado, $x(\sigma y) + (\sigma x)y = (a+b)xy$. Como a soma $\mathfrak{U} = \bigoplus \mathfrak{U}_a$ é direta, temos que $\sigma(xy) = x(\sigma y) + (\sigma x)y$, $\forall x, y \in \mathfrak{U}$, como requerido. ∎

Vamos agora mostrar que $\operatorname{ad}\mathfrak{g}$ é de fato um ideal de $\operatorname{Der}\mathfrak{g}$, para $\mathfrak{g}$ uma álgebra de Lie. Com efeito, para todo $\delta \in \operatorname{Der}\mathfrak{g}$ e todo $x, y \in \mathfrak{g}$, temos

$$\begin{aligned}
[\delta, \operatorname{ad} x](y) &= \delta \operatorname{ad} x(y) - \operatorname{ad} x(\delta y) \\
&= \delta([xy]) - [x, \delta y] \\
&= [x, \delta y] + [\delta x, y] - [x, \delta y] \\
&= [\delta x, y] = \operatorname{ad}(\delta x)(y),
\end{aligned}$$

isto é, $[\delta, \operatorname{ad} x] = \operatorname{ad}(\delta x) \in \operatorname{ad}\mathfrak{g}$.

Uma importante conseqüência deste fato e da não-degenerescência da forma de Killing é o seguinte teorema.

Teorema 38 *Se $\mathfrak{g}$ é semisimples, então* $\operatorname{ad}\mathfrak{g} = \operatorname{Der}\mathfrak{g}$*, isto é, toda derivação de $\mathfrak{g}$ é interna.*

Prova. Como $\mathfrak{g}$ é semisimples, temos $\mathfrak{g} \cong \operatorname{ad}\mathfrak{g}$, e $M = \operatorname{ad}\mathfrak{g}$ tem forma de Killing κ_M não-degenerada. Ademais, M é um ideal de $D = \operatorname{Der}\mathfrak{g}$, logo $\kappa_M = \kappa_D|_{M\times M}$.

Se $M^\perp = \{\delta \in D : \kappa_D(\delta, \operatorname{ad} x) = 0 : \forall x \in \mathfrak{g}\}$ é o subespaço de D ortogonal a M, então, $D = M \oplus M^\perp$, pois κ_M é não-degenerada. Mas, como M e $M^\perp$ são ambos ideais de D (κ_D é associativa), segue que $[M, M^\perp] = 0$.

Finalmente, se $\delta \in M^\perp$, então $\operatorname{ad}(\delta x) = [\delta, \operatorname{ad} x] = 0$ ($\forall x \in \mathfrak{g}$), e conseqüentemente $\delta = 0$ (pela injetividade de ad). ■

Este resultado nos permite introduzir uma "decomposição" de Jordan numa álgebra de Lie semisimples arbitrária $\mathfrak{g}$, denominada *Decomposição de Jordan Abstrata*. Como $\mathfrak{g} \cong \operatorname{ad} \mathfrak{g} = \operatorname{Der} \mathfrak{g}$, e $\operatorname{Der} \mathfrak{g}$ contém as partes semisimples e nilpotente de todos os seus elementos, cada $x \in \mathfrak{g}$, determina (em vista da injetividade de ad) únicos elementos $s, n \in \mathfrak{g}$, tais que $\operatorname{ad} x = \operatorname{ad} s + \operatorname{ad} n$ é a decomposição de Jordan usual de $\operatorname{ad} x$. Portanto, $x = s + n$, onde s é ad-semisimples, n é ad-nilpotente e $[sn] = 0$. Escrevemos $s = x_s$ e $n = x_n$, chamando-as, por abuso de linguagem, parte semisimples e parte nilpotente de x, respectivamente.

Para concluir esta subseção, vale notar que se $\mathfrak{g}$ é uma álgebra de Lie linear semisimples, ambas as decomposições de Jordan coincidem, o que justifica a notação acima. Isto será mostrado no Teorema 51.

2.3 Grupos e Álgebras de Lie

Os grupos de Lie constituem um assunto particularmente rico e de grande interesse na Matemática contemporânea. São objetos com propriedades algébricas (vistos como grupos), topológicas (vistos como espaços topológicos) e geométricas (vistos como variedades) fortemente inter-relacionadas, formando uma área de confluência entre a Álgebra, a Topologia e a Geometria.

Um objeto algébrico tem papel fundamental na compreensão destes aspectos, quando considerados isoladamente, ou coletivamente: as álgebras de Lie. Ao associar, de maneira bastante natural, uma álgebra de Lie a um grupo de Lie e vice-versa, ocorre que a estrutura da álgebra de Lie embute substanciais informações a respeito das propriedades do grupo de Lie subjacente. De fato, quase toda a geometria do grupo encontra-se lá engendrada. Esta transição é interessante, pois elimina toda eventual complicação topológica que o grupo possa ter, "linearizando-o". Isto representa uma grande simplificação, já que podemos nos beneficiar da teoria de classificação das álgebras de Lie, a qual, como veremos abaixo, encontra-se em estágio bastante avançado.

De fato, as álgebras de Lie semisimples de dimensão finita sobre corpos de característica 0 encontram-se completamente classificadas.

Nosso objetivo aqui é apenas dar uma ideia básica acerca dos grupos de Lie e destacar sua relação com as álgebras de Lie. Em particular, veremos como as representações de grupos de Lie induzem representações de álgebras de Lie.

2.3.1 Definição e exemplos

Definição 39 (Grupo de Lie) *Um* grupo de Lie *é um conjunto G dotado simultaneamente de uma estrutura algébrica de grupo e de variedade C^∞ compatíveis entre si, isto é, as aplicações de multiplicação e de inversão que dão a G uma estrutura de grupo,*

$$\cdot : G \times G \to G$$

e

$$\iota : G \to G,$$

são aplicações infinitamente diferenciáveis.

Um *homomorfismo entre grupos de Lie G* e H é uma aplicação $\varphi : G \to H$ que é simultaneamente diferenciável e homomorfismo de grupos. Um *endomorfismo* de G é um homomorfismo de G em G e um *automorfismo* é um endomorfismo bijetor. Os conjuntos de todas estas aplicações são denotados respectivamente por $\mathrm{Hom}(G, H)$, $\mathrm{End}(G)$ e $\mathrm{Aut}(G)$.

Em geral, quando dizemos que G é abeliano, estamos nos referindo à estrutura algébrica subjacente de G e quando dizemos que G é conexo, estamos nos referindo à sua estrutura de variedade. Por via de regra, qualificativos atribuídos a G se referem sempre a uma ou outra das estruturas subjacentes de G, sem que haja ambigüidades.

Um *subgrupo H* de um grupo de Lie G é um subconjunto H que é simultaneamente um subgrupo, no sentido estritamente algébrico, e uma subvariedade fechada de G. Esta é uma área de potencial confusão, onde o atributo "fechado" aparece de maneira crucial (cf. Fulton [FH, §7.1]).

Definimos, de maneira completamente análoga, um *grupo de Lie complexo* substituindo o conceito de variedade diferenciável pelo conceito de variedade complexa. Definimos, também, um *grupo de Lie algébrico* a partir do conceito de variedade algébrica.

Exemplo 40 (Grupo Geral Linear) O grupo geral linear $\mathrm{GL}(n, \mathbb{R})$ das matrizes reais $n \times n$ inversíveis é um subconjunto aberto do conjunto das matrizes $n \times n$ dotado de estrutura de variedade tal que as entradas de uma matriz são coordenadas em $\mathrm{GL}(n, \mathbb{R})$. A diferenciabilidade da multiplicação

$$\mathrm{GL}(n, \mathbb{R}) \times \mathrm{GL}(n, \mathbb{R}) \to \mathrm{GL}(n, \mathbb{R})$$

decorre da diferenciabilidade da multiplicação em $\mathbb{R}$. A diferenciabilidade da inversão ι : $\mathrm{GL}(n, \mathbb{R}) \to \mathrm{GL}(n, \mathbb{R})$ decorre da regra de Cramer para a inversa de uma matriz. Ocasionalmente, $\mathrm{GL}(n, \mathbb{R})$ aparece como o grupo dos automorfismos de um espaço vetorial V de dimensão n. Quando não desejamos fazer menção explícita às bases de V, denotamos $\mathrm{GL}(n, \mathbb{R})$ por $\mathrm{GL}(V)$ ou $\mathrm{Aut}(V)$. Muitos grupos de Lie têm origem como subgrupos de $\mathrm{GL}(n, \mathbb{R})$. Alguns exemplos são dados abaixo. $\square$

Como na Teoria de Grupos, um homomorfismo de grupos de Lie $\varphi : G \to \mathrm{GL}(V)$ é dito ser uma *representação* de G e V é dito *G-espaço*. Neste caso é usual denotar-se $\varphi(g)(v)$ por $g \cdot v$.

Exemplo 41 (Grupo Especial Linear) O *grupo especial linear* $\mathrm{SL}(n, \mathbb{R})$ dos automorfismos de $\mathbb{R}^n$ com com determinante 1. $\square$

Exemplo 42 O grupo B_n das matrizes triangulares superiores (o grupo dos automorfismos x de $\mathbb{R}^n$ estabilizando uma *bandeira*, i.é, uma seqüência de subespaços $0 = V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$, tais que, $\dim V_i = i$ *e* $x(V_i) \subset V_i$). $\square$

Exemplo 43 Alguns grupos Lie são obtidos como grupos de automorfismos $A : \mathbb{R}^n \to \mathbb{R}^n$, de determinante 1, conservando alguma forma bilinear $Q : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, isto é, $Q(Av, Aw) = Q(v, w)$ para todo $v, w \in \mathbb{R}^n$. O *grupo especial ortogonal* $\mathrm{SO}(n, \mathbb{R})$ tem origem quando Q é simétrica definida positiva. Se Q é simétrica, não-degenerada e indefinida, i.é, Q tem k autovalores positivos e l autovalores negativos, obtemos o grupo $\mathrm{SO}(k, l, \mathbb{R})$. Observemos que $\mathrm{SO}(k, l, \mathbb{R}) \simeq \mathrm{SO}(l, k, \mathbb{R})$. Se Q é anti-simétrica e não-degenerada (neste caso n deve ser par) obtemos o *grupo simplético* $\mathrm{Sp}(n, \mathbb{R})$.

É fácil escrever as equações matriciais que definem esses grupos. Se M é a matriz associada à forma bilinear Q, então

$$Q(v, w) = v^t M w,$$

para todo $v, w \in \mathbb{R}^n$. A condição da definição,

$$Q(Av, Aw) = Q(v, w),$$

torna-se

$$v^t A^t M A w = v^t M w.$$

Conseqüentemente,

$$A^t M A = M.$$

Pode-se mostrar que, no caso de $\mathrm{Sp}(2n, \mathbb{R})$, a condição determinante 1 é redundante, e que $\mathrm{SO}(k, l, \mathbb{R})$ tem duas componentes conexas se, e só se, k e l são ambos positivos. $\square$

2.3.2 A álgebra de Lie $\mathfrak{g}$ de um grupo de Lie G.

Os grupos de Lie, em geral, envolvem diversas complicações, como a não-enumerabilidade de seus elementos, por exemplo. Isto torna praticamente irrelevante a noção de geradores e relações. Felizmente, porém, há certas propriedades muito boas para auxiliar-nos no estudo desses grupos e suas representações. Muito do que acontece com um grupo de Lie está determinado pelo que acontece dentro de uma vizinhança (um subconjunto aberto) da unidade e. E mais, há uma ferramenta notável da qual podemos nos valer: as álgebras de Lie. Para começar, enunciamos a seguinte proposição.

Proposição 44 (Schreier) *Seja G um grupo de Lie conexo e U uma vizinhança qualquer da unidade e de G. Então U gera G.*

Prova. Consideremos o subgrupo H de G gerado por U. Então H é um subconjunto fechado de G, assim como são fechadas as classes de equivalência gH para todo $g \in G$ (a translação $h \mapsto gh$ por um elemento fixo $g \in G$ é um difeomorfismo de G). Mas, H é o complementar em

G do subconjunto fechado

$$\bigcup_{g \notin H} gH,$$

sendo, portanto, um subconjunto aberto de G. Como G é conexo devemos ter $G = H$. ∎

Esta proposição afirma que se $\varphi : G \to H$ é um homomorfismo de grupos de Lie conexos, então φ está completamente determinada por seu comportamento em uma vizinhança qualquer U da unidade $e \in G$. De fato, pode-se afirmar ainda que φ é unicamente determinada por sua diferencial $d\varphi_e : T_eG \to T_eH$ onde T_eG é o espaço tangente a G pela unidade e (cf. Fulton [FH, prop. 8.33]). Esta é uma situação excelente. Podemos descrever completamente um homomorfismo de grupos de Lie φ que, em geral, é bastante complicado estudando apenas uma transformação linear $d\varphi_e$ entre espaços vetoriais.

Consideremos a ação por conjugação de um grupo de Lie G sobre si mesmo, isto é, para cada $g \in G$ definimos a aplicação

$$\begin{array}{rcl} \Phi_g : G & \to & G \\ h & \mapsto & ghg^{-1} \end{array}$$

a qual é claramente um automorfismo de G. A diferencial desta aplicação avaliada na unidade e nos permite definir um importante homomorfismo,

$$\mathrm{Ad} : G \to \mathrm{Aut}(T_eG)$$

por

$$\mathrm{Ad}(g) = (d\Phi_g)_e : T_eG \to T_eG,$$

chamado *representação adjunta* de G.

Observamos que $\mathrm{Aut}(T_eG)$ é um subconjunto aberto do espaço vetorial dos endomorfismos de T_eG, de modo que, seu espaço tangente $T_e(\mathrm{Aut}(T_eG))$ se identifica naturalmente a $\mathrm{End}(T_eG)$. Desse modo, tomando a diferencial da representação adjunta calculada na unidade, obtemos uma aplicação linear

$$\mathrm{ad} = d(\mathrm{Ad})_e : T_eG \to \mathrm{End}(T_eG).$$

Esta, por sua vez, permite definir uma operação colchete

$$[\ ,\ ] : T_eG \times T_eG \to T_eG$$

por $[xy] = \mathrm{ad}(x)(y)$, para todo $x, y \in T_eG$.

Pode-se mostrar (cf. Fulton [FH, §8.1]) que T_eG com a operação colchete assim definida é uma álgebra de Lie, isto é, a operação colchete satisfaz as condições (L1)-(L3) da definição de álgebra de Lie. Além disso, para o caso particular $G = \mathrm{GL}(n, \mathbb{R})$, o espaço tangente T_eG se identifica a $\mathrm{End}\,\mathbb{R}^n = M_n(\mathbb{R})$, e obtemos explicitamente $[xy] = xy - yx$. Isto justifica a denotação do comutador acima. O mesmo se diga dos grupos de Lie que se originam como subgrupos de $\mathrm{GL}(n, \mathbb{R})$. Com esta estrutura de álgebra de Lie, T_eG é dito ser a álgebra de Lie do grupo G, denotado por $\mathfrak{g}$.

2.4 Módulos e o Teorema de Weyl

Nesta seção, $\mathfrak{g}$ é uma álgebra de Lie semisimples sobre um corpo arbitrário F. Para a maioria dos resultados apresentados, F é um corpo arbitrário. Entretanto, para os resultados envolvendo a decomposição de Jordan de um elemento $x \in \mathfrak{g}$ precisaremos que F seja algebricamente fechado (para podermos contar com os autovalores). Nosso objetivo principal é enunciar o Teorema de Weyl sobre a redutibilidade completa das representações de álgebras de Lie semisimples. Como importante corolário, obteremos a conservação da decomposição de Jordan por representações de $\mathfrak{g}$. Ao mesmo tempo, introduziremos alguma terminologia de utilidade posterior.

2.4.1 Definição e exemplos

Definição 45 (Ação de álgebra de Lie) *Seja V um espaço vetorial sobre F. A* ação *de uma álgebra de Lie $\mathfrak{g}$ sobre V é uma aplicação linear $\phi : \mathfrak{g} \otimes V \to V$ satisfazendo a condição*

$$\begin{aligned} \phi([xy] \otimes v) &= \phi(x \otimes \phi(y \otimes v)) - \phi(y \otimes \phi(x \otimes v)) \\ &= \phi(\mathrm{id} \otimes \phi)((x \otimes y - y \otimes x) \otimes v) \end{aligned} \tag{2.2}$$

para todo $x, y \in \mathfrak{g}$, e todo $v \in V$.

Denotaremos $\phi(x \otimes v)$ simplesmente por $x \cdot v$. Notemos que, em contraste com o que acontece com as álgebras associativas, não definimos ação lateral, pois $\mathfrak{g}$ não é associativa.

Definição 46 (Módulo) *Um* $\mathfrak{g}$-módulo *é um par* (V, ϕ) *consistindo de um espaço vetorial* V *sobre* F *e de uma ação* ϕ *de* $\mathfrak{g}$ *sobre* V.

Para fixar melhor as idéias e a notação acima, (V, ϕ) é um $\mathfrak{g}$-módulo, se, e só se, para todo $x, y \in \mathfrak{g}$ e todo $v \in V$, tivermos satisfeitas as seguintes condições:

(M1) $(ax + by) \cdot v = a(x \cdot v) + b(y \cdot v)$,

(M2) $x \cdot (av + bw) = a(x \cdot v) + b(x \cdot w)$,

(M3) $[xy] \cdot v = x \cdot y \cdot v - y \cdot x \cdot v$,

onde a condição (M3) é equivalente à condição (2.2) da definição de ação.

Se $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ é uma representação de $\mathfrak{g}$, então a aplicação $\phi : \mathfrak{g} \otimes V \to V$ dada por $x \otimes v \mapsto \varphi(x)(v)$ define uma ação de $\mathfrak{g}$ sobre V. Basta-nos verificar que ϕ satisfaz a condição (M3):

$$\begin{aligned}
\phi([xy] \otimes v) &= \varphi([xy])(v) \\
&= [\varphi(x)\varphi(y)](v) \\
&= \varphi(x)\varphi(y)(v) - \varphi(y)\varphi(x)(v) \\
&= \varphi(x)(\phi(y \otimes v)) - \varphi(y)(\phi(x \otimes y)) \\
&= \phi(x \otimes \phi(y \otimes v)) - \phi(y \otimes \phi(x \otimes v)).
\end{aligned}$$

Por outro lado, se $\phi : \mathfrak{g} \otimes V \to V$ é uma ação de $\mathfrak{g}$ sobre V, então para cada $x \in \mathfrak{g}$, a aplicação $v \mapsto \phi(x \otimes v)$ define um endomorfismo ρ_x de V, de modo que, a aplicação $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ dada por $x \mapsto \rho_x$ é uma representação de $\mathfrak{g}$. Precisamos apenas verificar que φ é um homomorfismo de álgebras de Lie. Com efeito,

$$\begin{aligned}
\varphi([xy])(v) &= \rho_{[xy]}(v) \\
&= \phi([xy] \otimes v)
\end{aligned}$$

$$\begin{aligned}
&= \phi(x \otimes \phi(y \otimes v)) - \phi(y \otimes \phi(x \otimes v)) \\
&= \phi(x \otimes \rho_y(v)) - \phi(y \otimes \rho_x(v)) \\
&= \rho_x(\rho_y(v)) - \rho_y(\rho_x(v)) \\
&= \varphi(x)\varphi(y)(v) - \varphi(y)\varphi(x)(v) \\
&= [\varphi(x)\varphi(y)](v),
\end{aligned}$$

para todo $v \in V$, donde $\varphi([xy]) = [\varphi(x)\varphi(y)]$, para todo $x, y \in \mathfrak{g}$.

Não havendo confusão, costumamos denotar ρ_x simplesmente por x e assim considerar x como sendo um elemento de $\mathfrak{g}$ ou um endomorfismo de V (via a representação ρ) indistintamente. Além disso, se (V, ϕ) é um $\mathfrak{g}$-módulo, omitimos a ação ϕ, dizendo, por abuso de linguagem, que V é um $\mathfrak{g}$-módulo.

É efetivamente útil interpretar $x \cdot y \cdot v$ como $xy \cdot v$, onde xy é a composição do endomorfismo y com o endomorfismo x, e refrasear a condição (M3) como $[xy] \cdot v = (xy - yx) \cdot v$, onde $xy - yx$ é exatamente o produto de Lie usual de $\mathfrak{gl}(V)$. Isto nos fornece de imediato uma razão para introduzir a condição (M3), a saber, garantir a equivalência entre a linguagem de representações e a linguagem de módulos. Podemos, assim, utilizar uma ou outra linguagem convenientemente.

Definição 47 (Homomorfismo de L-módulos) *Uma aplicação linear $\varphi : V \to W$ entre os $\mathfrak{g}$-módulos V e W é um* homomorfismo de $\mathfrak{g}$-módulos *se o seguinte diagrama é comutativo:*

$$\begin{tikzcd}
V \arrow[r, "\varphi"] \arrow[d, "x"'] & W \arrow[d, "x"] \\
V \arrow[r, "\varphi"] & W
\end{tikzcd}$$

ou equivalentemente, se $\varphi(x \cdot v) = x \cdot \varphi(v)$, para todo $x \in \mathfrak{g}$ e todo $v \in V$. Neste caso, também dizemos que φ é uma aplicação $\mathfrak{g}$-linear.

Um subespaço W de um $\mathfrak{g}$-módulo V é dito $\mathfrak{g}$-*submódulo* se for estável sob a ação de $\mathfrak{g}$ sobre V, ou seja, se satisfizer a condição

$$\{x \cdot w : x \in \mathfrak{g} \text{ e } w \in W\} \subset W.$$

Um $\mathfrak{g}$-módulo $V \neq 0$ que admite apenas os $\mathfrak{g}$-submódulos triviais 0 e V é dito ser *irredutível*. Se um $\mathfrak{g}$-módulo arbitrário V se escreve como soma direta de $\mathfrak{g}$-submódulos irredutíveis então V é dito ser *completamente redutível*.

Claramente, se $\varphi : V \to W$ é $\mathfrak{g}$-linear, então $\operatorname{Ker}\varphi$, $\operatorname{Im}\varphi$ são $\mathfrak{g}$-submódulos de V e W respectivamente. Ademais, se W é um $\mathfrak{g}$-submódulo de V, a ação de $\mathfrak{g}$ sobre V induz, de maneira óbvia, uma ação de $\mathfrak{g}$ sobre o espaço vetorial quociente V/W tornando-o num $\mathfrak{g}$-módulo. A saber, para todo $x \in \mathfrak{g}$ e todo $v \in V$ temos

$$x \cdot \bar{v} = x \cdot (v + W) = (x \cdot v) + W = \overline{x \cdot v},$$

onde $\bar{v}$ denota a classe de equivalência (módulo W) do elemento v. Em particular, valem os três teoremas clássicos de isomorfismos cujos enunciados são idênticos aos que se encontram na subseção 2.1.1.

Se $\{V_i\}_{i\in I}$ é uma família de $\mathfrak{g}$-módulos, então o produto direto $\prod_{i\in I} V_i$ e a soma direta $\bigoplus_{i\in I} V_i$ são $\mathfrak{g}$-módulos com ação de $\mathfrak{g}$ dada respectivamente por $x \cdot \prod_{i\in I} v_i = \prod_{i\in I} x \cdot v_i$, e $x \cdot \bigoplus_{i\in I} v_i = \bigoplus_{i\in I} x \cdot v_i$. Porém, é preciso cuidado ao considerar o produto tensorial $\bigotimes_{i\in I} V_i$. Para isso vamos necessitar do conceito de ação de grupo de Lie.

Suponhamos que G e H sejam um grupos de Lie conexos e simplesmente conexos, e que $\mathfrak{g}$ e $\mathfrak{h}$ sejam suas respectivas álgebras de Lie. Pode-se mostrar (cf. Fulton & Harris [FH, §8.1]) que homomorfismos de grupos de Lie $\varphi : G \to H$ induzem homomorfismos de álgebras de Lie $d\varphi_e : \mathfrak{g} \to \mathfrak{h}$, e que homomorfismos de álgebras de Lie $\psi : \mathfrak{g} \to \mathfrak{h}$ induzem homomorfismos $\varphi : G \to H$ tais que $d\varphi_e = \psi$. Particularmente, $\varphi : G \to \mathrm{GL}(V)$ é uma representação se, e só se, $d\varphi_e : \mathfrak{g} \to \mathfrak{gl}(V)$ o for, ou seja, V é um G-espaço se, e só se, for um $\mathfrak{g}$-módulo.

Agora, já podemos analisar o caso do produto tensorial $V \otimes W$ de dois $\mathfrak{g}$-módulos V e W, visto apenas como espaço vetorial. Se $x \in \mathfrak{g}$ e $\gamma : I \to G$ é um caminho (diferenciável) em G tal que $\gamma(0) = e$ e $\gamma'(0) = x$, temos por definição

$$x \cdot v = \frac{d}{dt}(\gamma(t) \cdot v)\bigg|_{t=0}$$

para todo $v \in V$, e igualmente para todo $w \in W$. Por outro lado, $V \otimes W$ é claramente um G-conjunto com a ação

$$g \cdot (v \otimes w) = (g \cdot v) \otimes (g \cdot w),$$

de modo que, $V \otimes W$ torna-se um $\mathfrak{g}$-módulo com a ação de $\mathfrak{g}$ dada por

$$\begin{aligned} x \cdot (v \otimes w) &= \frac{d}{dt}(\gamma(t) \cdot (v \otimes w))\Big|_{t=0} \\ &= \frac{d}{dt}((\gamma(t) \cdot v) \otimes (\gamma(t) \cdot w)\Big|_{t=0} \\ &= \frac{d}{dt}(\gamma(t) \cdot v)\Big|_{t=0} \otimes w + v \otimes \frac{d}{dt}(\gamma(t) \cdot w)\Big|_{t=0} \\ &= (x \cdot v) \otimes w + v \otimes (x \cdot w). \end{aligned}$$

A partir do argumento acima, concluímos que, se $I = \{1, \ldots, n\}$, então $V_1 \otimes \cdots \otimes V_n$ torna-se um $\mathfrak{g}$-módulo com ação de $\mathfrak{g}$ dada por

$$x \cdot (v_1 \otimes \cdots \otimes v_n) = \sum_{i=1}^{n} v_1 \otimes \cdots \otimes (x \cdot v_i) \otimes \cdots \otimes v_n. \tag{2.3}$$

Em particular, a n-ésima potência tensorial $T^n(V) = V^{\otimes n} = \underbrace{V \otimes \cdots \otimes V}_{n \text{ vezes}}$ de um $\mathfrak{g}$-módulo V é um $\mathfrak{g}$-módulo. Conseqüentemente, são $\mathfrak{g}$-módulos o produto simétrico $S^n(V)$ e o produto exterior, $\Lambda^n(V)$ (com as ações induzidas), assim como as álgebras tensorial

$$T(V) = \bigoplus_{n=0}^{\infty} T^n(V),$$

simétrica

$$S(V) = \bigoplus_{n=0}^{\infty} S^n(V)$$

e exterior

$$\Lambda(V) = \bigoplus_{n=0}^{\infty} \Lambda^n(V).$$

Outro caso que requer mais atenção é correspondente ao espaço vetorial dual V^* de um $\mathfrak{g}$-módulo V. A ação de G sobre V^* é dada em termos da ação de G sobre V por

$$\langle g \cdot f, v \rangle = \left\langle f, g^{-1} \cdot v \right\rangle .$$

Posto isso, se $x \in \mathfrak{g}$ e $\gamma : I \to G$ é um caminho em G tal que $\gamma(0) = e$ e $\gamma'(0) = x$, temos que

$$\begin{aligned} \langle x \cdot f, v \rangle &= \left\langle \frac{d}{dt}(\gamma(t) \cdot f)\bigg|_{t=0}, v \right\rangle \\ &= \frac{d}{dt} \langle \gamma(t) \cdot f, v \rangle \bigg|_{t=0} \\ &= \frac{d}{dt} \left\langle f, \gamma(t)^{-1} \cdot v \right\rangle \bigg|_{t=0} \\ &= \left\langle f, \frac{d}{dt}(\gamma(t)^{-1} \cdot v)\bigg|_{t=0} \right\rangle \\ &= \langle f, -x \cdot v \rangle \end{aligned}$$

o que torna V^* num $\mathfrak{g}$-módulo. De maneira análoga, se V é um $\mathfrak{g}$-módulo, então V^* torna-se um $\mathfrak{g}$-módulo com a ação prescrita.

Juntando estes dois últimos conceitos, se V e W são $\mathfrak{g}$-módulos de dimensão finita, então $\mathrm{Hom}(V, W)$ se identifica a $V^* \otimes W$, tornando-se num $\mathfrak{g}$-módulo com ação dada por

$$(x \cdot f)(v) = x \cdot f(v) - f(x \cdot v).$$

Antes de chegarmos ao resultado principal desta seção necessitaremos do conceito de Elemento de Casimir.

2.4.2 O Elemento de Casimir de uma representação

Nesta subseção empregaremos a convenção de soma sobre índices repetidos. Seja $\mathfrak{g}$ uma álgebra de Lie semisimples e seja $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação fiel de $\mathfrak{g}$. Definimos uma forma bilinear simétrica $\omega(x, y) = \mathrm{Tr}(\varphi(x)\varphi(y))$ em $\mathfrak{g}$. Então ω é associativa (cf. comentários antes do Lema 30) em relação ao comutador e seu radical S é um ideal de $\mathfrak{g}$. Além disso, ω é não-degenerada, pois (usando o Teorema 33 para $\varphi(S) \subset \varphi(\mathfrak{g})$), $\varphi(S) \cong S$ é um ideal solúvel de $\mathfrak{g}$, logo $S = 0$. Tomando $\varphi = \mathrm{ad}$ resulta $\omega = \kappa$, a forma de Killing de $\mathfrak{g}$.

Se $(x_1, \ldots, x_n)$ é uma base ordenada de $\mathfrak{g}$ então ω determina unicamente a base $(y_1, \ldots, y_n)$ de $\mathfrak{g}$, satisfazendo $\omega(x_i, y_j) = \delta_{ij}$, chamada *base dual* de $(x_1, \ldots, x_n)$ em relação a ω. (Notemos que esta definição é válida para qualquer forma bilinear não-degenerada ω de $\mathfrak{g}$). Se $x \in \mathfrak{g}$, escrevemos $[xx_i] = \sum_j a_{ij}x_j$ e $[xy_i] = \sum_j b_{ij}y_j$. Usando a associatividade de ω podemos calcular

$$\begin{aligned} a_{ik} &= \sum_j a_{ij}\omega(x_j, y_k) = \omega([xx_i], y_k) = \\ &= \omega(-[x_i x], y_k) = -\omega(x_i, [xy_k]) = -\sum_j b_{kj}\omega(x_i, y_j) = -b_{ki}. \end{aligned}$$

Se $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ é qualquer representação de $\mathfrak{g}$, escrevemos $c_\varphi(\omega) = \varphi(x_i)\varphi(y_i) \in \operatorname{End} V$, onde x_i, y_i variam sobre todos os respectivos elementos de bases duais. Em $\operatorname{End} V$ temos a seguinte identidade

$$[x(yz)] = xyz - yzx = xyz - yxz + yxz - yzx = [xy]z + y[xz],$$

para todo $x, y, z \in \operatorname{End} V$. Desse modo,

$$\begin{aligned} [\varphi(x)c_\varphi(\omega)] &= \sum_i ([\varphi(x)\varphi(x_i)]\varphi(y_i) + \varphi(x_i)[\varphi(x)\varphi(y_i)]) \\ &= \sum_{i,j} (a_{ij}\varphi(x_j)\varphi(y_i) + b_{ij}\varphi(x_i)\varphi(y_j)) = 0, \end{aligned}$$

já que $a_{ij} = -b_{ji}$. Isto significa que $c_\varphi(\omega)$ é um endomorfismo de V que comuta com todos os elementos de $\varphi(\mathfrak{g})$.

Voltemos ao caso em que $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ é uma representação fiel de $\mathfrak{g}$, com forma bilinear (associativa, simétrica e não-degenerada) ω como acima. Estando fixada uma base ordenada $(x_1, \ldots, x_n)$ escrevemos simplesmente c_φ para $c_\varphi(\omega)$, ao qual denominamos *elemento de Casimir* de φ.

Uma propriedade interessante do elemento de Casimir é obtida de seu traço:

$$\operatorname{Tr}(c_\varphi) = \sum_i \operatorname{Tr}(\varphi(x_i)\varphi(y_i)) = \sum_i \omega(x_i, y_i) = \dim \mathfrak{g}.$$

Se a representação for irredutível, então o Lema de Schur (cf. Lema 138 na pág. 150) garante que c_φ age diagonalmente sobre V com escalar $\dim \mathfrak{g}/\dim V$. Neste caso, c_φ é independente da escolha da base de $\mathfrak{g}$.

Exemplo 48 ($\mathfrak{s}l(2, F)$) Seja $\mathfrak{g} = \mathfrak{sl}(2, F)$, com base canônica (x, h, y) (cf. Exemplo 11), $V = F^2$, e $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ é a identidade. Por um cálculo direto, encontramos a base dual $(y, h/2, x)$ em relação à forma ω, de modo que,

$$c_\varphi = xy + h^2/2 + yx = \begin{pmatrix} 3/2 & 0 \\ 0 & 3/2 \end{pmatrix}.$$

Observemos que, $3/2 = \dim \mathfrak{g}/\dim V$, como esperávamos. □

Caso φ não seja fiel, podemos ainda definir um elemento de Casimir para φ. $\operatorname{Ker}\varphi$ é um ideal de $\mathfrak{g}$, logo, é soma de alguns ideais simples de $\mathfrak{g}$. Seja $\mathfrak{g}'$ a soma dos ideais simples restantes de $\mathfrak{g}$. Então a restrição de φ a $\mathfrak{g}'$ é fiel e podemos construir o elemento de Casimir como foi feito acima. O elemento de $\operatorname{End} V$ obtido desta maneira é também denominado elemento de Casimir de φ e é denotado por c_φ. Este claramente comuta com $\varphi(\mathfrak{g}) = \varphi(\mathfrak{g}')$.

2.4.3 O Teorema de Weyl

Este resultado é fundamental no estudo dos $\mathfrak{g}$-módulos de uma álgebra de Lie semisimples $\mathfrak{g}$, pois, permite-nos restringir o estudo aos casos de $\mathfrak{g}$-módulos irredutíveis. Para isso, vamos necessitar do seguinte lema.

Lema 49 *Seja $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação de uma álgebra de Lie semisimples $\mathfrak{g}$. Então $\varphi(\mathfrak{g}) \subset \mathfrak{sl}(V)$. Em particular, $\mathfrak{g}$ age trivialmente sobre qualquer $\mathfrak{g}$-módulo unidimensional.*

Prova. Pelo Corolário 36, $\mathfrak{g} = [\mathfrak{g}\mathfrak{g}] = \mathfrak{g}'$, para $\mathfrak{g}$ semisimples, logo $\varphi(\mathfrak{g}) = \varphi(\mathfrak{g}') = \varphi(\mathfrak{g})' \subset \mathfrak{gl}'(V)$. Os elementos de $\mathfrak{gl}'(V)$ têm traço nulo, pois são combinações lineares de comutadores de elementos de $\mathfrak{gl}(V)$. Portanto $\mathfrak{gl}'(V) \subset \mathfrak{sl}(V)$, concluindo a prova. ■

Teorema 50 (Weyl) *Se $\mathfrak{g}$ é uma álgebra de Lie semisimples e V é um $\mathfrak{g}$-módulo de dimensão finita, então V é completamente redutível.*

Prova. Consideremos inicialmente o caso em que V tem um $\mathfrak{g}$-submódulo W de codimensão 1. Pelo Lema 49, $\mathfrak{g}$ age trivialmente sobre $F = V/W$, e temos a seqüência exata curta (cf. Apêndice B.1)

$$0 \to W \to V \to F \to 0. \tag{2.4}$$

Por indução sobre $\dim W$, vamos mostrar que se W não é irredutível, então esta seqüência se cinde (cf. Proposição 163), isto é, W tem um complementar em V. Se W' é um $\mathfrak{g}$-submódulo próprio não-nulo de W, temos a seqüência exata curta

$$0 \to \frac{W}{W'} \to \frac{V}{W'} \to F \to 0.$$

Como $\dim W/W' < \dim W$, a hipótese de indução nos dá um $\mathfrak{g}$-submódulo $\tilde{W}/W'$ de V/W' complementar de W/W', tal que

$$\dim \frac{\tilde{W}}{W'} = \dim \frac{V}{W'} - \dim \frac{W}{W'} = 1.$$

Conseqüêntemente, é exata a seqüência curta

$$0 \to W' \to \tilde{W} \to F \to 0.$$

Novamente, $\dim W' < \dim W$, e usamos a hipótese de indução para obter um $\mathfrak{g}$-submódulo X de $\tilde{W}$ complementar W', tal que

$$\dim X = \dim \tilde{W} - \dim W' = 1.$$

Como $V/W' \cong W/W' \oplus \tilde{W}/W'$, temos $W \cap \tilde{W} = W'$, e de $\tilde{W} = W' \oplus X$ concluímos que $W \cap X = 0$. Portanto, $V = W \oplus X$, como requerido.

Por outro lado, se W é irredutível, o trabalho é um pouco mais complicado e vamos usar a linguagem de representações, tendo à mão o elemento de Casimir. Por conveniência, podemos assumir também que a representação $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ seja fiel sobre V. Seja $c = c_\varphi$ o elemento de Casimir de φ. Como c comuta com $\varphi(\mathfrak{g})$, c é um endomorfismo de $\mathfrak{g}$-módulos. Em particular, W é estável sob c e $\operatorname{Ker} c$ é um $\mathfrak{g}$-submódulo de V. A ação trivial de $\mathfrak{g}$ sobre V/W equivale a dizer que $\mathfrak{g}$ leva V em W, o mesmo devendo se suceder com c (pois este é combinação linear de elementos de $\varphi(\mathfrak{g})$). Então c tem traço zero em V/W, mas não pode ter traço zero em W, onde c age como escalar pelo Lema de Schur, ou teríamos $\dim \mathfrak{g} = \mathrm{Tr}_V(c) = 0$. Portanto, $V = W \oplus \operatorname{Ker} c$, como desejado.

Tendo visto o caso especial, podemos finalmente ir ao caso geral em que W é um $\mathfrak{g}$-submódulo não-nulo de V e mostrar que a seqüência exata curta

$$0 \to W \to V \to V/W \to 0$$

se cinde. Para isso, consideremos $\mathrm{Hom}(V, W)$ o espaço vetorial das aplicações lineares de V em W visto como um $\mathfrak{g}$-módulo. Seja $\mathcal{V}$ o subespaço de $\mathrm{Hom}(V, W)$ das aplicações cuja restrição a W é multiplicação por um escalar. Se $f \in \mathcal{V}$, então $f|_W = a \cdot 1$ para algum escalar $a \in F$, de modo que para todo $x \in \mathfrak{g}$, $w \in W$, temos

$$\begin{aligned} (x \cdot f)(w) &= x \cdot f(w) - f(x \cdot w) \\ &= x \cdot aw - a(x \cdot w) = 0, \end{aligned}$$

donde $x \cdot (f|_W) = 0$. Seja $\mathcal{W}$ o subespaço de $\mathcal{V}$ consistindo dos endomorfismos escalares cuja restrição a W é zero. Claramente, este é também um $\mathfrak{g}$-submódulo de $\mathrm{Hom}(V, W)$ e $\mathfrak{g}$ leva $\mathcal{V}$ em $\mathcal{W}$. Além disso, $\mathcal{W}$ tem codimensão 1 em $\mathcal{V}$, haja vista os elementos de $\mathcal{V}$ serem determinados (módulo $\mathcal{W}$) pelo escalar $f|_W$. Com isto, estamos precisamente no caso especial

$$0 \to \mathcal{W} \to \mathcal{V} \to \mathcal{V}/\mathcal{W} \to 0,$$

mencionado acima.

De acordo com a primeira parte da prova, $\mathcal{V}$ tem um $\mathfrak{g}$-submódulo unidimensional $\mathcal{X}$ complementar a $\mathcal{W}$. Seja f um dos geradores de $\mathcal{X}$. Sem perda de generalidade, podemos assumir $f|_W = 1_W$ (basta multiplicar f por um escalar adequado). Temos

$$0 = (x \cdot f)(v) = x \cdot f(v) - f(x \cdot v)$$

isto é f é um homomorfismo de $\mathfrak{g}$-módulos. Logo $\operatorname{Ker} f$ é um $\mathfrak{g}$-submódulo de V. Como f leva V em W e age como identidade sobre W, concluímos que $V = W \oplus \operatorname{Ker} f$. ∎

2.4.4 Conservação da decomposição de Jordan

Como aplicação imediata do Teorema de Weyl, vamos mostrar que a Decomposição de Jordan é "compatível" com as representações de $\mathfrak{g}$.

Teorema 51 *Seja V um espaço vetorial de dimensão finita sobre um corpo algebricamente fechado F e $\mathfrak{g} \subset \mathfrak{gl}(V)$ uma álgebra de Lie linear semisimples sobre F. Então $\mathfrak{g}$ contém as partes semisimples e nilpotente de todos os seus elementos em $\mathfrak{gl}(V)$. Particularmente, as decomposições de Jordan usual e abstrata em $\mathfrak{g}$ coincidem.*

Prova. Seja $x \in \mathfrak{g}$ qualquer e $x = x_s + x_n$ sua decomposição de Jordan em $\mathfrak{gl}(V)$. Temos que $\operatorname{ad}_{\mathfrak{gl}(V)} x(\mathfrak{g}) \subset \mathfrak{g}$, logo (prop. 28c) $\operatorname{ad}_{\mathfrak{gl}(V)} x_s(\mathfrak{g}) \subset \mathfrak{g}$ e $\operatorname{ad}_{\mathfrak{gl}(V)} x_n(\mathfrak{g}) \subset \mathfrak{g}$, o que equivale a dizer que $x_s, x_n \in N = N_{\mathfrak{gl}(V)}(\mathfrak{g})$. Este normalizador é a maior subálgebra de Lie de $\mathfrak{gl}(V)$ que contém $\mathfrak{g}$ como um ideal. Gostaríamos de poder afirmar que $N = \mathfrak{g}$, mas isso não ocorre, pois N contém os escalares, mas $\mathfrak{g} \subset \mathfrak{sl}(V)$ não. Precisamos achar uma subálgebra de $\mathfrak{gl}(V)$ que esteja contida propriamente em N e que contenha $\mathfrak{g}$ como um ideal, a qual provaremos ser igual a $\mathfrak{g}$.

Se W é qualquer $\mathfrak{g}$-submódulo de V, definimos $\mathfrak{g}_W = \{y \in \mathfrak{gl}(V) : y(W) \subset W \text{ e } \operatorname{Tr}(y|_W) = 0\}$. Se $z \in \mathfrak{g}$, é claro que $z(W) \subset W$, e como $\mathfrak{g} = [\mathfrak{g}\mathfrak{g}]$, temos $z = \sum_i [x_i y_i]$, para alguns $x_i, y_i \in \mathfrak{g}$, logo $\operatorname{Tr}(z|_W) = \operatorname{Tr}(\sum_i [x_i|_W, y_i|_W]) = 0$, i.é, $z \in \mathfrak{g}_W$. Portanto, $\mathfrak{g}$ está contida em todos os tais espaços $\mathfrak{g}_W$. Seja $\mathfrak{g}'$ a intersecção de N com todos os espaços $\mathfrak{g}_W$. Então $\mathfrak{g}'$ é uma subálgebra de N contendo $\mathfrak{g}$ como um ideal. Além disso, se $x \in \mathfrak{g}$, então x_s, x_n estão em $\mathfrak{g}_W$, logo estão também em $\mathfrak{g}'$.

Vamos mostrar que $\mathfrak{g} = \mathfrak{g}'$. Ocorre que $\mathfrak{g}'$ é um $\mathfrak{g}$-módulo de dimensão finita, logo o Teorema de Weyl nos permite escrever $\mathfrak{g}' = \mathfrak{g} \oplus M$ para algum $\mathfrak{g}$-submódulo M. Mas $[\mathfrak{g}\mathfrak{g}'] \subset \mathfrak{g}$, de modo que $\mathfrak{g}$ age trivialmente sobre M. Seja W qualquer $\mathfrak{g}$-submódulo irredutível de V. Se $y \in M$ então $[\mathfrak{g}, y] = 0$, donde o lema de Schur garante que y age sobre W como um escalar. Por outro lado $\operatorname{Tr}(y|_W) = 0$, pois $y \in \mathfrak{g}_W$. Portanto y age trivialmente sobre W. Como V pode ser escrito como soma direta de $\mathfrak{g}$-submódulos irredutíveis, então de fato $y = 0$, concluindo a prova. ∎

Corolário 52 *Seja $\mathfrak{g}$ uma álgebra de Lie semisimples e $\varphi : \mathfrak{g} \to \mathfrak{gl}(V)$ uma representação (de dimensão finita) de $\mathfrak{g}$. Se $x = s + n$ é a decomposição de Jordan abstrata de $x \in \mathfrak{g}$, então $\varphi(x) = \varphi(x_s) + \varphi(x_n)$ é a decomposição de Jordan usual de $\varphi(x)$.*

Prova. Se $\operatorname{ad}_{\mathfrak{g}} s(x) = \lambda x$, então $\operatorname{ad}_{\varphi(\mathfrak{g})} \varphi(s)(\varphi(x)) = \varphi(\operatorname{ad}_{\mathfrak{g}} s(x)) = \lambda\varphi(x)$. Isto mostra que $\varphi(\mathfrak{g})$ é gerada por autovetores de $\operatorname{ad}_{\varphi(\mathfrak{g})} \varphi(s)$, logo $\varphi(s)$ é ad-semisimples. Do mesmo modo, $\varphi(n)$ é ad-nilpotente e $[\operatorname{ad}_{\varphi(\mathfrak{g})} \varphi(s), \operatorname{ad}_{\varphi(\mathfrak{g})} \varphi(n)] = 0$. Portanto, $\varphi(x) = \varphi(s) + \varphi(n)$ é a decomposição de Jordan abstrata de $\varphi(x)$ em $\varphi(\mathfrak{g})$ (uma álgebra de Lie semisimples). Pelo teorema, esta coincide com a decomposição de Jordan usual de $\varphi(x)$ em $\varphi(\mathfrak{g})$. ■

2.5 Representações de dimensão finita de $\mathfrak{sl}(2, F)$

As representações de $\mathfrak{sl}(2, F)$ quando F é um corpo algebricamente fechado de característica 0 constituem o caso mais simples da teoria de representações de álgebras de Lie. Adiante, veremos que toda álgebra de Lie semisimples de dimensão finita é constituida de cópias de $\mathfrak{sl}(2, F)$, de modo que, estudar suas representações significa atender ao básico. De fato, vamos obter uma caracterização completa das representações de dimensão finita de $\mathfrak{sl}(2, F)$. A grande importância deste estudo ficará clara quando estivermos abordando a teoria de classificação adiante.

Nesta seção, F é um corpo algebricamente fechado de característica 0, $\mathfrak{g} = \mathfrak{sl}(2, F)$, e $\{x, h, y\}$ é a base canônica de $\mathfrak{g}$ conforme o Exemplo 11. Recordamos as relações de comutação que definem $\mathfrak{g}$:

$$[hx] = 2x, \qquad [xy] = h, \qquad [hy] = -2y.$$

Seja V um $\mathfrak{g}$-módulo irredutível de dimensão finita. Pelo Corolário 52, h age diagonalmente sobre V de modo que temos a decomposição

$$V = \bigoplus_{\lambda} V_\lambda \tag{2.5}$$

onde a soma se dá sobre todos os autovalores λ distintos do endomorfismo h de V. Notemos que esta é uma soma finita. Estes autovalores são denominados *pesos* e o espaço V_λ associado ao peso λ é chamado *espaço peso*.

A esta altura, surge uma indagação natural a respeito do modo como x e y agem sobre os diversos espaços V_λ. Isto pode ser analisado através da relação (M3) escrevendo, para todo $v \in V_\lambda$,

$$\begin{aligned} h \cdot x \cdot v &= x \cdot h \cdot v + [hx] \cdot v \\ &= x \cdot (\lambda v) + 2x \cdot v \\ &= (\lambda + 2) x \cdot v \end{aligned}$$

donde $x \cdot v$ é um autovetor de h associado ao autovalor $\lambda + 2$. Claramente, a ação de x é dada por

$$x : V_\lambda \to V_{\lambda+2}.$$

Um raciocínio análogo nos permite ver que a ação de y é tal que

$$y : V_\lambda \to V_{\lambda-2}.$$

Um resultado paralelo a estas expressões é que x e y são nilpotentes, o que já se concluía pelo Corolário 52.

Como a soma (2.5) é finita, deve haver um λ tal que $V_{\lambda+2} = 0$. Para tal λ, todo vetor não-nulo $v \in V_\lambda$ é chamado de *vetor maximal* de peso λ. Outra conseqüência imediata da ação descrita acima é que os pesos que aparecem na decomposição (2.5) devem ser todos congruentes módulo 2. Com efeito, se λ_0 for qualquer um deles, então o subespaço

$$\bigoplus_{n \in \mathbb{Z}} V_{\lambda_0 + 2n}$$

é estável sob a ação de $\mathfrak{g}$, ou seja, é um $\mathfrak{g}$-submódulo. Como V é irredutível, este submódulo deve ser todo V. Isto signfica também que os espaços pesos V_λ devem formar uma cadeia (finita) initerrupta de pesos da forma α, $\alpha + 2$, $\ldots$, $\alpha + 2k$, para algum $k = 0, 1, 2, \ldots$ Suponhamos que a cadeia fosse quebrada para algum i, isto é, $V_{\alpha+2i} = 0$. Então teríamos $V = U \oplus W$, onde $U = \bigoplus_{n=0}^{i} V_{\alpha+2n}$ e $W = \bigoplus_{n=i}^{k} V_{\alpha+2n}$ seriam dois $\mathfrak{g}$-submódulos distintos de V, o que é impossível. Conseqüentemente, há um único espaço peso cujos vetores são maximais, digamos

V_n. Este n é chamado *peso máximo* de V.

Tomemos qualquer vetor maximal $v_0 \in V_n$. Como $V_{n+2} = 0$, devemos ter $x \cdot v_0 = 0$. As ações iteradas de y sobre v_0 formam o conjunto $A = \{v_0, y \cdot v_0, y^2 \cdot v_0, \ldots\}$ e podemos considerar o subespaço W de V gerado por A. Vamos mostrar que, de fato, $W = V$. Basta mostrar que W é estável sob a ação de $\mathfrak{g}$. Claramente, $y \cdot W \subset W$, já que y apenas leva o vetor $y^i \cdot v_0$ no vetor 0 ou no vetor $y^{i+1} \cdot v_0$. Além disso, notamos que $y^i \cdot v_0 \in V_{n-2i}$ donde $h \cdot y^i \cdot v_0 = (n-2i)y^i \cdot v_0$. Portanto, $h \cdot W \subset W$. Esta observação garante imediatamente que os elementos não-nulos de A sejam linearmente independentes (como autovetores de h associados a autovalores distintos). Finalmente, usando um rápido argumento de indução, mostramos que $x \cdot y^i \cdot v_0 = i(n-i+1)y^{i-1} \cdot v_0$, e desse modo $x \cdot W \subset W$, completando a verificação.

Seja m o menor inteiro tal que $y^m \cdot v_0 = 0$ (o qual existe, pois V tem dimensão finita e A gera V). Formamos o subconjunto $B = \{v_0, y \cdot v_0, \ldots, y^{m-1} \cdot v_0\}$ de A, claramente uma base de V, consistindo de autovetores de h, cujos autovalores associados ocorrem todos com multiplicidade 1, de modo que $\dim V_\lambda = 1$, para todo peso λ. Temos ainda, que

$$0 = x \cdot y^m \cdot v_0 = m(n-m+1)y^{m-1} \cdot v_0,$$

donde $n - m + 1 = 0$. Em conseqüência disso, n e todos os demais pesos λ de V devem ser inteiros. Particularmente, $\dim V = n + 1$.

Obeservamos que em relação à base B, a matriz de h é diagonal, enquanto que as matrizes de x e y são triangulares, respectivamente, estritamente superior e estritamente inferior.

Para completar nossa análise, vemos que os pesos formam uma cadeia de inteiros diferindo de 2 entre si, simétrica em relação à origem de $\mathbb{Z} \subset F$,

$$-n, -n+2, \ldots, n-2, n.$$

Portanto, para cada $n = 0, 1, 2, \ldots$, há um único $\mathfrak{g}$-módulo irredutível de dimensão $n + 1$ (a menos de isomorfismos). Indicamos este $\mathfrak{g}$-módulo por $V^{(n)}$.

Devido ao fato de cada peso ocorrer simultaneamente com seu oposto, um $\mathfrak{g}$-módulo V arbitrário, cujos pesos tenham todos a mesma paridade, e ocorram com multiplicidade 1 (formando, portanto, uma cadeia simétrica em relação à origem), tem necessariamente que ser irredutível. Ademais, o número de fatores irredutíveis de um $\mathfrak{g}$-módulo arbitrário V é exatamente $\dim V_0 + \dim V_1$. Para ver isto, basta notarmos que, na decomposição de V, para cada fator irredutível temos uma única ocorrência do peso 0 ou do peso 1 (mas não de ambos, devido à paridade).

Exemplo 53 Seja $V = F$, o $\mathfrak{g}$-módulo trivial. Claramente, $V = V^{(0)}$. □

Exemplo 54 Consideremos o $\mathfrak{g}$-módulo canônico (bidimensional) $V = F \times F = F^2$, com base canônica $\{\tilde{x} = (1,0), \tilde{y} = (0,1)\}$. Então, a partir da matriz de h em (2.1) obtemos,

$$\begin{aligned} h \cdot \tilde{x} &= \tilde{x}, \\ h \cdot \tilde{y} &= -\tilde{y}. \end{aligned}$$

Pela observação no parágrafo anterior, $V = F\tilde{x} \oplus F\tilde{y} = V_{-1} \oplus V_1$ é exatamente $V^{(1)}$. □

Exemplo 55 Seja V o $\mathfrak{g}$-módulo canônico com base canônica $\{\tilde{x}, \tilde{y}\}$ e $W = S^2(V)$ a segunda potência simétrica de V. Então W é um $\mathfrak{g}$-módulo e $\{\tilde{x}^2, \tilde{x}\tilde{y}, \tilde{y}^2\}$[1] é uma base de W. A ação de $\mathfrak{g}$ sobre W é dada em termos da expressão (2.3) acima. Em particular, a ação de h é dada explicitamente por

$$\begin{aligned} h \cdot (\tilde{x}^2) &= (h \cdot \tilde{x})\tilde{x} + \tilde{x}(h \cdot \tilde{x}) = 2\tilde{x}^2, \\ h \cdot (\tilde{x}y) &= (h \cdot \tilde{x})\tilde{y} + \tilde{x}(h \cdot \tilde{y}) = 0, \\ h \cdot (\tilde{y}^2) &= (h \cdot \tilde{y})\tilde{y} + \tilde{y}(h \cdot \tilde{y}) = -2\tilde{y}^2, \end{aligned}$$

donde $W = F\tilde{x}^2 \oplus F\tilde{x}\tilde{y} \oplus F\tilde{y}^2 = W_{-2} \oplus W_0 \oplus W_2$ é exatamente o $\mathfrak{g}$-módulo $V^{(2)}$. De maneira geral, a n-ésima potência simétrica $S^n(V)$ tem base $\{\tilde{x}^n, \tilde{x}^{n-1}\tilde{y}, \ldots, \tilde{x}y^{n-1}, \tilde{y}^n\}$, e um cálculo direto nos mostra que a ação de h sobre os elementos dessa base é tal que

$$h \cdot (\tilde{x}^{n-k}\tilde{y}^k) = (n-2k)\tilde{x}^{n-k}\tilde{y}^k, \qquad k = 0, \ldots, n,$$

[1] O produto simétrico está denotado aqui por simples justaposição.

donde concluímos que os pesos de $S^n(V)$ formam a seqüência

$$-n, -n+2, \ldots, n-2, n,$$

ocorrendo cada um com multiplicidade 1. Pela observação acima, segue que $S^n(V)$ é irredutível, logo $V^{(n)} = S^n(V)$. Portanto, *há precisamente um $\mathfrak{g}$-módulo irredutível (a menos de isomorfismos) para cada $n \geq 0$.* □

2.5.1 Pletismo

Dado um $\mathfrak{g}$-módulo V qualquer, podemos formar novos $\mathfrak{g}$-módulos por meio de operações (multi)lineares algébricas, como $V \otimes V$, $S^k(V)$, $\Lambda^k(V)$, V^*, etc. Estes novos $\mathfrak{g}$-módulos certamente admitem uma decomposição em soma de fatores irredutíveis. *Pletismo* consiste exatamente em descrever as decomposições de $\mathfrak{g}$-módulos obtidos desta maneira. Vale recordar que se $V = U \oplus W$ é uma decomposição, temos então os isomorfismos naturais de $\mathfrak{g}$-módulos

$$T^n(V) \cong \bigoplus_{i+j=n} T^i(U) \otimes T^j(W),$$

$$S^n(V) \cong \textstyle\bigoplus_{i+j=n} S^i(U) \otimes S^j(W), \quad \text{e} \quad \Lambda^n(V) \cong \textstyle\bigoplus_{i+j=n} \Lambda^i(U) \otimes \Lambda^j(W).$$

Desse modo, conhecendo a decomposição em espaços pesos de um $\mathfrak{g}$-módulo V podemos claramente deduzir a decomposição em espaços pesos de quaisquer potências tensoriais de V. Por exemplo, se V_α e V_β são espaços pesos de V com respectivos pesos α e β então $V_\alpha \otimes V_\beta$ é um auto-espaço de $V \otimes V$ com peso $\alpha + \beta$. O mesmo se afirma para os produtos simétrico e exterior. Portanto, os pesos do produto se combinam aditivamente aos pares a partir dos pesos dos fatores, cobrindo todas as possíveis somas, com possíveis repetições. O peso total do produto é, então, simplesmente o produto do número de pesos dos fatores.

Para fixar as idéias, suponhamos que V seja o $\mathfrak{g}$-módulo canônico e desejamos estudar a decomposição de $V^{(2)} \otimes V^{(3)}$. Sabemos que os pesos de $V^{(2)}$ são $0, \pm 2$ e os pesos de $V^{(3)}$ são $\pm 1, \pm 3$. Conhecendo a ação de $\mathfrak{g}$ sobre $V^{(2)} \otimes V^{(3)}$, vem que este admite os $3 \cdot 4 = 12$ pesos ± 5, ± 3 (duas vezes), e ± 1 (três veses). Se v é um vetor de peso 5, então, $\{v, y \cdot v, \ldots, y^5 \cdot v\}$ é uma base para um $\mathfrak{g}$-submódulo de $V^{(2)} \otimes V^{(3)}$ isomorfo a $V^{(5)}$, o qual contabiliza uma ocorrência para cada um dos pesos $-5, -3, -1, 1, 3, 5$. O complementar de $V^{(5)}$ em $V^{(2)} \otimes V^{(3)}$ conta com os pesos ± 1(duas vezes) e ± 3, de modo que um vetor w de peso 3 gera um $\mathfrak{g}$-submódulo isomorfo a $S^3(V)$, contabilizando uma ocorrência para os pesos $-3, -1, 1, 3$. Finalmente, o complementar de $S^5(V) \oplus S^3(V)$ conta com os pesos $-1, 1$, donde é exatamente uma cópia de V. Conseqüentemente,

$$V^{(2)} \otimes V^{(3)} \cong V^{(5)} \oplus V^{(3)} \oplus V^{(1)}$$

Em geral, se a e b são inteiros positivos tais que $a \geq b$, é interessante obter uma expressão para a decomposição em pesos de $V^{(a)} \otimes V^{(b)}$. Para isso, associamos a uma seqüência simétrica de pesos $-a, -a+2, \ldots, a-2, a$ (a qual determina univocamente $V^{(a)}$), cada um ocorrendo com multiplicidade 1, um polinômio de Laurent

$$x^{-a} + x^{-a+2} + \cdots + x^{a-2} + x^{a} = \sum_{i=0}^{a} x^{a-2i},$$

na indeterminada x. Reciprocamente, dado um polinômio de Laurent tal que cada expoente apareça juntamente com seu negativo um igual número de vezes, podemos recuperar a seqüência de pesos simplesmente listando os expoentes de cada termo, contabilizando eventuais repetições. Dadas duas destas seqüências, $-a, \ldots, a$, e $-b, \ldots, b$, com seus respectivos polinômios, um cálculo direto nos permite verificar a fórmula combinatorial

$$\left(\sum_{i=0}^{a} x^{a-2i}\right)\left(\sum_{i=0}^{b} x^{b-2j}\right) = \sum_{k=0}^{b}\left(\sum_{l=0}^{a+b-2k} x^{a+b-2k-2l}\right).$$

Notemos que os expoentes que aparecem nos termos do lado direito desta expressão ocorrem juntamente com seu oposto um igual número de vezes (i.é, a seqüência e as multiplicidades são simétricas) e que todos os possíveis produtos dos termos aos pares (conseqüentemente todas as possíveis somas dos pesos aos pares) estão expressos do lado direito, donde obtemos a seqüência $-a-b$, $-a-b+2$ (2 vezes), $-a-b+4$ (3 vezes),..., $a+b-2$ (2 vezes), $a+b$. Notemos também que os termos medianos desta seqüência ocorrem com multiplicidade b formando uma subseqüência simétrica de comprimento $a-b+1$ (correspondente ao caso em que $k=b$ e l vai de 0 até $a-b$). Podemos ilustrar esta situação dispondo os elementos da seqüência de maneira a formar a seguinte pirâmide:

$$\begin{array}{lcccccccccccc}
k{=}b: & & & & -a{+}b, & -a{+}b{+}2, & ... & a{-}b{-}2, & a{-}b & & & \\
\vdots & & & & \vdots & \vdots & & \vdots & \vdots & & & \\
k{=}1: & & -a{-}b{+}2, & ... & -a{+}b, & -a{+}b{+}2, & ... & a{-}b{-}2, & a{-}b, & ... & a{+}b{-}2 & \\
k{=}0: & -a{-}b, & -a{-}b{+}2, & ... & -a{+}b, & -a{+}b{+}2, & ... & a{-}b{-}2, & a{-}b, & ... & a{+}b{-}2, & a{+}b
\end{array} \tag{2.6}$$

Em particular, vemos que o maior peso $a+b$ ocorre com multiplicidade 1, de modo que, um raciocínio semelhante ao desenvolvido acima nos dá um $\mathfrak{g}$-submódulo de $V^{(a)} \otimes V^{(b)}$ isomorfo a $V^{(a+b)}$, contabilizando exatamente uma ocorrência de cada um dos pesos correspondentes à linha inferior da pirâmide (2.6) acima. O complementar de $V^{(a+b)}$ em $V^{(a)} \otimes V^{(b)}$ comparece então com os pesos restantes na pirâmide, donde um simples argumento de indução sobre o peso máximo nos permite concluir que este complementar é isomorfo a $V^{(a+b-2)} \oplus \cdots \oplus V^{(a-b)}$. Conseqüentemente, obtemos a decomposição desejada:

$$V^{(a)} \otimes V^{(b)} \cong V^{(a+b)} \oplus V^{(a+b-2)} \oplus \cdots \oplus V^{(a-b)}. \tag{2.7}$$

Procedimentos semelhantes se aplicam aos produtos simétricos e exteriores de quaisquer $\mathfrak{g}$-módulos dados. Porém, nem sempre é fácil obter uma expressão geral como em (2.7). Para mais detalhes remetemos a Fulton & Harris[FH, §11].

2.5.2 Resumo

O seguinte resultado, juntamente com seu corolário, resumem a classificação das representações de $\mathfrak{sl}(2, F)$.

Teorema 56 *Seja V um $\mathfrak{g}$-módulo irredutível para $\mathfrak{g} = \mathfrak{sl}(2, F)$. Temos:*

(a) Em relação a h, V é soma direta de espaços pesos V_α, com $\alpha = -m, -m+2, \ldots, m-2, m$, onde $\dim V = m+1$ e $\dim V_\alpha = 1$ para cada α.

(b) V admite um único vetor maximal (a menos de múltiplos escalares), cujo peso (denominado peso máximo) é m.

(c) Há exatamente um $\mathfrak{g}$-módulo irredutível (a menos de isomorfismos) para cada possível dimensão $m+1$, denotado $V^{(m)}$, para $m \geq 0$.

Corolário 57 *Tomemos $\mathfrak{g} = \mathfrak{sl}(2, F)$ e seja V um $\mathfrak{g}$-módulo qualquer (de dimensão finita). Então os pesos de V são todos inteiros, cada um ocorrendo juntamente com seu oposto um número igual de vezes. Além disso, em qualquer decomposição de V em soma direta de $\mathfrak{g}$-submódulos irredutíveis, o número de parcelas é exatamente* $\dim V_0 + \dim V_1$. *Se os pesos de V ocorrem todos com a mesma paridade e todos comparecem com multiplicidade* 1, *então V é irredutível.*

2.6 Classificação das Álgebras de Lie Semisimples de Dimensão Finita

Nesta seção, $\mathfrak{g}$ denota uma álgebra de Lie semisimples. Vamos estudar detalhadamente a estrutura de $\mathfrak{g}$ através de sua representação adjunta. Neste caso, porém, não contamos com um único elemento "diagonal" h, como no caso das representações de $\mathfrak{sl}(2, F)$, permitindo decompor a representação numa soma direta de espaços pesos. Não obstante, veremos que é possível utilizar uma certa subálgebra $\mathfrak{h}$ de $\mathfrak{g}$, a qual tem papel análogo ao de h, e que os pesos não serão simplesmente números inteiros, mas elementos de $\mathfrak{h}^*$, o espaço vetorial dual de $\mathfrak{h}$.

2.6.1 Álgebras Torais Maximais

Como $\mathfrak{g}$ é semisimples, pelo Teorema de Engel, $\mathfrak{g}$ não pode consistir inteiramente de elementos nilpotentes (i.é, ad-nilpotentes). Isto significa que $\mathfrak{g}$ contém elementos semisimples (i.é, ad-semisimples), os quais geram subálgebras de $\mathfrak{g}$ consistindo unicamente de elementos semisimples (cf. Proposição 28 e Teorema 38), as quais chamamos de *subálgebras torais*.

Lema 58 *Seja T uma subálgebra toral de uma álgebra de Lie semisimples $\mathfrak{g}$. Então T é abeliana.*

Prova. Seja $x \in T$ qualquer. Como x é semisimples e F é um corpo de característica 0, $\operatorname{ad}_T x$ age diagonalmente sobre T. Basta, portanto, mostrar que $\operatorname{ad}_T x$ não tem autovalores não-nulos. Suponhamos que $\operatorname{ad}_T x(y) = ay$ para algum $a \in F$ e $y \in T$. Como $\operatorname{ad}_T y$ também é diagonalizável, podemos escrever x como combinação linear de autovetores de $\mathrm{ad}_T\, y$. Desse modo, temos que $\mathrm{ad}_T\, y(x) = -ay$ está simultaneamente num autoespaço (i.é, um subespaço contendo todos os autovetores) associado ao autovalor 0 e, eventualmente, num autoespaço associado a autovalores não-nulos de $\mathrm{ad}_T\, y$, logo deve ser $a = 0$. ■

Fixemos uma subálgebra toral maximal $\mathfrak{h}$ de $\mathfrak{g}$, a qual é abeliana pelo Lema 58. Em particular, $\mathrm{ad}_{\mathfrak{g}}\, \mathfrak{h}$ é uma família de endomorfismos diagonalizáveis que comutam entre si. Um resultado clássico da álgebra linear nos garante que endomorfismos com essa propriedade são simultaneamente diagonalizáveis. Isto equivale a dizer que $\mathfrak{g}$ se decompõe como soma direta de subespaços

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} : [hx] = \alpha(h)x \text{ para todo } h \in \mathfrak{h}\},$$

onde $\alpha \in \mathfrak{h}^*$. Note que $\mathfrak{g}_0$ é simplesmente o centralizador de $\mathfrak{h}$ em $\mathfrak{g}$, $C_{\mathfrak{g}}(\mathfrak{h})$. De fato, podemos afirmar mais [Hu, Prop. 8.2], que $C_{\mathfrak{g}}(\mathfrak{h}) = \mathfrak{h}$.

O conjunto de todos os $\alpha \in \mathfrak{h}^*$ não-nulos tais que $\mathfrak{g}_\alpha \neq 0$ é denotado por Φ e tais elementos são chamados *raízes* de $\mathfrak{g}$ em relação a $\mathfrak{h}$. Observe que Φ é um conjunto finito. Com esta notação, podemos escrever a *decomposição do espaço por raízes*

$$\mathfrak{g} = C_{\mathfrak{g}}(\mathfrak{h}) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha. \tag{2.8}$$

Exemplo 59 (Decomposição de $\mathfrak{s}l(n, F)$) Seja $\mathfrak{g} = \mathfrak{sl}(n, F)$, com a base canônica $h_i = e_{ii} - e_{i+1,i+1}$ $(1 \leq i < n)$, $e_{i,j}$ $(1 \leq i \neq j \leq n)$. Pode ser verificado que os h_i geram uma subálgebra toral maximal $\mathfrak{h}$ de $\mathfrak{g}$ e um cálculo direto nos mostra que essa base determina uma decomposição de $\mathfrak{g}$ por raízes. □

Pode ser mostrado (cf. Humphreys [Hu, caps. IV e V]) que Φ (assim como a decomposição por raízes) não depende essencialmente de uma escolha particular de $\mathfrak{h}$. Dentro dos interesses deste trabalho, e por razões de brevidade, vamos assumir como verdadeiro este resultado daqui por diante. Isto se relaciona com uma outra caracterização das subálgebras torais maximais de álgebras de Lie semisimples $\mathfrak{g}$ como subálgebras de Cartan de $\mathfrak{g}$ (CSA's), além de uma quantidade razoável de teoria, indicada na referência acima.

Proposição 60 *Para todo* $\alpha, \beta \in \mathfrak{h}^*$, $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subset \mathfrak{g}_{\alpha+\beta}$. *Se* $x \in \mathfrak{g}_\alpha$, $\alpha \neq 0$, *então* $\operatorname{ad} x$ *é nilpotente. Se* $\alpha, \beta \in \mathfrak{h}^*$, *e* $\alpha + \beta \neq 0$, *então* $\mathfrak{g}_\alpha$ *é ortogonal a* $\mathfrak{g}_\beta$ *relativamente à forma de Killing* κ *de* $\mathfrak{g}$.

Prova. Para todo $h \in \mathfrak{h}$, $x \in \mathfrak{g}_\alpha$, e $y \in \mathfrak{g}_\beta$ usando a identidade de Jacobi temos que

$$\operatorname{ad} h([xy]) = [[hx]y] + [x[hy]] = \alpha(h)[xy] + \beta(h)[xy] = (\alpha+\beta)(h)[xy],$$

provando a primeira afirmação. A segunda afirmação é conseqüência imediata da primeira e do fato de Φ ser finito.

Seja $h \in \mathfrak{h}$ tal que $(\alpha+\beta)(h) \neq 0$. Então, para todo $x \in \mathfrak{g}_\alpha$ e $y \in \mathfrak{g}_\beta$, pela associatividade de κ escrevemos

$$\kappa([hx], y) = -\kappa([xh], y) = -\kappa(x, [hy]),$$

ou seja,

$$\alpha(h)\kappa(x, y) = -\beta(h)\kappa(x, y),$$

e daí,

$$(\alpha+\beta)(h)\kappa(x, y) = 0.$$

Conseqüentemente, $\kappa(x, y) = 0$. ∎

Corolário 61 *A restrição da forma de Killing de* $\mathfrak{g}$ *a* $\mathfrak{g}_0 = C_{\mathfrak{g}}(\mathfrak{h})$ *é não-degenerada.*

Prova. Como $\mathfrak{g}$ é semisimples, κ é não-degenerada. Por outro lado, $\mathfrak{g}_0$ é ortogonal a $\mathfrak{g}_\alpha$ para todo $\alpha \in \Phi$. Se $x \in \mathfrak{g}_0$ é ortogonal a $\mathfrak{g}_0$ então $\kappa(x, \mathfrak{g}) = 0$, impondo $x = 0$. ∎

Proposição 62 *Seja* $\mathfrak{h}$ *uma subálgebra toral maximal de* $\mathfrak{g}$. *Então* $\mathfrak{h} = C_{\mathfrak{g}}(\mathfrak{h})$.

Esboço da prova. (1) $C = C_{\mathfrak{g}}(\mathfrak{h})$ contém as partes semisimples e nilpotente de seus elementos. (2) Todos os elementos semisimples de C estão em $\mathfrak{h}$. (3) A restrição de κ a $\mathfrak{h}$ é não-degenerada pelo Corolário 61. (4) C é nilpotente pelo Teorema de Engel. (5) $\mathfrak{h} \cap [CC] = 0$. (6) C é abeliana. (7) $C = \mathfrak{h}$, senão C conteria um elemento nilpotente não-nulo x por (1) e (2). $\operatorname{ad} x$ é nilpotente e comuta com $\operatorname{ad} y$ para todo $y \in C$ por (6) donde $\operatorname{ad} x \operatorname{ad} y$ é nilpotente e portanto $\kappa(x, y) = \operatorname{Tr}(\operatorname{ad} x \operatorname{ad} y) = 0$, contrariando o Corolário 61. ∎

Corolário 63 *A restrição de κ a $\mathfrak{h}$ é não-degenerada.*

Se $t \in \mathfrak{h}$, a aplicação $h \mapsto \kappa(t, h)$ define uma aplicação linear $\alpha_t : \mathfrak{h} \to F$. Além disso, se $t, u \in \mathfrak{h}$ e $a, b \in F$, então $\alpha_{at+bu}(h) = a\alpha_t(h) + b\alpha_u(h)$, pela bilinearidade de κ. Isto define uma aplicação linear $\phi : \mathfrak{h} \to \mathfrak{h}^*$ tal que $t \mapsto \alpha_t$ cujo núcleo é zero pois κ é não-degenerada em $\mathfrak{h}$. Como $\dim \mathfrak{h} = \dim \mathfrak{h}^* < \infty$, temos que ϕ é um isomorfismo entre $\mathfrak{h}$ e $\mathfrak{h}^*$. Isto nos permite identificar estes dois espaços do seguinte modo: para cada $\alpha \in \mathfrak{h}^*$ corresponde o (único) elemento $t_\alpha \in \mathfrak{h}$ satisfazendo a equação

$$\alpha(h) = \kappa(t_\alpha, h), \text{ para todo } h \in \mathfrak{h}. \tag{2.9}$$

Particularmente, Φ corresponde ao subconjunto $\{t_\alpha : \alpha \in \Phi\}$ de $\mathfrak{h}$.

2.6.2 Propriedades da decomposição do espaço por raízes

O objetivo desta subseção é obter uma caracterização precisa da decomposição do espaço por raízes e, particularmente, uma caracterização do conjunto de raízes Φ. A partir desta caracterização, e da correspondência que será estabelecida entre as álgebras de Lie semisimples e tais conjuntos, poderemos obter uma classificação completa das álgebras de Lie semisimples de dimensão finita. A seguinte proposição nos fornece propriedades de ortogonalidade entre os espaços de raízes.

Proposição 64 *(a) Φ gera $\mathfrak{h}^*$.*

(b) Se $\alpha \in \Phi$, então $-\alpha \in \Phi$.

(c) Se $\alpha \in \Phi$, $x \in \mathfrak{g}_\alpha$, e $y \in \mathfrak{g}_{-\alpha}$, então $[xy] = \kappa(x, y)t_\alpha$, onde t_α é tal como em (2.9).

(d) Para todo $\alpha \in \Phi$, $[\mathfrak{g}_\alpha \mathfrak{g}_{-\alpha}]$ é unidimensional, com base t_α.

(e) $\alpha(t_\alpha) = \kappa(t_\alpha, t_\alpha) \neq 0$, para todo $\alpha \in \Phi$.

(f) Se $\alpha \in \Phi$ e x_α é qualquer elemento não-nulo de $\mathfrak{g}_\alpha$, então existe $y_\alpha \in \mathfrak{g}_{-\alpha}$ tal que x_α, y_α, e $h_\alpha = [x_\alpha y_\alpha]$ geram uma subálgebra tridimensional de $\mathfrak{g}$ isomorfa a $\mathfrak{sl}(2, F)$.

(g) $h_\alpha = \dfrac{2t_\alpha}{\kappa(t_\alpha, t_\alpha)}$ *e* $h_\alpha = -h_{-\alpha}$.

Prova. (a) Se Φ não gera $\mathfrak{h}^*$, i.é, $\langle\Phi\rangle \subsetneq \mathfrak{h}^*$, então $0 \neq \langle\Phi\rangle^\perp \subset \mathfrak{h}$. Em particular, devemos ter um elemento não-nulo $h \in \mathfrak{h}$ tal que $\alpha(h) = 0$, para toda $\alpha \in \Phi$. Isto significa que $[h, \mathfrak{g}_\alpha] = \alpha(h)\mathfrak{g}_\alpha = 0$, para todo $\alpha \in \Phi$, o que por sua vez significa $[h\mathfrak{g}] = 0$, ou seja, $h \in Z(\mathfrak{g}) = 0$, o que é impossível.

(b) Seja $\alpha \in \Phi$. Se $-\alpha \notin \Phi$, isto é, $\mathfrak{g}_{-\alpha} = 0$, então, pela Proposição 60, devemos ter $\kappa(\mathfrak{g}_\alpha, \mathfrak{g}_\beta) = 0$, para todo $\beta \in \mathfrak{h}^*$. Como κ é não degenerada, isto obriga $\mathfrak{g}_\alpha = 0$, o que é absurdo.

(c) Sejam $\alpha \in \Phi$, $x \in \mathfrak{g}_\alpha$, e $y \in \mathfrak{g}_{-\alpha}$. Escolhemos $h \in \mathfrak{h}$ arbitrário, e obtemos um (único) $t_\alpha \in \mathfrak{h}$, tal que $\alpha(h) = \kappa(t_\alpha, h)$. Assim, temos

$$\begin{aligned} \kappa(h, [xy] - \kappa(x, y)t_\alpha) &= \kappa(h, [xy]) - \kappa(x, y)\kappa(h, t_\alpha) \\ &= \kappa([hx], y) - \alpha(h)\kappa(x, y) \\ &= \alpha(h)\kappa(x, y) - \alpha(h)\kappa(x, y) = 0. \end{aligned}$$

Mas, claramente, $[xy] \in \mathfrak{h}$, e a restrição de κ a $\mathfrak{h}$ é não-degenerada, portanto $[xy] = \kappa(x, y)t_\alpha$. Isto mostra, ainda, que $[\mathfrak{g}_\alpha\mathfrak{g}_{-\alpha}]$, se não-nulo, é gerado por t_α.

(d) Basta mostrar que se $\alpha \in \Phi$, então $[\mathfrak{g}_\alpha\mathfrak{g}_{-\alpha}] \neq 0$. Temos certamente $\kappa(\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}) \neq 0$, pois do contrário, $\kappa(\mathfrak{g}_\alpha, \mathfrak{g}) = 0$, o que não é possível. Particularmente, existem $x \in \mathfrak{g}_\alpha$ e $y \in \mathfrak{g}_{-\alpha}$ tais que $\kappa(x, y) \neq 0$ e, conseqüentemente, $0 \neq [xy] = \kappa(x, y)t_\alpha \in [\mathfrak{g}_\alpha\mathfrak{g}_{-\alpha}]$, como queríamos.

(e) Suponhamos $\alpha(t_\alpha) = 0$, de modo que $[t_\alpha, x] = 0 = [t_\alpha y]$, para todo $x \in \mathfrak{g}_\alpha$, $y \in \mathfrak{g}_{-\alpha}$. Como no item (d), podemos encontrar tais x e y satisfazendo $\kappa(x, y) \neq 0$. Multiplicando x ou y por um escalar conveniente, podemos supor que $\kappa(x, y) = 1$, e daí $[xy] = t_\alpha$. Segue que o subespaço S de $\mathfrak{g}$ gerado por x, y, t_α é uma álgebra solúvel tridimensional e $S \simeq \operatorname{ad}_\mathfrak{g} S \subset \mathfrak{gl}(\mathfrak{g})$. Em particular, $\operatorname{ad}_\mathfrak{g} s$ é nilpotente para todo $s \in [SS]$, de modo que, $\operatorname{ad}_\mathfrak{g} t_\alpha$ é simultaneamente semisimples e nilpotente, i.é, $\operatorname{ad}_\mathfrak{g} t_\alpha = 0$. Isto significa que $t_\alpha \in Z(\mathfrak{g}) = 0$, contrariando a nossa escolha de t_α.

(f) Dado $0 \neq x_\alpha \in \mathfrak{g}_\alpha$, encontramos $y_\alpha \in \mathfrak{g}_{-\alpha}$ tal que $\kappa(x_\alpha, y_\alpha) = \dfrac{2}{\kappa(t_\alpha, t_\alpha)}$, o que é possível pelo item (e) e pelo fato que $\kappa(x_\alpha, \mathfrak{g}_{-\alpha}) \neq 0$. Definimos $h_\alpha = \dfrac{2t_\alpha}{\kappa(t_\alpha, t_\alpha)}$. Então $[x_\alpha y_\alpha] = h_\alpha$, por (c). Além disso, $[h_\alpha x_\alpha] = \dfrac{2}{\alpha(t_\alpha)}[t_\alpha x_\alpha] = \dfrac{2\alpha(t_\alpha)}{\alpha(t_\alpha)} x_\alpha = 2x_\alpha$. De modo semelhante, $[h_\alpha y_\alpha] = -2y_\alpha$. Assim, $x_\alpha, y_\alpha, h_\alpha$ geram uma subálgebra tridimensional de $\mathfrak{g}$ que tem a mesma tábua de multiplicação que $\mathfrak{sl}(2, F)$.

(g) Recordando a definição de t_α, este item fica imediato.

■

Para cada par de raízes $(\alpha, -\alpha)$, a Proposição 64 nos fornece uma subálgebra $S_\alpha \cong \mathfrak{sl}(2, F)$ de $\mathfrak{g}$. Na seção 2.5, estudamos detalhadamente os S_α-módulos de dimensão finita. Esse estudo pode agora ser proveitosamente aplicado para obtermos propriedades de integralidade da decomposição do espaço por raízes.

Inicialmente, fixemos uma raíz $\alpha \in \Phi$, e consideremos o subespaço M de $\mathfrak{g}$ gerado por $\mathfrak{g}_0 = \mathfrak{h}$ juntamente com todos os espaços de raízes da forma $\mathfrak{g}_{c\alpha}$ para $c \in F$. Devido à Proposição 60, M é claramente um S_α-submódulo de $\mathfrak{g}$ contendo o próprio S_α como um S_α-submódulo. Se $x \in \mathfrak{g}_{c\alpha}$, temos $h_\alpha \cdot x = [h_\alpha x] = c\alpha(h_\alpha)x = 2cx$, de modo que, pelo Teorema 56, os pesos de h_α em M são os inteiros 0 e $2c$. Em particular, todos os c devem ser múltiplos inteiros de $1/2$.

O S_α-submódulo irredutível S_α de M contabiliza uma ocorrência do peso 0 e S_α age trivialmente sobre $\operatorname{Ker} \alpha$, de modo que, estes dois S_α-submódulos exaurem as possíveis ocorrências do peso 0. Com isto, exaurem também as possíveis ocorrências dos pesos pares em M. Portanto, os únicos pesos pares ocorrendo em M são 0 e ± 2. Isto significa que $2\alpha \notin \Phi$, i.é, *duas vezes uma raiz não pode ser uma raiz*, ou teríamos uma ocorrência do peso 4. Por este mesmo argumento, $\frac{1}{2}\alpha$ não pode ser uma raiz e, conseqüentemente, 1 não pode ocorrer como peso de h_α em M (assim como nenhum peso ímpar). Pelo Corolário 57, temos então $M = \mathfrak{h} + S_\alpha$ (a soma não é direta pois $\mathfrak{h} \cap S_\alpha = Fh_\alpha$). Particularmente, o peso 2 ocorre com multiplicidade 1 donde $\dim \mathfrak{g}_\alpha = 1$, e S_α fica unicamente determinada como a subálgebra de $\mathfrak{g}$ gerada por $\mathfrak{g}_\alpha$ e $\mathfrak{g}_{-\alpha}$. Além disso, os únicos valores não-nulos de c são ± 1, donde os únicos múltiplos inteiros de uma raiz α são $\pm\alpha$.

Na seqüência, vamos examinar a ação de S_α sobre os espaços de raízes $\mathfrak{g}_\beta$ com $\beta \neq \pm\alpha$. Definimos $K = \sum_{i \in \mathbb{Z}} \mathfrak{g}_{\beta+i\alpha}$. S_α age sobre cada espaço de raízes unidimensional $\mathfrak{g}_{\beta+i\alpha}$ levando-o em $\mathfrak{g}_{\beta+(i-1)\alpha} \oplus \mathfrak{g}_{\beta+i\alpha} \oplus \mathfrak{g}_{\beta+(i+1)\alpha} \subset K$ de modo que K é um S_α-submódulo de $\mathfrak{g}$ consistindo inteiramente de espaços de raízes unidimensionais correspondentes aos pesos inteiros distintos e não-nulos $\beta(h_\alpha) + 2i$ (para os valores de $i \in \mathbb{Z}$ tais que $\beta + i\alpha \in \Phi$). Estes são todos pares ou todos ímpares (dependendo do valor de $\beta(h_\alpha)$), de modo que os pesos 0 e 1 não podem ocorrer simultaneamente em K como pesos desta forma, logo estes formam uma cadeia finita e contígua, mais precisamente, uma progressão aritmética de razão 2, a saber

$$\beta(h_\alpha) - 2r, \quad \beta(h_\alpha) - 2(r-1), \quad \ldots, \quad \beta(h_\alpha) \quad \ldots, \quad \beta(h_\alpha) + 2q,$$

onde q e r são os maiores inteiros não-negativos tais que $\beta - r\alpha, \beta + q\alpha \in \Phi$. Isto mostra que K é irredutível e essa cadeia é simétrica, i.é, $\beta(h_\alpha) + 2q = -(\beta(h_\alpha) - 2r)$, ou seja $\beta(h_\alpha) = r - q$. Vamos denominar a correspondente cadeia de raízes

$$\beta - r\alpha, \quad \beta - (r-1)\alpha, \quad \ldots, \quad \beta \quad \ldots, \quad \beta + q\alpha,$$

uma *α-cadeia por β*. Finalmente, observamos que se $\alpha, \beta, \alpha + \beta \in \Phi$, então $0 \neq [\mathfrak{g}_\alpha \mathfrak{g}_\beta] \subset \mathfrak{g}_{\alpha+\beta}$, donde $[\mathfrak{g}_\alpha \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$.

Resumimos os resultados obtidos acima na seguinte proposição.

Proposição 65 *(a) Se $\alpha \in \Phi$ então $\dim \mathfrak{g}_\alpha = 1$. Em particular, $S_\alpha = \mathfrak{g}_\alpha + \mathfrak{g}_{-\alpha} + \mathfrak{h}_\alpha$ ($\mathfrak{h}_\alpha = [\mathfrak{g}_\alpha \mathfrak{g}_{-\alpha}]$), e dado $x_\alpha \in \mathfrak{g}_\alpha$ não-nulo existe um único $y_\alpha \in \mathfrak{g}_{-\alpha}$ satisfazendo $[x_\alpha y_\alpha] = h_\alpha$.*

(b) Se $\alpha \in \Phi$ então, os únicos múltiplos escalares de α que são raízes são α e $-\alpha$.

(c) Se $\alpha, \beta \in \Phi$ então $\beta(h_\alpha) \in \mathbb{Z}$, e $\beta - \beta(h_\alpha)\alpha \in \Phi$.

(d) Se $\alpha, \beta, \alpha + \beta \in \Phi$, então $[\mathfrak{g}_\alpha \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$.

(e) Sejam $\alpha, \beta \in \Phi$, com $\beta \neq \pm\alpha$. Sejam r e q, respectivamente, o maior e o menor inteiro não-negativos para os quais $\beta - r\alpha$, $\beta + q\alpha$ sejam raízes. Então $\beta + i\alpha \in \Phi$ para todo $i = -r, \ldots, q$ e $\beta(h_\alpha) = r - q$.

(f) $\mathfrak{g}$ *é gerada (como álgebra de Lie) pelos espaços de raízes* $\mathfrak{g}_\alpha$.

Os números
$$\beta(h_\alpha) = \frac{2\kappa(t_\beta, t_\alpha)}{\kappa(t_\alpha, t_\alpha)}$$
da Proposição 65 são chamados *Inteiros de Cartan*.

Como a restrição a $\mathfrak{h}$ da forma de Killing κ de $\mathfrak{g}$ é não-degenerada ($\mathfrak{g}$ semisimples), podemos transferir a forma para $\mathfrak{h}^*$ definindo $(\alpha, \beta) = \kappa(t_\alpha, t_\beta)$, para todo $\alpha, \beta \in \mathfrak{h}^*$.

Os Inteiros de Cartan aparecerão com grande freqüência no decorrer deste capítulo, por isso definimos
$$\langle \beta, \alpha \rangle = \frac{2(\beta, \alpha)}{(\alpha, \alpha)}.$$
Uma observação importante: *esta notação é linear apenas na primeira variável.*

Sabemos que Φ gera $\mathfrak{h}^*$, o que nos permite escolher uma base $\alpha_1, \ldots, \alpha_l$ de $\mathfrak{h}^*$ consistindo unicamente de raízes. É claro que, se $\beta \in \Phi$, podemos escrevê-la unicamente como $\beta = \sum_{i=1}^{l} c_i \alpha_i$, onde $c_i \in F$. Vamos mostrar que, na verdade, os $c_i \in \mathbb{Q}$ ($\operatorname{Car} F = 0$). Para cada $j = 1, \ldots, l$, temos $(\beta, \alpha_j) = \sum_{i=1}^{l} c_i(\alpha_i, \alpha_j)$. Multiplicando ambos os lados destas igualdades por $2/(\alpha_j, \alpha_j)$, resulta um sistema linear
$$\langle \beta, \alpha_j \rangle = \sum_{i=1}^{l} \langle \alpha_i, \alpha_j \rangle \, c_i, j = 1, \ldots, l$$
cujos coeficientes são inteiros de Cartan (em particular, racionais), cuja matriz $(\langle \alpha_i, \alpha_j \rangle)_{1 \le i,j \le l}$ é inversível, pois os α_i formam uma base e a forma é não-degenerada. Conseqüentemente, este sistema tem única solução sobre $\mathbb{Q}$, como afirmamos.

Com isto, acabamos de mostrar que o $\mathbb{Q}$-subespaço $E_{\mathbb{Q}}$ de $\mathfrak{h}^*$ gerado por todas as raízes tem dimensão $l = \dim_F \mathfrak{h}^*$ sobre $\mathbb{Q}$. Ademais, para todo $\alpha, \beta \in \Phi$ temos $(\alpha, \beta) \in \mathbb{Q}$, e a forma é definida-positiva em $E_{\mathbb{Q}}$.

A $\lambda, \mu \in \mathfrak{h}^*$ correspondem os elementos $t_\lambda, t_\mu \in \mathfrak{h}$, tais que
$$(\lambda, \mu) = \kappa(t_\lambda, t_\mu) = \operatorname{Tr}(\operatorname{ad} t_\lambda \operatorname{ad} t_\mu).$$

Os elementos t_λ e t_μ agem trivialmente sobre $\mathfrak{h}$ e agem como multiplicação sobre cada espaço unidimensional $\mathfrak{g}_\alpha$ por escalares $\alpha(t_\lambda)$ e $\alpha(t_\mu)$, respectivamente. Além disso, $\operatorname{ad} t_\lambda$ e $\operatorname{ad} t_\mu$ são matrizes diagonalizáveis (simultaneamente), de modo que, o traço de seu produto é simplesmente a soma do produto dos respectivos elementos das diagonais, i.é,

$$(\lambda, \mu) = \operatorname{Tr}(\operatorname{ad} t_\lambda \operatorname{ad} t_\mu) = \sum_{\alpha\in\Phi} \alpha(t_\lambda)\alpha(t_\mu) = \sum_{\alpha\in\Phi} (\alpha, \lambda)(\alpha, \mu).$$

Particularmente, se $\beta \in \Phi$, então $0 \neq (\beta, \beta) = \sum_{\alpha\in\Phi} (\alpha, \beta)^2$. Dividindo por $(\beta, \beta)^2$, obtemos $1/(\beta, \beta) = \sum_{\alpha\in\Phi} (\alpha, \beta)/(\beta, \beta) \in \mathbb{Q}$, pois para cada $\alpha \in \Phi$, $2(\alpha, \beta)/(\beta, \beta) \in \mathbb{Z}$. Portanto, $(\beta, \beta) \in \mathbb{Q}$ e, por sua vez, $(\alpha, \beta) \in \mathbb{Q}$. Como acima, se $\lambda \in E_\mathbb{Q}$, então $(\lambda, \lambda) = \sum_{\alpha\in\Phi} (\alpha, \lambda)^2$ é um número racional positivo, a menos que $\lambda = 0$, pois a forma de Killing é não-degenerada em $\mathfrak{h}$. Assim, a forma $(\ ,\ ) : E_\mathbb{Q} \times E_\mathbb{Q} \to \mathbb{Q}$ é bilinear simétrica definida positiva, ou seja, é um produto interno em $E_\mathbb{Q}$.

Seja E o espaço vetorial real obtido através da extensão do corpo base de $\mathbb{Q}$ para $\mathbb{R}$, isto é, $E = \mathbb{R} \otimes_\mathbb{Q} E_\mathbb{Q}$. O produto interno de $E_\mathbb{Q}$ se estende canonicamente para E, tal que E é um espaço euclideano. Observemos que Φ contém uma base de E e que $\dim_\mathbb{R} E = l$.

Recordemos que uma *reflexão* em E é uma transformação linear ortogonal fixando pontualmente algum *hiperplano* (i.é, um subespaço de codimensão 1) e levando qualquer vetor ortogonal a esse hiperplano em seu oposto. Assim, observamos que todo $\alpha \in \Phi$ define uma reflexão σ_α em E através da expressão

$$\sigma_\alpha(\beta) = \beta - \langle \beta, \alpha \rangle \alpha.$$

Esta claramente fixa pontualmente o hiperplano $P_\alpha = \{\beta \in E : (\beta, \alpha) = 0\}$ e leva α em $-\alpha$. Podemos refrasear o item (c) da Proposição 65 dizendo que Φ é invariante por reflexões σ_α ($\alpha \in \Phi$) ou, equivalentemente, que tais reflexões agem como permutações dos elementos de Φ.

Esta discussão se resume na seguinte proposição.

Proposição 66 *Sejam $\mathfrak{g}$, $\mathfrak{h}$, Φ, e E como acima. Então:*

(R1) Φ é finito, gera E, e $0 \notin \Phi$.

(R2) Os únicos múltiplos de $\alpha \in \Phi$ são $\pm\alpha$.

(R3) Se $\alpha \in \Phi$ então Φ é invariante pela reflexão σ_α.

(R4) Se $\alpha, \beta \in \Phi$ então $\langle \beta, \alpha \rangle \in \mathbb{Z}$.

Um subconjunto Φ de um espaço euclideano real E com as propriedades apresentadas por essa proposição é chamado *sistema de raízes* em E. O número $l = \dim_{\mathbb{R}} E$ é chamado *posto* do sistema de raízes Φ. Humphreys [Hu, cap. III] contém uma abordagem axiomática para os sistemas de raízes. A partir de um espaço real euclideano E, este define um sistema de raízes como um subconjunto Φ de E satisfazendo os "axiomas" R1-R4.

Com o que vimos até o momento, temos estabelecido uma correspondência $(\mathfrak{g}, \mathfrak{h}) \mapsto (E, \Phi)$. Na verdade, conforme já mencionamos, pode ser mostrado que a aparente dependência da escolha de $\mathfrak{h}$ não é essencial. Ademais, pode ser mostrado que esta correspondência é realmente 1-1. Vamos assumir este fato daqui por diante.

2.6.3 Sistemas de raízes

Nesta subseção, as condições R1-R4 da Proposição 66 serão consideradas axiomas sobre um subconjunto Φ de um espaço euclideano E (i.é, um espaço vetorial real de dimensão finita dotado de produto interno). Φ é um sistema de raízes em E se satisfizer R1-R4. Esta abordagem evidentemente inclui os subconjuntos Φ dos espaços E construídos na subseção anterior. Vamos usar um pouco da geometria euclideana para obter uma caracterização mais precisa dos sistemas de raízes. Na verdade, pretendemos estabelecer adiante uma classificação completa desses objetos e, conseqüentemente, uma classificação das álgebras de Lie semisimples.

O subgrupo $\mathcal{W}$ de $\mathrm{GL}(E)$ gerado por todas as reflexões σ_α ($\alpha \in \Phi$) é chamado *Grupo de Weyl* e tem papel fundamental no que se segue. Por (R3), $\mathcal{W}$ age como um grupo de permutações de Φ e, por (R1), gera Φ e é finito. Isto permite-nos enxergar $\mathcal{W}$ como um subgrupo do grupo simétrico do conjunto Φ (i.é, o menor grupo simétrico agindo transitivamente sobre Φ). Com efeito, os dois lemas seguintes nos permitem afirmar que dois sistemas de raízes "isomorfos" têm mesmo grupo de Weyl.

Lema 67 *Seja Φ um conjunto finito de geradores de E e suponhamos que Φ seja invariante por todas as reflexões σ_α ($\alpha \in \Phi$). Se Φ é invariante por $\sigma \in \mathrm{GL}(E)$, o qual fixa pontualmente um hiperplano P de E e leva algum vetor não-nulo $\alpha \in \Phi$ em seu oposto, então $\sigma = \sigma_\alpha$.*

Prova. Seja $\tau = \sigma\sigma_\alpha (= \sigma\sigma_\alpha^{-1})$. Então τ fixa Φ e α e age como identidade no subespaço $\mathbb{R}\alpha$ e no quociente $E/\mathbb{R}\alpha$. Assim 1 é o único autovalor de τ e o polinômio minimal de τ divide $(X-1)^l$, onde $l = \dim E$. Por outro lado, se $\beta \in \Phi$ e k é a cardinalidade de Φ (que é finita), nem todos os vetores $\beta, \tau(\beta), \ldots, \tau^k(\beta)$ podem ser distintos, i.é, alguma potência de τ fixa β. Escolhamos k suficientemente grande para que τ^k fixe todos os $\beta \in \Phi$. Como Φ gera E, τ^k fixa alguma base contida em Φ, portanto $\tau^k = 1$. Isto significa que o polinômio minimal de τ divide $X^k - 1$. Conseqüentemente, esse polinômio é exatamente $X - 1 = \text{mdc}(X^k - 1, (X-1)^l)$, o que implica $\tau = 1$. ■

Lema 68 *Seja Φ um sistema de raízes em E com grupo de Weyl $\mathcal{W}$. Se $\sigma \in \mathrm{GL}(E)$ deixa Φ invariante, então $\sigma\sigma_\alpha\sigma^{-1} = \sigma_{\sigma(\alpha)}$ para todo $\alpha \in \Phi$, e $\langle \beta, \alpha \rangle = \langle \sigma(\beta), \sigma(\alpha) \rangle$ para todo $\alpha, \beta \in \Phi$.*

Prova. Como $\sigma_\alpha(\beta) \in \Phi$, temos $\sigma\sigma_\alpha\sigma^{-1}(\sigma(\beta)) = \sigma\sigma_\alpha(\beta) \in \Phi$. Esta igualdade equivale a $\sigma(\beta - \langle \beta, \alpha \rangle \alpha) = \sigma(\beta) - \langle \beta, \alpha \rangle \sigma(\alpha)$. Como $\sigma|_\Phi$ age transitivamente sobre Φ, concluímos que $\sigma\sigma_\alpha\sigma^{-1}$ deixa Φ invariante. Ademais, $\sigma\sigma_\alpha\sigma^{-1}$ fixa o hiperplano $\sigma(P_\alpha)$ e leva $\sigma(\alpha)$ em $-\sigma(\alpha)$. Pelo Lema 67, temos $\sigma\sigma_\alpha\sigma^{-1} = \sigma_{\sigma(\alpha)}$. Comparando a equação acima com a equação $\sigma_{\sigma(\alpha)}(\sigma(\beta)) = \sigma(\beta) - \langle \sigma(\beta), \sigma(\alpha) \rangle \sigma(\alpha)$, completamos a prova do lema. ■

Um *isomorfismo* entre dois sistemas de raízes Φ e Φ' em respectivos espaços euclideanos E e E' é um isomorfismo de espaços vetoriais (não necessariamente uma isometria) $\varphi : E \to E'$, que leva Φ sobre Φ' tal que $\langle \varphi(\beta), \varphi(\alpha) \rangle = \langle \beta, \alpha \rangle$ para todo $\beta, \alpha \in \Phi$. Segue que

$$\begin{aligned}
(\sigma_{\varphi(\alpha)} \circ \varphi)(\beta) &= \varphi(\beta) - \langle \varphi(\beta), \varphi(\alpha) \rangle \varphi(\alpha) \\
&= \varphi(\beta) - \langle \beta, \alpha \rangle \varphi(\alpha) \\
&= \varphi(\beta - \langle \beta, \alpha \rangle \alpha) \\
&= (\varphi \circ \sigma_\alpha)(\beta),
\end{aligned}$$

isto é, temos uma correspondência bijetora $\sigma_\alpha \mapsto \sigma_{\varphi(\alpha)} = \varphi \circ \sigma_\alpha \circ \varphi^{-1}$, para todo $\alpha \in \Phi$. Esta se estende claramente a um isomorfismo natural $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ entre os grupos de Weyl $\mathcal{W}$ de Φ e $\mathcal{W}'$ de Φ', respectivamente. O Lema 68 nos assegura que *um automorfismo de Φ é precisamente um automorfismo de E fixando* Φ. Em particular, podemos enxergar $\mathcal{W}$ como um subgrupo de $\mathrm{Aut}\,\Phi$.

O axioma R4 impõe uma severa limitação nos possíveis ângulos ocorrendo entre pares de raízes. Recordamos que o cosseno do ângulo θ entre dois vetores $\alpha, \beta \in E$ é dado pela fórmula $\|\alpha\|\|\beta\| \cos\theta = (\alpha, \beta)$. Portanto,

$$\langle \beta, \alpha \rangle = \frac{2(\beta, \alpha)}{(\alpha, \alpha)} = 2\frac{\|\beta\|}{\|\alpha\|} \cos\theta$$

e daí,

$$\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle = 4\cos^2\theta.$$

Este número deve ser um inteiro não-negativo. Mas, $0 \leq \cos^2\theta \leq 1$, e $\langle \alpha, \beta \rangle$ e $\langle \beta, \alpha \rangle$ têm mesmo sinal, resultando nas possibilidades listadas na seguinte tabela quando $\alpha \neq \beta$, e $\|\beta\| \geq \|\alpha\|$:

$\langle \alpha, \beta \rangle$	$\langle \beta, \alpha \rangle$	θ	$\|\beta\|^2 / \|\alpha\|^2$
0	0	$\pi/2$	indet.
1	1	$\pi/3$	1
-1	-1	$2\pi/3$	1
1	2	$\pi/4$	2
-1	-2	$3\pi/4$	2
1	3	$\pi/6$	3
-1	-3	$5\pi/6$	3

(2.10)

A partir da informação contida nesta tabela podemos obter um critério simples, porém muito útil, expresso no seguinte lema.

Lema 69 *Sejam α, β duas raízes tais que $\beta \neq \pm\alpha$. Se $(\alpha, \beta) > 0$ então $\alpha - \beta$ é uma raiz, se $(\alpha, \beta) < 0$ então $\alpha + \beta$ é uma raiz, e se $(\alpha, \beta) = 0$, então $\alpha - \beta \in \Phi \Leftrightarrow \alpha + \beta \in \Phi$.*

Prova. Inicialmente, note que (α, β) e $\langle \alpha, \beta \rangle$ têm o mesmo sinal. A tabela mostra que $\langle \beta, \alpha \rangle$ ou $\langle \alpha, \beta \rangle$ é igual a ± 1. Se $\langle \alpha, \beta \rangle = \pm 1$, então $\sigma_\beta(\alpha) = \alpha \pm \beta \in \Phi$. Se $\langle \beta, \alpha \rangle = \pm 1$, então $\beta \pm \alpha \in \Phi$, e portanto $\sigma_{\beta \pm \alpha}(\beta \pm \alpha) = \alpha \pm \beta \in \Phi$.

A segunda afirmação segue da primeira, aplicada a $-\beta$ ao invés de β enquanto que a última afirmação é óbvia. $\blacksquare$

Sejam α, β duas raízes tais que $\beta \neq \pm\alpha$. Consideremos a α-cadeia por β, isto é, todas as raízes da forma $\beta + i\alpha$, para $i \in \mathbb{Z}$. Sejam r, q os maiores inteiros não-negativos tais que $\beta - r\alpha$ e $\beta + q\alpha$ são raízes (os quais existem devido a R1). Então a cadeia de raízes iniciando em $\beta - r\alpha$ e terminando em $\beta + q\alpha$ é ininterrupta, isto é, forma uma progressão aritmética

$$\beta - r\alpha, \quad \beta - (r-1)\alpha, \quad \ldots, \quad \beta \quad \ldots, \quad \beta + (q-1)\alpha, \quad \beta + q\alpha.$$

de razão α. (cf. prop. 65e). Do contrário, existem inteiros p, s tais que $-r \leq p < s \leq q$ tais que $\beta + p\alpha \in \Phi$, $\beta + (p+1)\alpha \notin \Phi$, $\beta + (s-1)\alpha \notin \Phi$ e $\beta + s\alpha \in \Phi$. Nesse caso, pelo Lema 68, devemos ter simultaneamente $(\alpha, \beta + p\alpha) \geq 0$ e $(\alpha, \beta + s\alpha) \leq 0$, o que é absurdo, pois $p < s$ e $(\alpha, \alpha) > 0$.

Notemos que σ_α apenas soma ou subtrai um múltiplo de α (possivelmente 0) a qualquer raiz, logo a cadeia é invariante por σ_α. Como $\sigma_\alpha(\beta + i\alpha) = \beta - i\alpha - \langle \beta, \alpha \rangle \alpha$ $(-r \leq i \leq q)$, cada elemento da cadeia refletida por α é exatamente o respectivo elemento da progressão aritmética de razão α

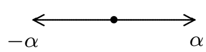
$$\beta - q\alpha, \quad \beta - (q-1)\alpha, \quad \ldots, \quad \beta \quad \ldots, \quad \beta + (r-1)\alpha, \quad \beta + r\alpha.$$

deslocado do fator constante $-\langle \beta, \alpha \rangle \alpha$. Esta cadeia refletida deve coincidir com a cadeia original (que é invariante por σ_α), tornando claro que, geometricamente, σ_α reverte os elementos da cadeia. Em particular, a cadeia refletida inicia-se com a raiz $\sigma_\alpha(\beta + q\alpha) = \beta - q\alpha - \langle \beta, \alpha \rangle \alpha$, a qual deve ser igual a $\beta - r\alpha$ (pela definição de r). Portanto, devemos ter $\langle \beta, \alpha \rangle = r - q$.

A tabela (2.10) permite-nos então concluir que uma α-cadeia por β contém no máximo quatro raízes. Com efeito, temos $3 \geq \langle \beta + q\alpha, \alpha \rangle = \langle \beta, \alpha \rangle + q \langle \alpha, \alpha \rangle = r - q + 2q = r + q \geq 0$, donde o comprimento da α-cadeia por β é $r + q + 1 \leq 4$ (cf. Jacobson [Ja, IV, pág. 117] para uma prova diferente, porém muito interessante).

Quando o posto l do sistema de raízes Φ é menor ou igual a 2 podemos representá-lo simplesmente desenhando uma figura, conforme veremos nos exemplos seguintes.

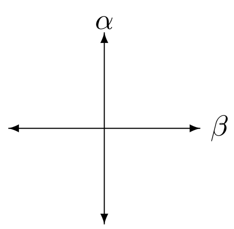
Exemplo 70 (Posto 1) Em vista de (R2), no caso unidimensional a única possibilidade é o sistema de raízes A_1,



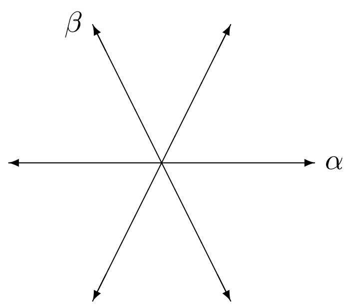
correspondente à álgebra de Lie $\mathfrak{sl}(2, F)$. $\square$

Exemplo 71 (Posto 2) No caso bidimensional, notemos que (R3) determina a constância do ângulo entre duas raízes adjacentes quaisquer. De acordo com a tabela (2.10), esse ângulo pode ser qualquer um dos quatro ângulos $\pi/2$, $\pi/3$, $\pi/4$, $\pi/6$. Com excessão do primeiro ângulo, o comprimento relativo entre as raízes fica determinado pela propriedade (R4). Portanto, a menos de múltiplos escalares, há exatamente quatro sistemas de raízes com posto 2, representados na figura abaixo, para cada um desses ângulos respectivamente.

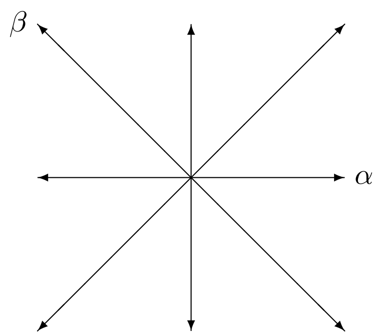
$A_1 \times A_1$



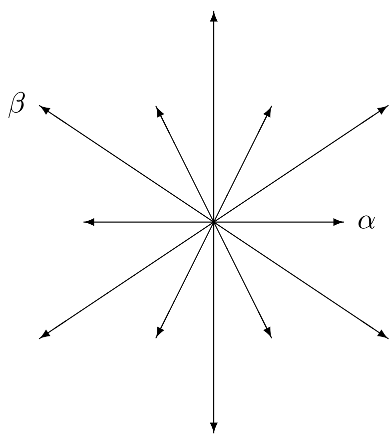
A_2



B_2



G_2



Os três primeiros sistemas de raízes correspondem às álgebras clássicas $\mathfrak{sl}(2, F) \oplus \mathfrak{sl}(2, F) \cong$

$\mathfrak{so}(4, F)$, $\mathfrak{sl}(3, F)$ e $\mathfrak{so}(5, F) \cong \mathfrak{sp}(4, F)$, respectivamente. O sistema G_2 não corresponde a nenhuma das álgebras clássicas. Porém, pode ser mostrado que existe de fato uma álgebra de Lie (excepcional) de posto 2 cujo sistema de raízes é G_2 (cf. Humphreys [Hu, §12.1]).

Observando que $\sigma_\alpha \sigma_\beta$ é uma rotação de ângulo 2θ, onde θ é o ângulo entre as raízes α e β, claramente a ordem de $\sigma_\alpha \sigma_\beta$ é 2, 3, 4 e 6, para cada um dos respectivos ângulos $\theta = \pi/2$, $\pi/3$ (ou $2\pi/3$), $\pi/4$ (ou $3\pi/4$) e $\pi/6$ (ou $5\pi/6$). Para cada sistema de raízes deste exemplo, é evidente que $\sigma_\alpha \sigma_\beta$ e σ_α (ou σ_β) são geradores para o grupo de Weyl. Assim, se D_n é o grupo diedral de ordem $2n$, temos que os grupos de Weyl dos sistemas $A_1 \times A_1$, A_2, B_2 e G_2 são respectivamente D_2, D_3, D_4 e D_6. □

2.6.4 Raízes simples

Como na subseção anterior, Φ denota um sistema de raízes de posto l no espaço euclideano E com grupo de Weyl $\mathcal{W}$. De acordo com R1, Φ contém geradores de E; em particular contém uma base de E. Dentre as possíveis bases de E vamos destacar aquelas com uma propriedade adicional e reservar o termo base para designar precisamente tais conjuntos (em ingles há duas palavras para designar base: **basis** designa uma base no sentido familiar, enquanto que **base** refere-se a uma particular base com determinada propriedade. Como não temos esta distinção em português, vamos empregar o mesmo termo - base - para indicar ambos os casos, sem observações, quando o contexto assim o permitir).

Definição 72 (Base para um sistema de raízes) *Um subconjunto Δ de Φ é uma* base *se satisfizer as condições*

(B1) Δ é uma base E no sentido usual.

(B2) Cada raiz β pode ser escrita como combinação linear $\sum_{\alpha \in \Phi} k_\alpha \alpha$, com coeficientes inteiros k_α todos não-negativos ou todos não-positivos.

As raízes de Δ são chamadas *simples*. Devido a B1, a cardinalidade de Δ é l e a expressão para β é única. Isto nos permite definir a *altura* de uma raiz β (em relação a Δ) por $\mathrm{ht}\,\beta = \sum_{\alpha \in \Delta} k_\alpha$. Se todos os k_α forem positivos (respec. negativos) dizemos que β é positiva (respec. negativa) e escrevemos $\beta \succ 0$ (respec. $\beta \prec 0$). Com isto, Δ define uma relação de ordem parcial em E: $\beta \prec \alpha \Leftrightarrow \alpha - \beta$ é uma soma de raízes positivas (equivalentemente, de raízes simples). Desse modo, Φ é a reunião disjunta dos conjuntos Φ^+ e Φ^- das raízes positivas e das raízes negativas, respectivamente.

O único problema com a Definição 72 é que ela não garante a existência de uma base em Φ. Reparemos que as raízes α e β dos exemplos (70) e (71) formam uma base de E. Não obstante, pode ser mostrado (cf. Humphreys [Hu, §10.1]) que Φ tem sempre uma base.

Seja Δ uma base fixada de Φ. Vamos agora estabelecer alguns resultados muito úteis envolvendo as raízes simples.

Lema 73 *Para todo $\alpha, \beta \in \Delta$, com $\alpha \neq \beta$, temos $(\beta, \alpha) \leq 0$ (i.é, o ângulo entre β e α é obtuso), e $\alpha - \beta$ não é uma raiz.*

Prova. Suponhamos $(\beta, \alpha) > 0$. Então $\alpha - \beta$ é uma raiz, violando a condição B2, sendo esta uma combinação de raízes simples misturando sinais nos coeficientes. ∎

Lema 74 *Seja α uma raiz simples. Então σ_α permuta as raízes positivas distintas de α.*

Prova. Seja $\beta \in \Phi^+ - \{\alpha\}$. Então $\beta = \sum_{\gamma \in \Delta} k_\gamma \gamma$, com os $k_\gamma \geq 0$ e inteiros. Claramente $\beta \neq \pm\alpha$, logo $k_\gamma > 0$ para algum $\gamma \neq \alpha$. Porém, o coeficiente de γ em $\sigma_\alpha(\beta) = \beta - \langle \beta, \alpha \rangle \alpha$ ainda é k_γ. Em outras palavras, $\sigma_\alpha(\beta)$ tem ao menos um coeficiente positivo (em relação a Δ), obrigando-a a ser positiva. Ademais, $\sigma_\alpha(\beta) \neq \alpha$, pois α é a imagem de $-\alpha$. ∎

Corolário 75 *Seja $\delta = \dfrac{1}{2} \sum_{\beta \succ 0} \beta$. Então $\sigma_\alpha(\delta) = \delta - \alpha$, para todo $\alpha \in \Delta$.*

O sistema de raízes Φ é dito *irredutível* se não puder ser particionado numa união disjunta de dois subconjuntos próprios tais que cada raiz de um dos subconjuntos seja ortogonal a todas as raízes do outro subconjunto. Por exemplo, A_1, A_2, B_2, G_2 são irredutíveis, enquanto que $A_1 \times A_1$ não é irredutível. Como seria esperado, podemos fazer a mesma classificação sobre a redutibilidade de Φ olhando apenas para uma de suas bases Δ [Hu, §10.4], isto é, Φ é irredutível se, e só se, Δ não puder ser particionado da maneira prescrita acima.

Suponhamos que Φ não seja irredutível. Então $\Delta = \Delta_1 \cup \cdots \cup \Delta_t$ é uma partição de Δ em subconjuntos mutuamente ortogonais. Seja E_i o subespaço de E gerado pelo conjunto Δ_i.

Claramente, $E = E_1 \oplus \cdots \oplus E_t$ é uma soma direta ortogonal. Além disso, os conjuntos Φ_i consistindo das $\mathbb{Z}$-combinações lineares dos elementos de Δ_i formam sistemas de raízes em E_i, cujo grupo de Weyl é dado simplesmente pela restrição do subgrupo de $\mathcal{W}$ gerado por todas as reflexões σ_α com $\alpha \in \Delta_i$. Cada E_i é invariante sob $\mathcal{W}$, uma vez que $\alpha \notin \Delta_i$ implica σ_α age trivialmente sobre E_i. Finalmente, é claro que se uma reflexão σ_α deixa E_i invariante, então ou $\alpha \in E_i$, ou $E_i \subset P_\alpha$. Pela ortogonalidade, esta segunda condição não pode ocorrer, logo $\alpha \in E_i$. Segue que cada raiz está contida unicamente em um dos E_i, isto é, $\Phi = \Phi_1 \cup \cdots \cup \Phi_t$ (reunião disjunta). Com isto, mostramos a seguinte proposição.

Proposição 76 *Φ se decompõe (unicamente) como a reunião disjunta de sistemas de raízes irredutíveis Φ_i em respectivos subespaços E_i de E e $E = E_1 \oplus \cdots \oplus E_t$ é uma soma direta ortogonal.*

Lema 77 *Seja Φ irredutível. Então $\mathcal{W}$ age irredutivelmente sobre E. Particularmente, uma $\mathcal{W}$-órbita de uma raiz α gera E.*

Prova. Dada $\alpha \in \Phi$, a $\mathcal{W}$-órbita de α é o subconjunto não-vazio $\mathcal{W}_\alpha = \{\sigma(\alpha) : \sigma \in \mathcal{W}\}$ de E. O subespaço de E gerado por $\mathcal{W}_\alpha$ é claramente $\mathcal{W}$-invariante, logo, a segunda afirmação do lema segue da primeira.

Consideremos um subespaço não-nulo e $\mathcal{W}$-invariante E' de E. O complemento ortogonal E'' de E' em E é também $\mathcal{W}$-invariante, e $E = E' \oplus E''$. Se $\alpha \in \Phi$, então ou $\alpha \in E'$ ou $E' \subset P_\alpha$, pois $\sigma_\alpha(E') = E'$. Portanto, cada raiz está num subespaço ou no outro, particionando Φ em dois subconjuntos mutuamente ortogonais. Conseqüentemente, um ou outro subconjunto deve ser vazio. Concluímos que $E' = E$, pois Φ gera E. ∎

Lema 78 *Seja Φ irredutível. Então ocorrem no máximo dois comprimentos de raízes em Φ.*

Prova. Sejam α e β duas raízes arbitrárias e $\mathcal{W}_\alpha$ a $\mathcal{W}$-órbita de α. Pelo Lema 77, $\mathcal{W}_\alpha$ gera E, logo nem todos os elementos de $\mathcal{W}_\alpha$ podem ser ortogonais a β. Se $(\alpha, \beta) \neq 0$, a tabela (2.10) nos mostra que os possíveis quocientes dos quadrados comprimentos de α e de β são 1, 2, 3, 1/2, e 1/3. Assim, se houvesse um terceiro comprimento de raiz, estas duas observações garantiriam a ocorrência de um quociente 3/2, o que é impossível. ∎

Quando Φ for irredutível contendo dois comprimentos distintos de raízes, distinguiremos as raízes em *raízes curtas* e *raízes longas*. Por convenção, se Φ tiver um único comprimento de raiz, estas serão ditas longas.

2.6.5 Teorema de Classificação

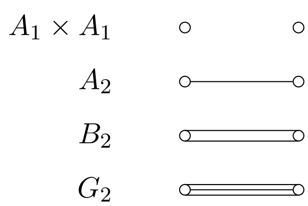
Vamos classificar completamente os sistemas de raízes irredutíveis, o que equivale a classificar completamente as álgebras de Lie semisimples de dimensão finita. De acordo com o Teorema de Classificação e com o Teorema de Existência e Unicidade, há uma, e apenas uma, álgebra de Lie simples de dimensão finita (a menos de isomorfismos) cujo sistema de raízes corresponde a A_l $(l \geq 1)$, B_l $(l \geq 2)$, C_l $(l \geq 3)$, D_l $(l \geq 4)$, E_6, E_7, E_8, F_4 e G_2. Por razões de brevidade, não vamos rever o teorema de existência e de unicidade, nem fazer a construção explícita de cada um dos sistemas obtidos (cf. Humphreys [Hu, §18-§19]).

Fixada uma base ordenada de raízes simples $(\alpha_1, \ldots, \alpha_l)$, definimos a *Matriz de Cartan* de Φ como a matriz $(\langle \alpha_i, \alpha_j \rangle)$ formada com os *Inteiros de Cartan*. Por exemplo, considerando o posto 2 temos as matrizes

$$A_1 \times A_1 \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad A_2 \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}, \quad B_2 \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}, \quad G_2 \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

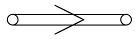
O grupo de Weyl $\mathcal{W}$ age transitivamente sobre a coleção das bases de Φ (cf. Humphreys [Hu, §10.3]), logo, a Matriz de Cartan independe da escolha de Δ (mas depende da ordem escolhida, o que não é muito sério). Além disso, a matriz de Cartan é não-singular, pois Δ é uma base de E no sentido usual, e esta caracteriza Φ completamente.

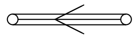
Sejam α e β duas raízes positivas distintas. Então a tabela (2.10) fornece-nos $\langle \beta, \alpha \rangle \langle \alpha, \beta \rangle =$ 0, 1, 2, ou 3. Definimos o *Grafo de Coxeter* de Φ como o grafo constituído de l vértices, sendo o i-ésimo vértice conectado ao j-ésimo vértice por $\langle \alpha_i, \alpha_j \rangle \langle \alpha_j, \alpha_i \rangle$ arestas. Por exemplo:



Nos casos em que os vértices do grafo de Coxeter são desconectados ou conectados por apenas uma aresta, os inteiros de Cartan $\langle \alpha_i, \alpha_j \rangle = \langle \alpha_j, \alpha_i \rangle$ ficam determinados. Porém, quando algum par de vértices do grafo for conectado por dois ou três vértices, não será possível determinar qual dos vértices corresponde a uma raiz curta e qual corresponde a uma raiz longa. Como os comprimentos relativos entre as raízes não são afetados pela ação do grupo Weyl, esse grupo fica completamente determinado pelo grafo de Coxeter.

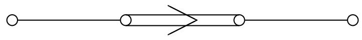
Uma maneira de contornar essa dificuldade com o grafo de Coxeter é acrescentar-lhe uma informação adicional, tornando possível a distinção entre os dois comprimentos das raízes, caso necessário. Para isso, basta orientar as arestas conectando os vértices afetados desenhando uma flexa partindo da raiz longa para a raiz curta, conforme os exemplos abaixo:

B_2 

G_2 

A esta nova figura denominamos *Diagrama de Dynkin* de Φ.

Para exemplo de como reobter a matriz de Cartan a partir de um diagrama de Dynkin, consideremos o sistema de raízes dado por:

F_4 

Enumerando as raízes simples da esquerda para a direita $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, o diagrama nos fornece imediatamente que

$$\begin{aligned} \langle \alpha_1, \alpha_2 \rangle \langle \alpha_2, \alpha_1 \rangle &= 1 \\ \langle \alpha_2, \alpha_3 \rangle \langle \alpha_3, \alpha_2 \rangle &= 2 \\ \langle \alpha_3, \alpha_4 \rangle \langle \alpha_4, \alpha_3 \rangle &= 1 \end{aligned}$$

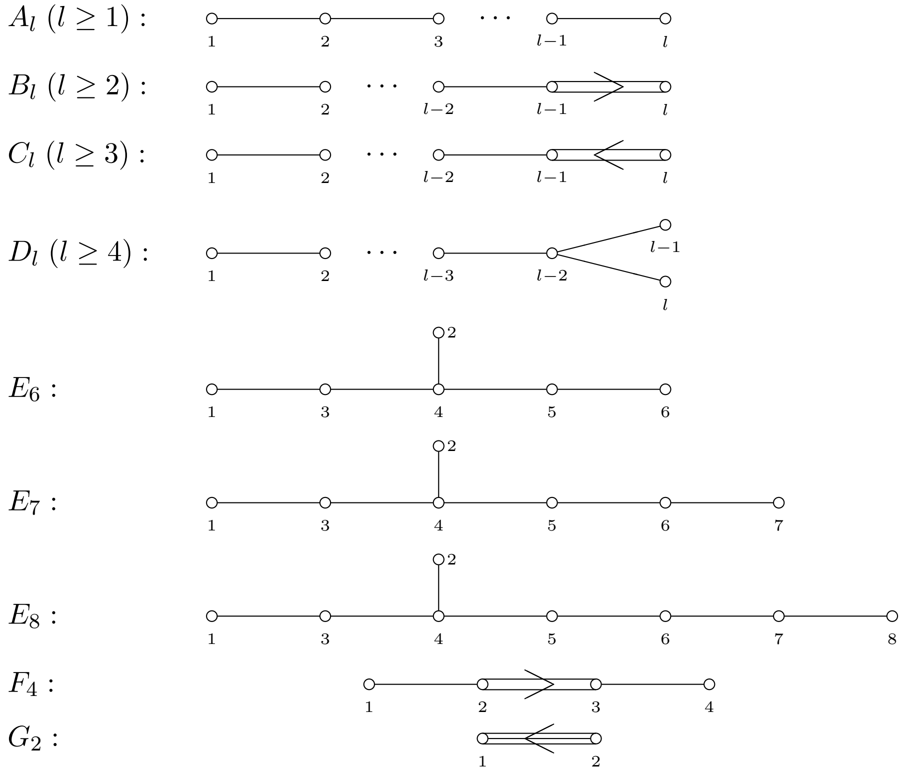
Pelo Lema 73, sabemos que $\langle \alpha_i, \alpha_j \rangle \leq 0$, para todo $i \neq j$, logo $\langle \alpha_1, \alpha_2 \rangle = \langle \alpha_2, \alpha_1 \rangle = \langle \alpha_3, \alpha_4 \rangle = \langle \alpha_4, \alpha_3 \rangle = -1$. A indicação sobre os comprimentos relativos entre as raízes α_2 e α_3 contida no diagrama nos fornece $\langle \alpha_2, \alpha_3 \rangle = -2$, e $\langle \alpha_3, \alpha_2 \rangle = -1$. Ademais, sabemos que $\langle \alpha_i, \alpha_i \rangle = 2$, e que $\langle \alpha_i, \alpha_j \rangle = 0$ se as raízes α_i e α_j não são adjacentes no diagrama. Disso resulta a matriz de

Cartan de F_4:

$$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

A esta altura, deve estar claro que um sistema de raízes Φ é irredutível se, e só se, seu grafo de Coxeter for conexo. Graças à Proposição 76, basta-nos classificar os sistemas de raízes irredutíveis, ou equivalentemente os diagramas de Dynkin conexos.

Proposição 79 *Se Φ é um sistema de raízes irredutível de posto l, então seu diagrama de Dynkin é um dos seguintes:*



Prova. A prova é extensa, e será feita em dez passos. Inicialmente, vamos classificar todos os possíveis Grafos de Coxeter, ignorando os comprimentos relativos entre as raízes. Em seguida, construímos todos os Diagramas de Dynkin que deles resultam. Desse modo, iremos considerar apenas vetores unitários (já que estamos ignorando os comprimentos das raízes). Temporariamente vamos permitir que E seja um espaço euclideano de dimensão arbitrária e vamos fixar um conjunto $U = \{e_1, \ldots, e_n\}$ de vetores unitários e linearmente independentes satisfazendo $(e_i, e_j) \leq 0$ $(i \neq j)$ e $4(e_i, e_j)^2 = 0, 1, 2,$ ou 3 $(i \neq j)$. Qualquer subconjunto de E satisfazendo essas condições será dito *admissível*. Notemos que os elementos de uma base divididos por seu respectivo comprimento formam um conjunto admissível, de modo que não perdemos a generalidade.

A partir do conjunto admissível U construímos um grafo Γ da mesma maneira que fizemos para as raízes simples, com os vértices $i \neq j$ ligados por $4(e_i, e_j)^2$ arestas. Devemos agora encontrar todos os grafos conexos associados a conjuntos admissíveis de vetores, o que será feito por etapas.

(1) *Se alguns dos e_i forem descartados, os vetores restantes continuam a formar um conjunto admissível, cujo grafo é obtido de Γ omitindo-se os vértices correspondentes e todas as arestas a eles adjacentes.*

(2) *O número de pares de vértices em Γ conectados ao menos por uma aresta é estritamente inferior a n.* Seja $v = \sum_{i=1}^{n} e_i$. Como U é um conjunto linearmente independente, certamente $v \neq 0$, de modo que

$$0 < (v, v) = \sum_{i,j=1}^{n} (e_i, e_j) = \sum_{i<j} (e_i, e_j) + \sum_{i=1}^{n} (e_i, e_i) + \sum_{i>j} (e_i, e_j) = n + 2 \sum_{i<j} (e_i, e_j).$$

Sejam i, j um par de índices distintos tais que $(e_i, e_j) \neq 0$, significando que os vértices i e j estão conectados. Então $4(e_i, e_j)^2 = 1, 2,$ ou 3, isto é, $2(e_i, e_j) = -1, -\sqrt{2}$, ou $-\sqrt{3}$. Em particular, $2(e_i, e_j) \leq -1$. Voltando à desigualdade acima, vemos que o número de tais pares não pode ser maior do que $n - 1$.

(3) Γ *não contém nenhum ciclo.* Um ciclo seria um subgrafo Γ' de Γ correspondente a um subconjunto admissível $U' \subset U$ consistindo de, digamos, $m \leq n$ elementos. Isto obviamente contraria (2) com m substituindo n.

(4) *Um vértice de Γ não pode ter mais do que três arestas adjacentes.* Seja

$$U' = \{w, v_1, \ldots, v_k\} \subset U$$

um subconjunto de vetores distintos, tais que, $v_1, \dots, v_k$ estejam conectados a w, i.é, $(w, v_i) < 0$, com respectivo grafo Γ'. Devido a (3) Γ' não pode conter ciclos, ou seja, $(v_i, v_j) = 0$ $(i \neq j)$. Como U' é um conjunto linearmente independente, pode ser verificado por um cálculo direto que o vetor

$$v_0 = \frac{1}{\sqrt{1 - \sum_{i=1}^{k} (w, v_i)^2}} (w - (w, v_1)v_1 - \cdots - (w, v_k)v_k),$$

pertencente ao subespaço de E gerado por U', é unitário, ortogonal a $\{v_1, \dots, v_k\}$ e $(w, v_0) \neq 0$. Agora, $w = \sum_{i=0}^{k} (w, v_i)v_i$, de modo que $1 = (w, w) = (w, \sum_{i=0}^{k} (w, v_i)v_i) = \sum_{i=0}^{k} (w, v_i)^2$. Isto torna obrigatório $\sum_{i=1}^{n} (w, v_i)^2 < 1$, logo $4 \sum_{i=1}^{n} (w, v_i)^2 < 4$. O lado esquerdo desta última desigualdade é exatamente o número de vértices adjacentes a w em Γ.

(5) *O único grafo conexo Γ de um conjunto admissível U contendo uma aresta tripla é o grafo de Coxeter de G_2 :* . Isto é conseqüência imediata de (4).

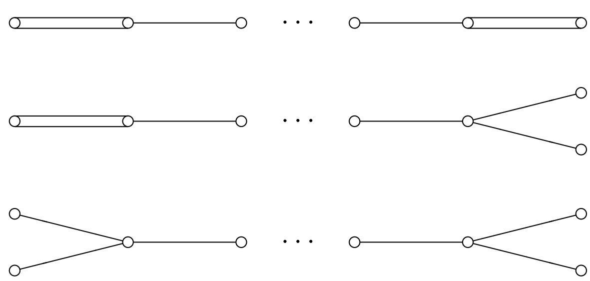
(6) *Suponhamos que $\{e_1, \dots, e_k\} \subset U$ corresponda ao subgrafo*

isto é, uma cadeia simples em Γ. Se $v = \sum_{i=1}^{k} e_i$, e $U' = (U - \{e_1, \dots, e_k\}) \cup \{v\}$, então U' é admissível. (Em outras palavras, o grafo de U' é obtido de Γ simplesmente contraindo a cadeia simples a um único vértice). Por hipótese, $2(e_i, e_{i+1}) = -1$ $(1 \leq i \leq k-1)$, logo

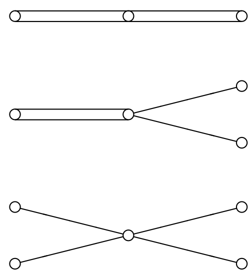
$$(v, v) = k + 2 \sum_{i<j} (e_i, e_j) = k - (k-1) = 1,$$

i.é, v é um vetor unitário. Qualquer que seja $w \in U - \{e_1, \dots, e_k\}$, este pode estar conectado a no máximo um dos vértices $e_1, \dots, e_k$, pela inexistência de ciclos (3), daí $(w, v) = 0$ ou $(w, v) = (w, v_i)$ para algum $i = 1, \dots, k$. Conseqüentemente, $4(w, v)^2 = 0$, 1, 2, ou 3.

(7) *O grafo* Γ *não contém nenhum subgrafo da forma:*

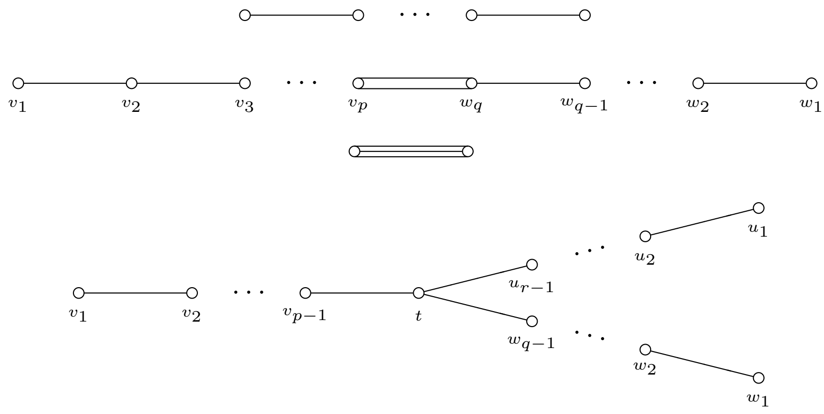


Se assim fosse, por (1) seria o grafo de um conjunto admissível. Porém, (6) permite-nos substituir a cadeia simples em cada um dos casos por um único vértice, resultando nos seguintes grafos



respectivamente, contendo um vértice com quatro arestas adjacentes, contrariando (4).

(8) *Qualquer grafo conexo* Γ *de um conjunto admissível* U *deve ser de um dos quatro tipos seguintes*:

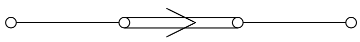


De fato apenas pode conter uma aresta tripla, por (5). Um grafo conexo Γ contendo mais do que uma aresta dupla certamente contém um subgrafo

o que não é permitido por (7), logo apenas uma aresta dupla pode ocorrer. De modo semelhante, se esse grafo contiver dois pontos de ramificação (i.é, um vértice donde partem três arestas ligadas a outros três vértices distintos), conterá um subgrafo

também proíbido por (7), e assim sendo apenas um ponto de ramificação pode ocorrer. Disto concluímos imediatamente (ainda por (7)) que ambos, uma aresta dupla e um ponto de ramificação, não podem ocorrer simultaneamente. Com isto, liquidamos os tipos 2-4. Finalmente, se o grafo conexo Γ contém apenas arestas simples e não contém pontos de ramificação, como não pode conter ciclos, deve ser uma cadeia simples, que é do tipo 1.

(9) *Os únicos grafos conexos do segundo tipo em (8) são o grafo de Coxeter* F_4*,*



e o grafo de Coxeter $B_n (= C_n)$*,*

.

Sejam $v = \displaystyle\sum_{i=1}^{p} i v_i$ e $w = \sum_{i=1}^{q} i v_i$. Por hipótese, $2(v_i, v_{i+1}) = -1 = 2(w_i, w_{i+1})$, e outros pares envolvendo esses vetores são ortogonais, logo

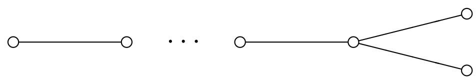
$$(v, v) = \sum_{i=1}^{p} i^2 - \sum_{i=1}^{p-1} i(i+1) = \frac{p(p+1)}{2}$$

e de modo similar, $(w,w) = \dfrac{q(q+1)}{2}$. Como $4(v_p, w_q)^2 = 2$, devemos ter também

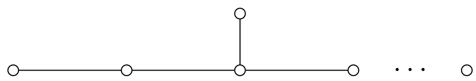
$$(v,w)^2 = p^2q^2(v_p,w_q)^2 = \frac{p^2q^2}{2}.$$

Sendo v e w linearmente independentes, a desigualdade de Cauchy-Schwarz nos permite obter $(v,w)^2 < (v,v)(w,w)$, ou seja, $p^2q^2/2 < p(p+1)q(q+1)/4$, e portanto $(p-1)(q-1) < 2$. As únicas possibilidades para os inteiros positivos p e q são $p = q = 2$, resultando em F_4, ou $p = 1$ e $q = n-1$ (ou vice-versa) resultando em B_n.

(10) *Os únicos grafos conexos do quarto tipo em (8) são o grafo de Coxeter D_n,*



e o grafo de Coxeter de E_n ($n = 6$, 7, ou 8),



.

Sejam $v = \displaystyle\sum_{i=1}^{p-1} iv_i$, $w = \sum_{i=1}^{q-1} iv_i$ e $u = \sum_{i=1}^{r-1} iu_i$. Claramente, v, w, u são mutuamente ortogonais, linearmente independentes e t não está no subespaço de E gerado por eles. Procedendo da mesma maneira que na prova de (4), obtemos $\cos^2\theta_1 + \cos^2\theta_2 + \cos^2\theta_3 < 1$, onde $\theta_1, \theta_2, \theta_3$ são os respectivos ângulos entre t e v, w, u. O mesmo cálculo realizado em (9) aplicado a $p-1$ ao invés de p nos dá $(v,v) = p(p-1)/2$, e de maneira similar, $(w,w) = q(q-1)/2$ e $(u,u) = r(r-1)/2$. Portanto,

$$\cos^2\theta_1 = \frac{(v,t)^2}{(v,v)(t,t)} = \frac{(p-1)^2(v_{p-1},t)^2}{(v,v)} = \frac{1}{4}\,\frac{2(p-1)^2}{p(p-1)} = \frac{1}{2}\left(1-\frac{1}{p}\right).$$

Analogamente, temos $\cos^2\theta_2 = \frac{1}{2}\left(1-\frac{1}{q}\right)$ e $\cos^2\theta_3 = \frac{1}{2}\left(1-\frac{1}{r}\right)$. Somando estas três igualdades, obtemos

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1. \tag{2.11}$$

Renomeando os vetores, podemos assumir que $1/p \leq 1/q \leq 1/r \leq 1/2$ (se p, q, ou r fosse igual a 1 estaríamos de volta ao tipo A_n). Em particular, temos que

$$\frac{3}{2} \geq \frac{3}{r} = \frac{1}{r} + \frac{1}{r} + \frac{1}{r} \geq \frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1,$$

donde $r = 2$. Disto resulta sucessivamente $1/p + 1/q > 1/2$, $2/q > 1/2$ e $2 \leq q < 4$. Se $q = 3$, então $1/p > 1/6$, i.é, $p < 6$, e se $q = 2$, obviamente p pode ser qualquer inteiro maior ou igual a 2. Portanto, as únicas triplas (p, q, r) possíveis são $(p, 2, 2)$, $(3, 3, 2)$, $(4, 3, 2)$, $(5, 3, 2)$, resultando em D_n, E_6, E_7, e E_8, respectivamente.

Com isto, mostramos que os grafos conexos de conjuntos admissíveis de vetores devem estar entre os tipos $A-G$. Particularmente, encontramos entre eles os Grafos de Coxeter de sistemas de raízes. Em todos os casos, exceto B_l e C_l, o grafo de Coxeter determina unicamente o diagrama de Dynkin, pois estes não requerem distinção entre comprimentos de raízes. ∎

A razão para as restrições impostas aos casos $A - D$ no enunciado do teorema é apenas evitar duplicação. Com relação à ordem escolhida para a enumeração das raízes simples nos diagramas, temos as seguintes matrizes de Cartan:

$$A_l : \left(\begin{array}{cccccccccc}
2 & -1 & 0 & & & . & . & . & & 0 \\
-1 & 2 & -1 & 0 & & . & . & . & & 0 \\
0 & -1 & 2 & -1 & 0 & . & . & . & & 0 \\
. & . & . & . & . & . & . & . & . & -1 \\
0 & 0 & 0 & 0 & & . & . & . & -1 & 2
\end{array}\right)$$

$$B_l : \left(\begin{array}{cccccccccc}
2 & -1 & 0 & & & . & . & . & & 0 \\
-1 & 2 & -1 & 0 & & . & . & . & & 0 \\
0 & -1 & 2 & -1 & 0 & . & . & . & & 0 \\
. & . & . & . & . & . & . & . & . & -2 \\
0 & 0 & 0 & 0 & & . & . & . & -1 & 2
\end{array}\right)$$

$$C_l : \left(\begin{array}{cccccccccc}
2 & -1 & 0 & & & . & . & . & & 0 \\
-1 & 2 & -1 & 0 & & . & . & . & & 0 \\
0 & -1 & 2 & -1 & 0 & . & . & . & & 0 \\
. & . & . & . & . & . & . & . & . & -1 \\
0 & 0 & 0 & 0 & & . & . & . & -2 & 2
\end{array}\right)$$

$$D_l : \left(\begin{array}{cccccccccc}
2 & -1 & 0 & & . & . & . & & & 0 \\
-1 & 2 & -1 & & . & . & . & & & 0 \\
. & . & . & . & . & . & . & . & . & . \\
0 & 0 & & . & . & -1 & 2 & -1 & 0 & 0 \\
0 & 0 & & . & . & & -1 & 2 & -1 & -1 \\
0 & 0 & & . & . & & 0 & -1 & 2 & 0 \\
0 & 0 & & . & . & & 0 & -1 & 0 & 2
\end{array}\right)$$

2.7 A álgebra universal envolvente $U\mathfrak{g}$ de uma álgebra de Lie $\mathfrak{g}$

Nesta seção, F é um corpo arbitrário. Vamos associar à cada álgebra de Lie $\mathfrak{g}$ sobre F uma álgebra associativa $U\mathfrak{g}$ com unidade $1 \in F$, que seja o mais "livre" possível, sujeita às relações de comutação de $\mathfrak{g}$. Esta é denominada a álgebra universal envolvente de $\mathfrak{g}$ e tem papel fundamental na teoria de representações das álgebras de Lie. Como se sabe, o produto tensorial de duas álgebras de Lie $\mathfrak{g}$ e $\mathfrak{g}'$ não é necessariamente uma álgebra de Lie. Contudo, o produto tensorial de suas respectivas álgebras universais envolventes $U\mathfrak{g}$ e $U\mathfrak{g}'$ é uma álgebra universal envolvente, a saber, $U(\mathfrak{g} \oplus \mathfrak{g}')$, a qual contém $\mathfrak{g}$ e $\mathfrak{g}'$ (veremos que toda álgebra de Lie está contida em sua álgebra universal envolvente). Assim, a teoria geral das representações das álgebras de Lie se reduz à teoria das representações de álgebras associativas. Com isso, não é surpresa o fato das álgebras universais envolventes desempenharem um papel essencial na Teoria dos Grupos Quânticos. Seus exemplos mais comuns, como veremos, são provenientes de deformações das

$U\mathfrak{g}$.

2.7.1 A construção de $U\mathfrak{g}$

A *álgebra universal envolvente* de $\mathfrak{g}$ é um par $(U\mathfrak{g}, i)$ consistindo de uma álgebra associativa com unidade $U\mathfrak{g}$, e de uma aplicação linear $i : \mathfrak{g} \to U\mathfrak{g}$, satisfazendo:

(i) A condição

$$i([xy]) = i(x)i(y) - i(y)i(x), \tag{2.12}$$

para todo $x, y \in \mathfrak{g}$;

(ii) A seguinte propriedade universal: para todo par (A, j) consistindo de uma álgebra associativa com unidade A, e de uma aplicação linear $j : \mathfrak{g} \to A$ satisfazendo (2.12), existe um único homomorfismo de álgebras $\varphi : U\mathfrak{g} \to A$ tornando comutativo o diagrama

$$\begin{tikzcd} & U\mathfrak{g} \arrow[dd, "\varphi"] \\ \mathfrak{g} \arrow[ur, "i"] \arrow[dr, "j"'] & \\ & A \end{tikzcd}$$

Sabemos que um objeto definido por meio de propriedade universal é único, a menos de isomorfismos. Porém, precisamos construir um exemplar concreto a fim de garantir a existência desse objeto. É o que fazemos a seguir.

Seja $T\mathfrak{g} = \bigoplus_{i=0}^{\infty} T^i\mathfrak{g}$ a álgebra tensorial (cf. Exemplo 150) de $\mathfrak{g}$, e seja J o ideal (bilateral) de $T\mathfrak{g}$ gerado por todos os elementos da forma $x \otimes y - y \otimes x - [xy]$, para $x, y \in \mathfrak{g}$. Definimos $U\mathfrak{g} = T\mathfrak{g}/J$ e seja $\pi : T\mathfrak{g} \to U\mathfrak{g}$ a projeção canônica. Observamos que J não contém os escalares $T^0\mathfrak{g} = F$, logo π leva F isomorficamente em $U\mathfrak{g}$. Surpreendentemente, π também leva $\mathfrak{g}$ isomorficamente em $U\mathfrak{g}$. Isto será provado na próxima subseção.

Definindo $i : \mathfrak{g} \to U\mathfrak{g}$ como a restrição de π a $T^1\mathfrak{g} = \mathfrak{g}$, afirmamos que o par $(U\mathfrak{g}, i)$ é uma álgebra universal envolvente de $\mathfrak{g}$. Com efeito, seja (A, j) conforme a definição. A propriedade universal de $T\mathfrak{g}$ nos fornece um homomorfismo de álgebras $\varphi' : T\mathfrak{g} \to A$ tornando comutativo o diagrama

$$\begin{tikzcd} & T\mathfrak{g} \arrow[dd, "\varphi'"] \\ \mathfrak{g} \arrow[ur, "i'"] \arrow[dr, "j"'] & \\ & A \end{tikzcd}$$

onde $i' : \mathfrak{g} \to T\mathfrak{g}$ é a inclusão natural. Devido à propriedade (2.12) satisfeita por j, temos

$$\begin{aligned} \varphi'(x \otimes y - y \otimes x - [xy]) &= \varphi'(x)\varphi'(y) - \varphi'(y)\varphi'(x) - \varphi'([xy]) \\ &= j(x)j(y) - j(y)j(x) - j([xy]) = 0, \end{aligned}$$

logo $J \subset \ker \varphi'$. Pelo Teorema 90, há um único homomorfismo de álgebras φ tornando comutativo o diagrama

$$\begin{tikzcd} T\mathfrak{g} \arrow[rr, "\varphi'"] \arrow[dr, "\pi"'] & & A \\ & T\mathfrak{g}/J \arrow[ur, "\varphi"'] & \end{tikzcd}$$

provando a afirmação.

Exemplo 80 Seja $\mathfrak{g}$ uma álgebra de Lie abeliana. Então o ideal J acima coincide com o ideal gerado por todos os elementos da forma $x \otimes y - y \otimes x$, para $x, y \in \mathfrak{g}$. Portanto, $\mathfrak{U}(\mathfrak{g})$ coincide com a álgebra simétrica $S\mathfrak{g}$, tratada no Exemplo 153.

2.7.2 O Teorema de Poincaré-Birkhoff-Witt

Vamos tornar mais evidente a estrutura da álgebra $U\mathfrak{g}$, mostrando que esta contém uma imagem isomórfica de $\mathfrak{g}$, e encontrando explicitamente uma base. Estes resultados são corolários do Teorema de Poincaré-Birkhoff-Witt (PBW).

Antes, porém, precisamos de algumas definições. Sejam $\mathfrak{T} = T\mathfrak{g}$, $\mathfrak{S} = S\mathfrak{g}$ e $\mathfrak{U} = U\mathfrak{g}$. Similarmente, escrevemos $T^m = T^m\mathfrak{g}$ e $S^m = S^m\mathfrak{g}$. Definimos uma filtração (cf. pág. 175) em $\mathfrak{T}$ por $T_m = T^0 \oplus T^1 \oplus \cdots \oplus T^m$, e seja $U_m = \pi(T_m)$, $U_{-1} = 0$. Claramente, $U_m \subset U_{m+1}$ e $U_m U_n \subset U_{m+n}$. Definindo $G^m = U_m/U_{m-1}$ (como quociente de espaços vetoriais), a multiplicação de $\mathfrak{U}$ define uma aplicação bilinear $G^m \times G^n \to G^{m+n}$, a qual se estende a uma aplicação bilinear $\mathfrak{G} \times \mathfrak{G} \to \mathfrak{G}$, onde $\mathfrak{G} = \bigoplus_{m=0}^{\infty} G^m$. Assim, esta torna-se uma álgebra associativa graduada com unidade.

Consideremos a composição $\phi_m : T^m \to U_m \to G^m = U_m/U_{m-1}$. Esta é sobrejetora, pois $\pi(T_m - T_{m-1}) = U_m - U_{m-1}$. As aplicações ϕ_m dão então origem a uma aplicação linear $\phi : \mathfrak{T} \to \mathfrak{G}$, a qual é sobrejetora e leva 1_T em $1_{\mathfrak{G}}$.

Lema 81 *$\phi : \mathfrak{T} \to \mathfrak{G}$ é um homomorfismo de álgebras e $\phi(I) = 0$, onde I é o ideal de T gerado por todos os elementos da forma $x \otimes y - y \otimes x$. Portanto há um único homomorfismo de álgebras ω tornando comutativo o diagrama*

$$\begin{tikzcd}
\mathfrak{T} \arrow[rr, "\phi"] \arrow[dr] & & \mathfrak{G} \\
& I \arrow[ur, "\omega"'] &
\end{tikzcd}$$

Prova. Seja $x \in T^m$, $y \in T^n$, tensores homogêneos. Pela definição do produto em $\mathfrak{G}$, temos $\phi(xy) = \phi(x)\phi(y)$, logo ϕ é multiplicativa. Seja $x \otimes y - y \otimes x$, com $x, y \in \mathfrak{g}$, um gerador de I. Então, $\pi(x \otimes y - y \otimes x) \in U_2$, por definição. Por outro lado, $\pi(x \otimes y - y \otimes x) = \pi([xy]) \in U_1$, logo $\pi(x \otimes y - y \otimes x) \in U_1/U_1 = 0$. Segue que $I \subset \ker \phi$. ■

O seguinte resultado é fundamental para o estudo de $U\mathfrak{g}$. Sua prova pode ser encontrada em Humphreys [Hu, §17.4].

Teorema 82 (PBW) *O homomorfismo $\omega : \mathfrak{S} \to \mathfrak{G}$ é um isomorfismo de álgebras.*

■

Corolário 83 *Seja W um subespaço de T^m. Se a aplicação canônica $T^m \to S^m$ leva W isomorficamente sobre S^m, então $\pi(W)$ é um complementar de U_{m-1} em U_m.*

Prova. Consideremos o diagrama

$$\begin{tikzcd}
T^m \arrow[r] \arrow[d] & U^m \arrow[d] \\
S^m \arrow[r] & G^m
\end{tikzcd}$$

De acordo com o Lema 81, e com as definições acima, este diagrama é comutativo. Como $\omega : \mathfrak{S} \to \mathfrak{G}$ é um isomorfismo, a composição $T^m \to S^m \to G^m$ leva W isomorficamente sobre sobre G^m. O mesmo deve acontecer com a composição $T^m \to U_m \to S^m$, completando a prova.

■

Corolário 84 *O homomorfismo canônico $i : \mathfrak{g} \to U\mathfrak{g}$ é injetor (logo, $\mathfrak{g}$ pode ser identificada com $i(\mathfrak{g})$).*

Prova. Este é um caso particular do corolário anterior, com $W = T^1 = \mathfrak{g}$. ∎

Corolário 85 (Base PBW) *Seja $(x_1, x_2, x_3 \ldots)$ uma base ordenada qualquer de $\mathfrak{g}$. Então, os elementos da forma $x_{i_1} \cdots x_{i_m} = \pi(x_{i_1} \otimes \cdots \otimes x_{i_m})$, com $i_1 \leq \cdots \leq i_m$, $m \in \mathbb{Z}^+$, formam uma base de $U\mathfrak{g}$, denominada* Base PBW*.*

Prova. Seja W o subespaço de $U\mathfrak{g}$ gerado por $x_{i_1} \otimes \cdots \otimes x_{i_m}$, $i_1 \leq \cdots \leq i_m$. Claramente W é levado isomorficamente sobre S^m, logo pelo Corolário 83 $\pi(W)$ é um complementar de U_{m-1} em U_m. ∎

Capítulo 3

Álgebras de Hopf

3.1 Álgebras Associativas com Unidade

A definição clássica de álgebra associativa com unidade baseia-se na asserção de alguns axiomas expressos em termos dos elementos da álgebra. Por uma razão que se tornará clara na seção seguinte, é útil definir uma álgebra sem recorrer explicitamente aos seus elementos, utilizando a linguagem das funções (também chamadas setas) e dos diagramas comutativos. Também, vale a pena notar o senso comum de que a informação visual expressa pelos diagramas freqüentemente nos provê de mais informação, e nos proporciona maior agilidade na síntese do conhecimento, do que a linguagem verbal.

Utilizando essa linguagem, enunciaremos e provaremos o Teorema Fundamental do Isomorfismo para álgebras. Este é um resultado elementar, que servirá de inspiração ao enunciado e prova de teoremas análogos para as coálgebras, biálgebras e álgebras de Hopf, a seguir. Não obstante, a idéia de se formar quocientes é extremamente poderosa e nos auxilia no estudo de estruturas algébricas mais sofisticadas, e constitui ferramenta essencial, juntamente com as somas, produtos diretos, e produtos tensoriais, etc, na construção de novos objetos algébricos com propriedades desejadas.

3.1.1 Definição e exemplos

Seja A uma álgebra associativa com unidade 1_A sobre um corpo F. Observamos que a operação de multplicação de A define uma aplicação linear

$$\begin{aligned} \mu_A : A \otimes_F A &\rightarrow A \\ a \otimes_F b &\mapsto a \cdot b \end{aligned}$$

denominada *aplicação multiplicação*. Aqui, o símbolo "$\otimes_F$" denota o produto tensorial usual de espaços vetoriais. Não havendo confusão, costumamos omitir o subscrito F em "$\otimes_F$".

Com esta notação, a associatividade da multiplicação se traduz na comutatividade do diagrama

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "\mu_A \otimes \mathrm{id}"] \arrow[d, "\mathrm{id} \otimes \mu_A"'] & A \otimes A \arrow[d, "\mu_A"] \\ A \otimes A \arrow[r, "\mu_A"] & A \end{tikzcd} \tag{3.1}$$

ou, equivalentemente, $\mu_A \circ (\mu_A \otimes \mathrm{id}) = \mu_A \circ (\mathrm{id} \otimes \mu_A)$, onde $\mathrm{id} : A \rightarrow A$ é a aplicação identidade $a \mapsto a$, e o símbolo "$\circ$" indica a composição de aplicações.

A unidade 1_A da álgebra permite-nos definir uma aplicação linear $\eta_A : F \rightarrow A$, denominada *aplicação unidade*, por $\eta_A(\lambda) = \lambda 1_A$. Utilizando estas definições, um cálculo direto nos mostra que os seguintes diagramas são comutativos:

$$\begin{tikzcd} A \otimes F \arrow[r, "\mathrm{id} \otimes \eta_A"] \arrow[d, "\cong"'] & A \otimes A \arrow[d, "\mu_A"] \\ A \arrow[r, "\mathrm{id}"] & A \end{tikzcd} \qquad \begin{tikzcd} F \otimes A \arrow[r, "\eta_A \otimes \mathrm{id}"] \arrow[d, "\cong"'] & A \otimes A \arrow[d, "\mu_A"] \\ A \arrow[r, "\mathrm{id}"] & A \end{tikzcd} \tag{3.2}$$

ou, equivalentemente, $\mu_A \circ (\mathrm{id} \otimes \eta_A) = \mathrm{id} = \mu_A \circ (\eta_A \otimes \mathrm{id})$. As aplicações indicadas por $\cong$ na vertical representam o isomorfismo natural entre A e $A \otimes F$, sob o qual temos as identificações $\lambda \otimes a = a \otimes \lambda = \lambda a$ (cf. pág. 159).

O subscrito A em μ_A e η_A será omitido quando puder ser obtido do contexto sem que haja confusão. É também costumeiro dizer simplesmente que μ é a multiplicação e η a unidade da álgebra A.

Mais geralmente, se A é um espaço vetorial sobre F dotado de duas aplicações lineares μ e η

tornando comutativos os diagramas (3.1) e (3.2) acima, é claro que μ define uma multiplicação associativa em A e $\eta(1)$ é uma unidade de A com respeito a essa multiplicação. De fato, denotando $\mu(a \otimes b)$ por $a \cdot b$ vemos imediatamente que a linearidade de μ equivale aos axiomas usuais da bilinearidade da multiplicação. A associatividade e a existência da unidade 1_A vêm respectivamente de

$$(a \cdot b) \cdot c = (\mu \circ (\mu \otimes \mathrm{id}))(a \otimes b \otimes c) = (\mu \circ (\mathrm{id} \otimes \mu))(a \otimes b \otimes c) = a \cdot (b \cdot c)$$

e

$$a \cdot \eta(1) = (\mu \circ (\mathrm{id} \otimes \eta))(a \otimes 1) = \mathrm{id}(a \otimes 1) = a \otimes 1 \equiv a,$$

para todo $a, b, c \in A$. Com isto podemos formular a seguinte definição.

Definição 86 (Álgebra associativa com unidade) *Uma álgebra associativa com unidade é uma tripla (A, μ, η) consistindo de um espaço vetorial A sobre um corpo F e de duas aplicações lineares $\mu : A \otimes A \to A$ e $\eta : F \to A$ tornando comutativos os diagramas (3.1) e (3.2).*

As aplicações μ e η são chamadas *aplicações de estrutura.* Daqui por diante, salvo menç ão em contrário, diremos simplesmente álgebra quando desejarmos nos referir a uma álgebra associativa com unidade.

Um *homomorfismo de álgebras* entre as álgebras A e B é uma aplicação linear $\varphi : A \to B$ tornando comutativos os diagramas

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\varphi \otimes \varphi} & B \otimes B \\ \downarrow{\scriptstyle \mu_A} & & \downarrow{\scriptstyle \mu_B} \\ A & \xrightarrow{\varphi} & B \end{array} \tag{3.3}$$

$$\begin{array}{ccc} F & \xrightarrow{\mathrm{id}} & F \\ \downarrow{\scriptstyle \eta_A} & & \downarrow{\scriptstyle \eta_B} \\ A & \xrightarrow{\varphi} & B \end{array} \tag{3.4}$$

ou, equivalentemente, $\varphi \circ \mu_A = \mu_B \circ (\varphi \otimes \varphi)$ e $\varphi \circ \eta_A = \eta_B$. Isto quer dizer simplesmente que $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, para todo $a, b \in A$ e $\varphi(1_A) = 1_B$.

Se A e B são espaços vetoriais e $A \otimes B$ é o produto tensorial de A e B sobre F, definimos a *aplicação transposição (ou aplicação twist)*

$$\begin{aligned} \tau : A \otimes B &\rightarrow B \otimes A \\ a \otimes b &\mapsto b \otimes a \end{aligned}$$

para todo $a \in A$, $b \in B$, que é um isomorfismo de espaços vetoriais (cf. pág. 160).

Uma álgebra A é *comutativa* se sua multiplicação satisfaz $\mu \circ \tau = \mu$, isto é $a \cdot b = b \cdot a$, para todo $a, b \in A$.

Se A e B são álgebras, definimos a aplicação

$$\mu_{A\otimes B} : (A \otimes B) \otimes (A \otimes B) \rightarrow A \otimes B$$

por $\mu_{A\otimes B} = (\mu_A \otimes \mu_B) \circ (\mathrm{id} \otimes \tau \otimes \mathrm{id})$, e também a aplicação

$$\eta_{A\otimes B} : F \rightarrow A \otimes B$$

por $\eta_{A\otimes B} = \eta_A \otimes \eta_B$. É fácil verificar que $\mu_{A\otimes B}$ e $\eta_{A\otimes B}$ são lineares (como composição de aplicações lineares) e satisfazem aos diagramas comutativos (3.1) e (3.2) acima, substituindo A por $A \otimes B$. Conseqüentemente $(A \otimes B, \mu_{A\otimes B}, \eta_{A\otimes B})$ é uma álgebra associativa com unidade $1_A \otimes 1_B$, chamada *produto tensorial* das álgebras A e B.

Exemplo 87 Um corpo F é uma álgebra associativa com unidade se definirmos $\mu(a \otimes b) = ab$ e $\eta(\lambda) = \lambda$. $\square$

Exemplo 88 (Álgebra de Grupo) Sejam G um grupo e F um corpo arbitrários. Consideremos as somas formais $\sum_{g\in G} a_g g$, onde $a_g \in F$ é zero quase sempre, i.é, as somas são finitas. Denotemos por FG o conjunto de todas as somas correspondentes a diferentes escolhas dos coeficientes. Podemos definir em FG uma adição e uma multiplicação por escalar, a saber

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

e

$$\lambda \cdot (\sum_{g\in G} a_g g) = \sum_{g\in G} \lambda a_g g$$

fazendo de FG um espaço vetorial sobre F. Em outras palavras, FG é o F-módulo livre gerado pelo conjunto G.

A operação de G (denotada por justaposição) induz uma multiplicação $\mu : FG \otimes FG \to FG$ definida por

$$\mu((\sum_{g\in G} a_g g) \otimes (\sum_{h\in G} b_h h)) = \sum_{g,h\in G} a_g b_h gh = \sum_{g,h\in G} a_g b_{hg^{-1}} h.$$

A associatividade desta multiplicação é imediatamente verificada a partir da associatividade da operação em G. Finalmente, podemos definir uma aplicação unidade $\eta : F \to FG$ por $\eta(\lambda) = \lambda e$, onde e é o elemento neutro da operação de G. Desse modo, (FG, μ, η) é uma álgebra associativa com unidade sobre F. $\square$

Exemplo 89 O espaço vetorial $\mathbb{R}^n$ com aplicação multiplicação $\mu : \mathbb{R}^n \otimes \mathbb{R}^n \to \mathbb{R}^n$definida por

$$\mu((x_1, \ldots, x_n) \otimes (y_1, \ldots, y_n)) = (x_1 y_1, \ldots, x_n y_n)$$

e com aplicação unidade $\eta : F \to \mathbb{R}^n$ verificando

$$\eta(\lambda) = (\lambda, \ldots, \lambda)$$

é uma álgebra associativa com unidade sobre $\mathbb{R}$. $\square$

Dada uma álgebra (A, μ, η), um subespaço vetorial $B \subset A$ é uma *subálgebra* se satisfizer às condições $\mu(B \otimes B) \subset B$ e $\operatorname{Im} \eta \subset B$. Neste caso B é uma álgebra por si mesma com as aplicações de estrutura $\mu|_{B\otimes B}$ e η.

Um subespaço J de A é dito *ideal à esquerda* (*direita*) se satisfizer $\mu(A\otimes J) \subset J$ ($\mu(J\otimes A) \subset J$), e é dito *ideal bilateral* se satisfizer $\mu(A \otimes J + J \otimes A) \subset J$. Claramente J é ideal bilateral se, e só se, for ideal à esquerda e à direita simultaneamente. Quando J for um ideal bilateral, diremos simplesmente que J é um ideal.

3.1.2 Teorema Fundamental do Isomorfismo

Vamos agora enunciar e provar esse importante resultado, utilizando apenas a linguagem dos diagramas e algum conhecimento sobre os espaços vetoriais.

Teorema 90 (TFI) *Seja A uma álgebra, J um ideal e $\pi : A \to A/J$ a projeção natural de A sobre o quociente de espaços vetoriais A/J. Então:*

(a) A/J tem uma única estrutura de álgebra fazendo com que π seja um homomorfismo de álgebras.

(b) Se $f : A \to A'$ é um homomorfismo de álgebras, então $\ker f$ é um ideal de A.

(c) Se $J \subset \ker f$ então existe um único homomorfismo de álgebras $\bar{f}$ tornando comutativo o diagrama

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & J \\ & A/J \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Prova. (a) Consideremos φ a composição

$$A \otimes A \xrightarrow{\mu} A \xrightarrow{\pi} A/J.$$

Observando que $\varphi(A \otimes J + J \otimes A) = J$, isto é, $A \otimes J + J \otimes A \subset \ker \varphi$, e que

$$\frac{A \otimes A}{A \otimes J + J \otimes A} \cong \frac{A}{J} \otimes \frac{A}{J}$$

como espaços vetoriais, vemos que existe uma única aplicação linear $\bar{\mu}$ tornando comutativo o diagrama

$$\begin{tikzcd} A \otimes A \arrow[r, "\mu"] \arrow[d, "\pi\otimes\pi"'] & A \arrow[d, "\pi"] \\ \frac{A}{J} \otimes \frac{A}{J} \arrow[r, "\bar{\mu}"] & \frac{A}{J} \end{tikzcd} \tag{3.5}$$

Afirmamos que $\bar{\mu}$ é associativa. Com efeito, denotando $\pi(a)$ por $\bar{a}$, e $\mu(a \otimes b)$ por ab temos,

$$(\bar{\mu} \circ (\bar{\mu} \otimes \mathrm{id}))(\bar{a} \otimes \bar{b} \otimes \bar{c}) \quad = \quad \bar{\mu}(\overline{ab} \otimes \bar{c}) = \overline{abc} =$$

$$= \quad \bar{\mu}(\bar{a} \otimes \overline{bc}) = (\bar{\mu} \circ (\mathrm{id} \otimes \bar{\mu}))(\bar{a} \otimes \bar{b} \otimes \bar{c}),$$

para todo $a, b, c \in A$. Como π é sobrejetora, segue que $\bar{\mu} \circ (\bar{\mu} \otimes \mathrm{id}) = \bar{\mu} \circ (\mathrm{id} \otimes \bar{\mu})$, provando a afirmação.

Definindo $\bar{\eta}$ pela composição $F \xrightarrow{\eta} A \xrightarrow{\pi} A/J$, por um cálculo semelhante ao realizado acima, concluímos que $\bar{\mu} \circ (\mathrm{id} \otimes \bar{\eta}) = \mathrm{id} = \bar{\mu} \circ (\bar{\eta} \otimes \mathrm{id})$, isto é, $\bar{\eta}$ é uma unidade. Conseqüentemente, $(A/J, \bar{\mu}, \bar{\eta})$ é uma álgebra associativa com unidade. Ademais, (3.5) juntamente com a definição de $\bar{\eta}$ definem π como um homomorfismo de álgebras, mostrando (a).

(b) Uma vez que f é homomorfismo de álgebras, torna comutativo o diagrama

$$\begin{tikzcd}
A \otimes A \arrow[r, "\varphi \otimes \varphi"] \arrow[d, "\mu"'] & A' \otimes A' \arrow[d, "\mu'"] \\
A \arrow[r, "\varphi"] & A'
\end{tikzcd}$$

logo,

$$0 = (\mu' \circ f \otimes f)(A \otimes \ker f + \ker f \otimes A) = f(\mu(A \otimes \ker f + \ker f \otimes A)),$$

i.é, $\mu(A \otimes \ker f + \ker f \otimes A) \subset \ker f$, resultando (b).

(c) Como $J \subset \ker f$, existe uma única aplicação linear $\bar{f}$ tornando comutativo o diagrama

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & J \\
& A/J \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

Aplicando $\bar{\eta}$ a este diagrama, temos

$$\bar{f} \circ \bar{\eta} = \bar{f} \circ \pi \circ \eta = f \circ \eta = \eta',$$

pois f é homomorfismo de álgebras. De maneira semelhante, com a notação introduzida no item (a), verificamos que

$$\begin{aligned}
(\bar{f} \circ \mu)(\bar{a} \otimes \bar{b}) &= (\bar{f} \circ \pi)(ab) \\
&= f(ab) = (\mu' \circ (f \otimes f))(a \otimes b)
\end{aligned}$$

$$= (\mu' \circ (\bar{f} \otimes \bar{f}))(\bar{a} \otimes \bar{b}).$$

Novamente, como π é sobrejetora, resulta $\bar{f} \circ \mu = \mu' \circ (\bar{f} \otimes \bar{f})$, i.é, $\bar{f}$ é um homomorfismo de álgebras.

As aplicações $\bar{\mu}$ e $\bar{\eta}$ são as únicas aplicações lineares satisfazendo as condições do enunciado, logo, também devem ser únicas como aplicações de estrutura. ∎

3.2 Coálgebras

O conceito de álgebra é um dos mais familiares da Matemática. Intuitivamente, estas correspondem a diferentes maneiras de se multiplicar ou "agregar" números e outros objetos algébricos. Um conceito análogo a este é o de coálgebra que corresponde às diferentes maneiras de se "desagregar" ou "dividir" objetos. Esta repartição denomina-se comultiplicação. Assim como a unidade é o elemento neutro da multiplicação, a counidade é o elemento neutro da comultiplicação.

Nesta seção, definimos o conceito de coálgebra, apresentamos alguns exemplos elementares e estudamos superficialmente alguns dos principais resultados sobre suas propriedades. Como ficará claro, a teoria das coálgebras é, em certo sentido, análoga à teoria das álgebras, porém, invertendo-se todas as setas dos diagramas correspondentes. É por essa razão que na seção anterior reformulamos o conceito de álgebra na linguagem dos diagramas comutativos. Convém ter sempre em mente os diagramas (3.1) e (3.2) acima.

3.2.1 Definição e exemplos

Definição 91 (Coálgebra) *Dado um corpo F, uma* coálgebra *sobre F é uma tripla (C, Δ, ε) consistindo de um espaço vetorial C sobre F, de uma aplicação linear $\Delta : C \to C \otimes C$, chamada* comultiplicação*, e de uma aplicação linear $\varepsilon : C \to F$, chamada* counidade*, tornando comutativos os diagramas*

$$\begin{tikzcd} C \otimes C \otimes C & C \otimes C \arrow[l, "\Delta \otimes \mathrm{id}"'] \\ C \otimes C \arrow[u, "\mathrm{id} \otimes \Delta"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"'] \end{tikzcd} \tag{3.6}$$

$$
\begin{tikzcd}
C \otimes F & C \otimes C \arrow[l, "\mathrm{id} \otimes \varepsilon"'] \\
C \arrow[u, "\cong"] & C \arrow[l, "\mathrm{id}"] \arrow[u, "\Delta"']
\end{tikzcd}
\qquad
\begin{tikzcd}
F \otimes C & C \otimes C \arrow[l, "\varepsilon \otimes \mathrm{id}"'] \\
C \arrow[u, "\cong"] & C \arrow[l, "\mathrm{id}"] \arrow[u, "\Delta"']
\end{tikzcd}
\tag{3.7}
$$

Equivalentemente, temos as relações

$$(\Delta \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \Delta) \circ \Delta, \tag{3.8}$$

chamada *coassociatividade*, e

$$(\mathrm{id} \otimes \varepsilon) \circ \Delta = \mathrm{id} = (\varepsilon \otimes \mathrm{id}) \circ \Delta, \tag{3.9}$$

respectivamente.

Um *homomorfismo de coálgebras* é uma aplicação linear $\varphi : C \to D$ de uma coálgebra C em uma coálgebra D tornando comutativos os diagramas

$$
\begin{tikzcd}
D \otimes D & C \otimes C \arrow[l, "\varphi \otimes \varphi"'] \\
D \arrow[u, "\Delta_D"] & C \arrow[l, "\varphi"] \arrow[u, "\Delta_C"']
\end{tikzcd}
\tag{3.10}
$$

$$
\begin{tikzcd}
F & F \arrow[l, "\mathrm{id}"'] \\
D \arrow[u, "\varepsilon_D"] & C \arrow[l, "\varphi"] \arrow[u, "\varepsilon_C"']
\end{tikzcd}
\tag{3.11}
$$

Equivalentemente, temos respectivamente as condições $(\varphi \otimes \varphi) \circ \Delta_C = \Delta_D \circ \varphi$ e $\varepsilon_D \circ \varphi = \varepsilon_C$.

Exemplo 92 (Coálgebra de Grupo) Seja G um grupo e FG o módulo livre gerado por G sobre F. Definimos duas aplicações lineares

$$\Delta : FG \to FG \otimes FG, \qquad \varepsilon : FG \to F$$

por $\Delta(g) = g \otimes g$ e $\varepsilon(g) = 1$, para todo $g \in G$ (estendidas a todo FG por linearidade). Então, verifica-se que

$$(\Delta \otimes \mathrm{id}) \circ \Delta(g) = g \otimes g \otimes g = (\mathrm{id} \otimes \Delta) \circ \Delta(g)$$

e

$$(\varepsilon \otimes \mathrm{id}) \circ \Delta(g) = g = (\mathrm{id} \otimes \varepsilon) \circ \Delta(g),$$

donde Δ é uma comultiplicação coassociativa e ε é uma counidade em FG, portanto, $(FG, \Delta, \varepsilon)$ é uma coálgebra. $\square$

Exemplo 93 Seja $(S, \preceq)$ um conjunto parcialmente ordenado e localmente finito, i.é, se $x \preceq y$, então há apenas um número finito de elementos $z \in S$ tais que $x \preceq z \preceq y$. Seja T o conjunto de pares ordenados $\{(x, y) \in S \times S : x \preceq y\}$. Consideremos V o módulo livre gerado por T sobre F, onde definimos $\Delta : V \to V \otimes V$ e $\varepsilon : V \to F$ respectivamente por

$$\Delta(x, y) = \sum_{x \preceq z \preceq y} (x, z) \otimes (z, y),$$

$$\varepsilon(x, y) = \begin{cases} 0 & se\ x \neq y \\ 1 & se\ x = y \end{cases}$$

então (V, Δ, ε) é uma coálgebra. $\square$

Há uma notação muito conveniente introduzida por Sweedler [Sw] para expressar as relações dadas pelos diagramas (3.6) e (3.7) acima em termos de elementos de C. Para ver isto, seja c um elemento qualquer de C. Podemos escrever o elemento $\Delta(c) \in C \otimes C$, como

$$\Delta(c) = \sum_{i=1}^{n} c_{i1} \otimes c_{i2} \tag{3.12}$$

para algum inteiro positivo n, e elementos c_{i1}, c_{i2} de C. Aqui, n não tem nenhum significado especial, mas indica apenas que a somatória é finita. Além disso, não exigimos que essa somatória se expresse unicamente em termos dos elementos de C. É útil denotar (3.12) de maneira sintética escrevendo simplesmente

$$\Delta(c) = c_{(1)} \otimes c_{(2)}. \tag{3.13}$$

Notemos que $c_{(1)}$ e $c_{(2)}$ *não* são propriamente elementos de C, e não têm nenhum significado isoladamente, mas seu aparecimento em conjunto tem o significado da somatória (3.12). Nesta notação, as propriedades de coassociatividade (3.8) e counidade (3.9) acima se escrevem como

$$c_{(1)(1)} \otimes c_{(1)(2)} \otimes c_{(2)} = c_{(1)} \otimes c_{(2)(1)} \otimes c_{(2)(2)}$$

e

$$\varepsilon(c_{(1)})c_{(2)} = c = c_{(1)}\varepsilon(c_{(2)}),$$

repectivamente, para todo $c \in C$.

Se $\tau : C \otimes C \to C \otimes C$ é a aplicação transposição tal que $\tau(a \otimes b) = b \otimes a$, consideremos a aplicação linear $\Delta' = \tau \circ \Delta$. Uma coálgebra C é *cocomutativa* quando sua comultiplicação satisfaz $\Delta = \Delta'$, isto é, $c_{(1)} \otimes c_{(2)} = c_{(2)} \otimes c_{(1)}$, para todo $c \in C$.

Se f, g são aplicações lineares de uma coálgebra C em uma coálgebra D então,

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

o que nos motiva a definir a notação

$$(f \otimes g) \circ \Delta(c) = f(c_{(1)}) \otimes g(c_{(2)}).$$

Se f é um homomorfismo de coálgebras, temos ainda,

$$f(c_{(1)}) \otimes f(c_{(2)}) = (f \otimes f) \circ \Delta(c) = \Delta \circ f(c) = f(c)_{(1)} \otimes f(c)_{(2)}.$$

Em particular, a aplicação identidade $\mathrm{id} : C \to C$ e a comultiplicação são aplicações lineares, donde está bem-definida uma aplicação linear $\Delta^2 : C \to C \otimes C \otimes C$ dada por

$$\Delta^2(c) \quad = \quad (\mathrm{id} \otimes \Delta) \circ \Delta(c) = c_{(1)} \otimes c_{(2)(1)} \otimes c_{(2)(2)} = c_{(1)(1)} \otimes c_{(1)(2)} \otimes c_{(2)} \tag{3.14}$$

$$= \quad c_{(1)} \otimes c_{(2)} \otimes c_{(3)}.$$

A coassociatividade continua válida em geral, o que nos permite definir indutivamente

$$\Delta^n(c) = (\underbrace{\mathrm{id} \otimes \cdots \otimes \mathrm{id}}_{n-1 \text{ vezes}} \otimes \Delta) \circ \Delta^{n-1}(c) = c_{(1)} \otimes \cdots \otimes c_{(n)}.$$

A counidade é também uma aplicação linear de C sobre F, daí

$$\begin{aligned} c &= (\varepsilon \otimes \mathrm{id}) \circ \Delta(c) = \varepsilon(c_{(1)})c_{(2)} \\ &= (\mathrm{id} \otimes \varepsilon) \circ \Delta(c) = c_{(1)}\varepsilon(c_{(2)}), \end{aligned}$$

onde identificamos $F \otimes C$ e C através do isomorfismo natural.

Temos ainda algumas relações interessantes envolvendo ε e Δ, que são resumidas na seguinte proposição.

Proposição 94 *Seja c um elemento de C. Então*

1. $\Delta(c) = \Delta(c_{(1)})\varepsilon(c_{(2)}) = \varepsilon(c_{(1)})\Delta(c_{(2)})$,
2. $\Delta(c) = c_{(1)} \otimes \varepsilon(c_{(2)})c_{(3)} = c_{(1)} \otimes \varepsilon(c_{(3)})c_{(2)}$,
3. $c = \varepsilon(c_{(1)})\varepsilon(c_{(3)})c_{(2)}$.

Prova. É imediata a partir das propriedades das aplicações lineares Δ e ε. Para ilustrar, vamos mostrar a primeira delas. Temos

$$\begin{aligned} \Delta(c_{(1)})\varepsilon(c_{(2)}) &= (\Delta \otimes \varepsilon) \circ \Delta(c) \\ &= (\mathrm{id} \otimes \mathrm{id} \otimes \varepsilon) \circ (\Delta \otimes \mathrm{id}) \circ \Delta(c) \\ &= (\mathrm{id} \otimes \mathrm{id} \otimes \varepsilon) \circ (\mathrm{id} \otimes \Delta) \circ \Delta(c) \\ &= (\mathrm{id} \otimes ((\mathrm{id} \otimes \varepsilon) \circ \Delta)) \circ \Delta(c) \\ &= (\mathrm{id} \otimes \mathrm{id}) \circ \Delta(c) = \Delta(c). \end{aligned}$$

Alternativamente, poderíamos ter utilizado a notação de Sweedler juntamente com a relação

(3.14) do seguinte modo:

$$\begin{aligned}
\Delta(c_{(1)})\varepsilon(c_{(2)}) &= c_{(1)(1)} \otimes c_{(1)(2)} \otimes \varepsilon(c_{(2)}) \\
&= c_{(1)} \otimes c_{(2)(1)} \otimes \varepsilon(c_{(2)(2)}) \\
&= c_{(1)} \otimes c_{(2)} = \Delta(c)
\end{aligned}$$

■

Como conseqüência desta proposição, temos

$$c_{(1)} \otimes \cdots \otimes \varepsilon(c_{(i)}) \otimes \cdots \otimes c_{(n+1)} = c_{(1)} \otimes c_{(2)} \otimes \cdots \otimes c_{(n)}.$$

Sejam C e D duas coálgebras sobre F, e consideremos $C \otimes D$ o produto tensorial de C e D como módulos sobre F. Definimos as aplicações lineares

$$\Delta_{C\otimes D} : C \otimes D \to (C \otimes D) \otimes (C \otimes D)$$

por $\Delta_{C\otimes D} = (\mathrm{id} \otimes \tau \otimes \mathrm{id}) \circ (\Delta_C \otimes \Delta_D)$, e

$$\varepsilon_{C\otimes D} : C \otimes D \to F$$

por $\varepsilon_{C\otimes D} = \varepsilon_C \varepsilon_D$. Um cálculo direto permite-nos verificar que $\Delta_{C\otimes D}$ é uma comultiplicação coassociativa em $C \otimes D$, e $\varepsilon_{C\otimes D}$ é uma counidade. Conseqüentemente $(C \otimes D, \Delta_{C\otimes D}, \varepsilon_{C\otimes D})$ é uma coálgebra. Com efeito,

$$\begin{aligned}
\Delta_{C\otimes D}(a \otimes b) &= (\mathrm{id} \otimes \tau \otimes \mathrm{id})(a_{(1)} \otimes a_{(2)} \otimes b_{(1)} \otimes b_{(2)}) \\
&= a_{(1)} \otimes b_{(1)} \otimes a_{(2)} \otimes b_{(2)} = (a \otimes b)_{(1)} \otimes (a \otimes b)_{(2)}.
\end{aligned}$$

Daqui por diante, omitiremos o subscrito $C \otimes D$ de tais aplicações.

3.2.2 Dualidade entre álgebras e coálgebras

Dado um espaço vetorial V sobre o corpo F, é bem conhecida a sua relação com o espaço vetorial dual V^*. Nesta subseção, veremos que quando V é uma álgebra ou uma coálgebra, seu dual V^* admite uma única estrutura de coálgebra ou de álgebra respectivamente, ao menos quando V tem dimensão finita. Neste caso, o *emparelhamento* entre V^* e V é definido como uma forma bilinear simétrica e não degenerada $\langle\ ,\ \rangle : V^* \times V \to F$ dada por $\langle f, v\rangle = f(v)$, para toda $f \in V^*$ e todo $v \in V$. Claramente, a não-degenerescência segue do isomorfismo natural entre V^* e V.

Se V e W são espaços vetoriais sobre F e V^* e W^* são seus respectivos duais algébricos, recordamos que a aplicação linear

$$\begin{aligned} \rho : V^* \otimes W^* &\to (V \otimes W)^* \\ \langle \rho(f \otimes g), v \otimes w\rangle &= \langle f, v\rangle \langle g, w\rangle \end{aligned}$$

é injetora, mas em geral não é sobrejetora. Não obstante, a imagem de $V^* \otimes W^*$ por ρ é densa em $(V \otimes W)^*$ e, por conseguinte, quando V e W têm dimensão finita, ρ é sobrejetora. Nesse caso, temos um isomorfismo natural entre os espaços vetoriais $V^* \otimes W^*$ e $(V \otimes W)^*$. Se V e W forem ambos álgebras ou coálgebras, essa identificação natural se estende unicamente a um isomorfismo natural de álgebras ou de coálgebras respectivamente.

Seja (C, Δ, ε) uma coálgebra sobre F. Então as aplicações lineares Δ e ε induzem as aplicações lineares duais $\Delta^* : (C \otimes C)^* \to C^*$ e $\varepsilon^* : F^* \to C^*$. Seja $\mu : C^* \otimes C^* \to C^*$ a composição

$$C^* \otimes C^* \xrightarrow{\rho} (C \otimes C)^* \xrightarrow{\Delta^*} C^*$$

e $\eta : F \to C^*$ a composição

$$F \xrightarrow{\cong} F^* \xrightarrow{\varepsilon^*} C^*.$$

Regredindo momentaneamente à notação extensa, suponhamos que $\Delta(c) = \sum_{i=1}^{n} c_{i1} \otimes c_{i2}$ com $c_{i1}, c_{i2} \in C$. Então, para todo $f, g \in C^*$ e todo $c \in C$, temos

$$\begin{aligned} \langle \mu(f \otimes g), c\rangle &= \langle (\Delta^* \circ \rho)(f \otimes g), c\rangle \\ &= \langle \rho(f \otimes g), \Delta(c)\rangle \end{aligned}$$

$$
\begin{aligned}
&= \left\langle \rho(f \otimes g), \sum_{i=1}^{n} c_{i1} \otimes c_{i2} \right\rangle \\
&= \sum_{i=1}^{n} \langle \rho(f \otimes g), c_{i1} \otimes c_{i2} \rangle \\
&= \sum_{i=1}^{n} \langle f, c_{i1} \rangle \langle g, c_{i2} \rangle .
\end{aligned}
$$

Escrevendo $\mu(f \otimes g) = fg$ e voltando à notação de Sweedler, vem que

$$
\begin{aligned}
\langle fg, c \rangle &= \langle f \otimes g, \Delta(c) \rangle = \left\langle f \otimes g, c_{(1)} \otimes c_{(2)} \right\rangle \\
&= \left\langle f, c_{(1)} \right\rangle \left\langle g, c_{(2)} \right\rangle .
\end{aligned} \tag{3.15}
$$

Mostremos que μ define uma multiplicação associativa com unidade em C^*. De fato, a aplicação sucessiva de (3.15) resulta em

$$
\begin{aligned}
\langle (fg)h, c \rangle &= \left\langle fg, c_{(1)} \right\rangle \left\langle h, c_{(2)} \right\rangle \\
&= \left\langle f, c_{(1)(1)} \right\rangle \left\langle g, c_{(1)(2)} \right\rangle \left\langle h, c_{(2)} \right\rangle \\
&= \left\langle f, c_{(1)} \right\rangle \left\langle g, c_{(2)(1)} \right\rangle \left\langle h, c_{(2)(2)} \right\rangle \\
&= \left\langle f, c_{(1)} \right\rangle \left\langle gh, c_{(2)} \right\rangle \\
&= \langle f(gh), c \rangle ,
\end{aligned}
$$

para todo $f, g, h \in C^*$ e $c \in C$. Além disso, definindo $1_{C^*} = \eta(1)$, temos,

$$
\begin{aligned}
\langle f \cdot 1_{C^*}, c \rangle &= \left\langle f, c_{(1)} \right\rangle \left\langle \varepsilon, c_{(2)} \right\rangle \\
&= \left\langle f, c_{(1)} \varepsilon(c_{(2)}) \right\rangle \\
&= \langle f, c \rangle .
\end{aligned}
$$

Analogamente, $\langle 1_{C^*} \cdot f, c \rangle = \langle f, c \rangle$, donde 1_{C^*} é unidade de C^* em relação a μ. Portanto, (C^*, μ, η) é uma álgebra associativa com unidade. Como as aplicações μ e η estão unicamente determinadas, segue que esta é a única estrutura de álgebra admissível em C^*.

A esta altura parece natural indagar se o espaço vetorial dual A^* de uma álgebra associativa com unidade (A, μ, η) admite uma única estrutura de coálgebra. Como a aplicação ρ não é sobrejetora em geral, vemos que isso nem sempre é verdade. Porém, quando A tem dimensão finita, podemos dar uma resposta afirmativa, como segue.

Definimos as aplicações lineares $\Delta : A^* \to A^* \otimes A^*$ e $\varepsilon : A^* \to F$ respectivamente pelas composições

$$A^* \xrightarrow{\mu^*} (A \otimes A)^* \xrightarrow{\rho^{-1}} A^* \otimes A^*$$

e

$$A^* \xrightarrow{\eta^*} F^* \xrightarrow{\xi} F.$$

onde ξ é o isomorfismo natural definido por $\xi(f) = \langle f, 1 \rangle$. Para operar expressões envolvendo Δ, identificamos $(A \otimes A)^*$ com $A^* \otimes A^*$ (via ρ) de modo que omitimos ρ^{-1}. Assim, para $f \in A^*$ e $a, b \in A$ arbitrários, podemos escrever

$$\begin{aligned} \langle \Delta(f), a \otimes b \rangle &= \langle \mu^*(f), a \otimes b \rangle \\ &= \langle f, \mu(a \otimes b) \rangle \\ &= \langle f, ab \rangle . \end{aligned}$$

Para a aplicação linear ε, como $1_A = \eta(1_F)$, obtemos

$$\varepsilon(f) = (\xi \circ \eta^*)(f) = \xi(f \circ \eta) = \langle f, \eta(1_F) \rangle = \langle f, 1_A \rangle .$$

Com esta notação, podemos escrever

$$\begin{aligned} \langle (\Delta \otimes \mathrm{id}) \circ \Delta(f), a \otimes b \otimes c \rangle &= \langle (\mu^* \otimes \mathrm{id})(\Delta(f)), a \otimes b \otimes c \rangle \\ &= \langle \Delta(f), ab \otimes c \rangle \\ &= \langle f, abc \rangle . \end{aligned}$$

Analogamente, $\langle (\mathrm{id} \otimes \Delta) \circ \Delta(f), a \otimes b \otimes c \rangle = \langle f, abc \rangle$, e portanto Δ é coassociativa.

Usando a identificação natural $a \mapsto 1 \otimes a$ entre A e $F \otimes A$, escrevemos

$$\langle (\varepsilon \otimes \mathrm{id}) \circ \Delta(f), a \rangle = \langle \Delta(f), (\eta \otimes \mathrm{id})(1 \otimes a) \rangle$$

$$
\begin{aligned}
&= \langle \Delta(f), 1_A \otimes a\rangle \\
&= \langle f, a\rangle \,.
\end{aligned}
$$

Do mesmo modo, $\langle (\mathrm{id} \otimes \varepsilon) \circ \Delta(f), a\rangle = \langle f, a\rangle$, donde concluímos que ε é uma counidade. Mostramos, assim, que $(A^*, \Delta, \varepsilon)$ define uma coálgebra sobre F.

Temos interessantes relações entre homomorfismos de coálgebras e homomorfismos de álgebras dadas pelas seguintes proposições.

Proposição 95 *Se C e D são coálgebras arbitrárias sobre F e $\varphi : C \to D$ é um homorfismo de coálgebras, então a aplicação linear induzida $\varphi^* : D^* \to C^*$ é um homorfismo de álgebras.*

Prova. Para todo $f, g \in D^*$ e todo $c \in C$, temos

$$
\begin{aligned}
\langle \varphi^*(fg), c\rangle &= \langle fg, \varphi(c)\rangle = \langle f \otimes g, \varphi(\Delta(c))\rangle \\
&= \left\langle f, \varphi(c)_{(1)}\right\rangle \left\langle g, \varphi(c)_{(2)}\right\rangle \\
&= \left\langle f, \varphi(c_{(1)})\right\rangle \left\langle g, \varphi(c_{(2)})\right\rangle \\
&= \left\langle \varphi^*(f), c_{(1)}\right\rangle \left\langle \varphi^*(g), c_{(2)}\right\rangle \\
&= \langle \varphi^*(f)\varphi^*(g), c\rangle
\end{aligned}
$$

e φ^* é multiplicativa. Temos, também,

$$
\langle \varphi^*(1), c\rangle = \langle 1, \varphi(c)\rangle = (\varepsilon \circ \varphi)(c) = \varepsilon(c) = \langle 1, c\rangle
$$

o que conclui a prova. ∎

Naturalmente, esperamos que a recíproca desta proposição seja verdadeira. Porém, isto não acontece em geral, pois, como já sabemos, o espaço dual de uma álgebra é garantidamente uma coálgebra quando este tem dimensão finita. Com esta restrição, temos a seguinte proposição.

Proposição 96 *Se A e B são álgebras de dimensão finita e $\varphi : A \to B$ é um homomorfismo de álgebras, então a aplicação linear induzida $\varphi^* : B^* \to A^*$ é um homorfismo de coálgebras.*

Prova. Usando a notação de Sweedler juntamente com a identificação $\varphi^* \otimes \varphi^* = (\varphi \otimes \varphi)^*$, temos

$$\begin{aligned}
\langle((\varphi^* \otimes \varphi^*) \circ \Delta)(f), a \otimes b\rangle &= \langle\Delta(f), \varphi(a) \otimes \varphi(b)\rangle \\
&= \langle f, \varphi(a)\varphi(b)\rangle \\
&= \langle f, \varphi(ab)\rangle \\
&= \langle\varphi^*(f), ab\rangle \\
&= \langle(\Delta \circ \varphi), a \otimes b\rangle
\end{aligned}$$

para todo $a, b \in A$ e toda $f \in B^*$. Além disso,

$$(\varepsilon \circ \varphi^*)(f) = \langle\varphi^*(f), 1\rangle = \langle f, \varphi(1)\rangle = \langle f, 1\rangle = \varepsilon(f).$$

■

3.2.3 Subcoálgebras e coideais

É natural estudar uma álgebra através de suas subálgebras e ideais. Assim, é desejável introduzir conceitos que tenham papel análogo no estudo das coálgebras. Estes são as subcoálgebras e os coideais.

Dado um subespaço D de uma coálgebra C, a noção de coideal em D permitirá atribuir ao quociente de espaços vetoriais C/D uma única estrutura de coálgebra.

Dada uma coálgebra (C, Δ, ε) sobre F, uma *subcoálgebra* é um subespaço D de C satisfazendo à condição $\Delta(D) \subset D \otimes D$. Neste caso, D é uma coálgebra sobre F por si mesma com aplicações de estrutura dadas pelas restrições $\Delta|_D$ e $\varepsilon|_D$ de Δ e ε, respectivamente. A inclusão natural $D \hookrightarrow C$ é claramente um homomorfismo de coálgebras.

Proposição 97 *Seja (C, Δ, ε) uma coálgebra sobre F. Então um subespaço D de C é uma subcoálgebra se, e somente se, $D^\perp \subseteq C^*$ é um ideal bilateral de C^*.*

Prova. $(\Rightarrow)$ A inclusão $i : D \hookrightarrow C$ induz um homomorfismo de álgebras $i^* : C^* \to D^*$, cujo núcleo é exatamente $D^\perp$.

($\Leftarrow$) Recordamos que $D^{\perp\perp} = D$ (cf. Teorema 158 na pág. 170). Seja $c \in D$ e suponhamos que $\Delta(c) = \sum_{i=1}^{n} c_{i1} \otimes c_{i2}$, com $c_{i1}, c_{i2} \in C$. Sem perda de generalidade, podemos assumir que os c_{i2} são linearmente independentes. Se $\Delta(c) \notin D \otimes C$, então devemos ter, a menos de uma reordenação dos índices, $c_{11} \notin D$. Isto significa que deve existir um elemento $f \in D^{\perp}$ tal que $\langle f, c_{11} \rangle \neq 0$. Escolhamos $g \in C^*$ tal que $g(c_{j2}) = \delta_{1j}$. Então, como $D^{\perp}$ é um ideal, $fg \in D^{\perp}$ e daí $\langle fg, c \rangle = 0$. Mas, $\langle fg, c \rangle = \langle f \otimes g, \Delta(c) \rangle$, pela definição da estrutura dual, logo

$$\begin{aligned} 0 &= \langle fg, c \rangle = \left\langle f \otimes g, \sum_{i=1}^{n} c_{i1} \otimes c_{i2} \right\rangle \\ &= \sum_{i=1}^{n} \langle f, c_{i1} \rangle \langle g, c_{i2} \rangle \\ &= \langle f, c_{11} \rangle \langle g, c_{12} \rangle \neq 0, \end{aligned}$$

o que é absurdo. Portanto, devemos ter $\Delta(c) \in D \otimes C$. Analogamente, $\Delta(c) \in C \otimes D$. Finalmente, $\Delta(c) \in (D \otimes C) \cap (C \otimes D) = D \otimes D$, e D é uma subcoálgebra de C ■

Um subespaço D de C é dito um *coideal à esquerda* de C se $\Delta(D) \subset C \otimes D$, um *coideal à direita* de C se $\Delta(D) \subset D \otimes C$, e um *coideal* se $\varepsilon(D) = 0$ e $\Delta(D) \subset D \otimes C + C \otimes D$.

Observamos que, ao contrário do que acontece com ideais de uma álgebra, se D é um coideal, não é preciso que seja coideal à direita ou à esquerda. Além disso, se D é simultaneamente coideal à direita e à esquerda, então D é uma subcoálgebra, e não é um coideal, a menos que $D = 0$, pois somente nesse caso temos $D \otimes C + C \otimes D = D \otimes D$ e $\varepsilon(D) = 0$. Apesar dessa aparente falta de analogia com os ideais, os coideais são as estruturas adequadas à noção de coálgebra quociente. Além disso, os coideais e subcoálgebras de uma coálgebra tem relação com os ideais e subálgebras da álgebra dual na forma expressa pelas seguintes proposições.

Proposição 98 *Seja (C, Δ, ε) uma coálgebra e D um subespaço de C.*

(a) Se D é um coideal à direita (esquerda) então $D^{\perp}$ é um ideal à direita (esquerda) em C^*.

(b) Se I é um ideal à direita (esquerda) em C^* então $I^{\perp}$ é um coideal à direita (esquerda) em C.

(c) D é um coideal à direita (esquerda) se, e somente se, $D^{\perp} \subseteq C^*$ é um ideal à direita (esquerda) de C^*.

Prova. Seja (C^*, μ, η) a álgebra dual. (a) Se D é um coideal, devemos mostrar que $\mu(D^\perp \otimes C^*) \subset D^\perp$, o que equivale a mostrar que $\left\langle \rho(D^\perp \otimes C^*), \Delta(D) \right\rangle = 0$. Mas, isto é verdade pois, $\Delta(D) \subset D \otimes C$, já que D é coideal à direita, e $\left\langle \rho(D^\perp \otimes C^*), D \otimes C \right\rangle = 0$, pela definição de ρ.

(b) Seja I um ideal à direita de C^* e $c \in I^\perp$. Suponhamos que $\Delta(c) = \sum_{i=1}^n a_i \otimes b_i$, com $a_i, b_i \in C$. Sem perda de generalidade, podemos supor que os b_i sejam linearmente independentes. Se $\Delta(c) \notin I^\perp \otimes C$, então, a menos de uma reordenação nos índices, podemos supor que $a_1 \notin I^\perp$. Logo, existe $f \in I$ tal que $\langle f, a_1 \rangle \neq 0$. Escolhemos $g \in C^*$ tal que $\langle g, b_j \rangle = \delta_{1j}$. Então, como I é um ideal à direita, temos $fg \in I$, logo $\langle fg, c \rangle = 0$. Mas, $\langle fg, c \rangle = \langle f \otimes g, \Delta(c) \rangle$, e conseqüentemente

$$\begin{aligned} 0 &= \langle fg, c \rangle \\ &= \left\langle f \otimes g, \sum_{i=1}^n a_i \otimes b_i \right\rangle \\ &= \sum_{i=1}^n \langle f, a_i \rangle \langle g, b_i \rangle \\ &= \langle f, a_1 \rangle \langle g, b_1 \rangle \neq 0. \end{aligned}$$

Com isso, mostramos que, $\Delta(I^\perp) \subset I^\perp \otimes C$, isto é, $I^\perp$ é um coideal à direita de C. A prova para o caso em que I é um ideal à esquerda é análoga.

(c) Segue de (a) e (b) e do fato que $D^{\perp\perp} = D$ (cf. item (d) do Teorema 158 na pág. 146).■

Proposição 99 *Seja (C, Δ, ε) uma coálgebra e D um subespaço de C.*

(a) Se D é um coideal então $D^\perp$ é uma subálgebra *de C^*.*

(b) Se I é uma subálgebra de C^* então $I^\perp$ é um coideal de C.

(c) D é um coideal se, e somente se, $D^\perp$ é uma subálgebra de C^*.

Prova. (a) Como $\varepsilon(D) = 0$, então $\varepsilon \in D^\perp$. Devemos mostrar que $\mu(D^\perp \otimes D^\perp) \subset D^\perp$ ou, equivalentemente, $\left\langle \rho(D^\perp \otimes D^\perp), \Delta(D) \right\rangle = 0$. Esta igualdade é verdadeira, pois $\Delta(D) \subset D \otimes C + C \otimes D$ e

$$\left\langle \rho(D^\perp \otimes D^\perp), \Delta(D) \right\rangle \subset \left\langle \rho(D^\perp \otimes D^\perp), D \otimes C \right\rangle + \left\langle \rho(D^\perp \otimes D^\perp), C \otimes D \right\rangle = 0,$$

pela definição de ρ.

(b) Como I é uma subálgebra de C^*, então $\varepsilon \in I$, isto é, $\varepsilon(I^\perp) = 0$. Além disso, $\mu(I \otimes I) \subset I$, donde $\left\langle \rho(I \otimes I), \Delta(I^\perp) \right\rangle = \left\langle \Delta^* \rho(I \otimes I), I^\perp \right\rangle = \left\langle \mu(I \otimes I), I^\perp \right\rangle \subset \left\langle I, I^\perp \right\rangle = 0$, ou seja, $\Delta(I^\perp) \subset \rho(I \otimes I)^\perp$. Pelo Teorema 159 na pág. 146, segue que $\Delta(I^\perp) \subset C \otimes I^\perp + I^\perp \otimes C$, logo $I^\perp$ é um coideal de C.

(c) Segue de (a) e (b) e de $I^{\perp\perp} = I$. ■

3.2.4 Teorema Fundamental do Isomorfismo para Coálgebras

Podemos, finalmente, enunciar o resultado principal desta subseção.

Teorema 100 (TFI para coálgebras) *Seja C uma coálgebra, D um coideal e $\pi : C \to C/D$ a projeção natural de C sobre o quociente de espaços vetoriais C/D. Então:*

(a) C/D tem uma única estrutura de coálgebra fazendo com que π seja um homomorfismo de coálgebras.

(b) Se $f : C \to C'$ é um homomorfismo qualquer entre coálgebras, então $\ker f$ é um coideal de C.

(c) Se $D \subset \ker f$ então existe um único homomorfismo de coálgebras $\bar{f}$ tornando comutativo o diagrama

$$\begin{tikzcd} C \arrow[rr, "f"] \arrow[dr, "\pi"'] & & C' \\ & C/D \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Prova. (a) Seja C' o espaço vetorial C/D. Como D é um coideal, $D \subset \ker \varepsilon$. Logo, existe uma única aplicação linear $\bar{\varepsilon}$ tornando comutativo o diagrama

$$\begin{tikzcd} C \arrow[rr, "\varepsilon"] \arrow[dr, "\pi"'] & & F \\ & C' \arrow[ur, "\bar{\varepsilon}"'] & \end{tikzcd} \tag{3.16}$$

Seja φ a composição

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{\pi \otimes \pi} C' \otimes C'.$$

Temos $\ker \pi = D$, logo $\ker \pi \otimes \pi = C \otimes D + D \otimes C \supset \Delta(D)$. Portanto, $D \subset \ker \varphi$. Podemos definir $\bar{\Delta}$ como a única aplicação linear tornando comutativo o diagrama

$$\begin{tikzcd} C \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & C' \otimes C' \\ & C' \arrow[u, "\bar{\Delta}"'] \end{tikzcd} \tag{3.17}$$

Um cálculo direto nos permite verificar que (3.17) implica

$$(\mathrm{id} \otimes \bar{\Delta}) \circ \bar{\Delta}(\pi(c)) = (\bar{\Delta} \otimes \mathrm{id}) \circ \bar{\Delta}(\pi(c)),$$

para todo $c \in C$. Como π é sobrejetora, segue que $\bar{\Delta}$ é coassociativa. Similarmente, (3.16) e (3.17) implicam que $\bar{\varepsilon}$ é uma counidade. Conseqüentemente, $(C', \bar{\Delta}, \bar{\varepsilon})$ é uma coálgebra.

Os diagramas (3.16) e (3.17) definem π como um homomorfismo de coálgebras, e como $\bar{\Delta}$ e $\bar{\varepsilon}$ são as únicas aplicações lineares tornando comutativos esses diagramas, certamente são as únicas aplicações de estrutura possíveis. Isto conclui a prova de (a).

(b) Como homomorfismo de coálgebras, f torna comutativo o diagrama

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "f"'] & C \otimes C \arrow[d, "f \otimes f"] \\ C' \arrow[r, "\Delta'"] & C' \otimes C' \end{tikzcd}$$

logo

$$\Delta(\ker f) \subset \ker f \otimes f = C \otimes \ker f + \ker f \otimes C$$

que é a primeira condição da definição de coideal. Ademais, é comutativo o diagrama

$$\begin{tikzcd} C \arrow[dr, "\varepsilon"] \arrow[dd, "f"'] & \\ & F \\ C' \arrow[ur, "\varepsilon'"'] & \end{tikzcd}$$

donde $\varepsilon(\ker f) = 0$, e $\ker f$ é um coideal.

(c) Vamos mostrar que a única aplicação linear que torna comutativo o diagrama

$$\begin{tikzcd} C \arrow[rr, "f"] \arrow[dr, "\pi"'] & & C' \\ & C/D \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

é realmente um homomorfismo de coálgebras.

Aplicando ε' a este diagrama, obtemos

$$\begin{aligned} \varepsilon'(\bar{f}(\pi(c)) &= \varepsilon'(f(c)) = \varepsilon(c) \\ &= \varepsilon(\pi(c)), \end{aligned}$$

pois f é homomorfismo de coálgebras. Como π é sobrejetora, concluímos que $\varepsilon' \circ \bar{f} = \varepsilon$. Do mesmo modo,

$$\begin{aligned} \Delta'(\bar{f}(\pi(c)) &= \Delta' f(c) = (f \otimes f)\Delta(c) \\ &= (\bar{f} \circ \pi) \otimes (\bar{f} \circ \pi)(\Delta(c)) \\ &= (\bar{f} \otimes \bar{f})(\pi \otimes \pi)\Delta(c) \\ &= (\bar{f} \otimes \bar{f})(\Delta'(\pi(c)), \end{aligned}$$

pois π é homomorfismo de coálgebras.

Finalmente, a sobrejetividade de π garante que $\Delta' \circ \bar{f} = (\bar{f} \otimes \bar{f}) \circ \Delta'$. Como antes, a unicidade de $\bar{f}$ como aplicação linear garante sua unicidade como homomorfismo de coálgebras, completando a prova. ∎

3.2.5 Conclusão

Seguimos principalmente o tratamento encontrado no clássico livro de Sweedler [Sw]. Porém, as idéias sobre dualidade foram obtidas de Majid [Ma]. Pudemos observar que nossa intuição tende a falhar na expectativa de encontrar relações completamente análogas entre os ideais de uma álgebra e os coideais de uma coálgebra dual. Explicitamente, tenderiamos a crer que o dual de um ideal fosse um coideal e o dual de uma subálgebra fosse uma subcoálgebra. Apesar da relação ser exatamente oposta, isto não representa nenhuma dificuldade, pois, como vimos, um Teorema Fundamental de Isomorfismo pode ser enunciado e provado utilizando apenas a definição e alguns conceitos da Álgebra Linear. Na verdade, desejávamos encontrar um conceito de coideal que, em certo sentido, fosse compatível com o conceito de ideal em um mesmo conjunto. Isto será posto de maneira mais precisa na seção seguinte.

3.3 Biálgebras

Nas duas seções anteriores, revimos o conceito de álgebra associativa com unidade, e introduzimos o conceito de coálgebra. Dado um conjunto, este poderia ter ambas as estruturas sem que houvesse qualquer relação entre elas. Além disso, como vimos, podemos sempre olhar para uma ou outra estrutura, independentemente. Nesta seção, porém, vamos estudar conjuntos dotados de ambas as estruturas, coexistindo de maneira compatível. Isto é, vamos poder multiplicar e "desagregar" objetos de um mesmo conjunto, dando origem a novos fenômenos algébricos. O objetivo principal é estabelecer um contexto para o estudo das álgebras de Hopf.

3.3.1 Definição e exemplos

Definição 101 (Biálgebra) *Uma* biálgebra *é uma quíntupla $(B, \mu, \eta, \Delta, \varepsilon)$, onde B é um espaço vetorial sobre um corpo F dotado de aplicações lineares μ, η, Δ, ε, tais que:*

(i) (B, μ, η) define uma álgebra,

(ii) (B, Δ, ε) define uma coálgebra,

(iii) A multiplicação μ e a unidade η são homomorfismos de coálgebras,

(iii') A comultiplicação Δ e a counidade ε são homomorfismos de álgebras.

Pode ser mostrado [A, pág. 57] que as condições de compatibilidade (iii) e (iii') da definição são equivalentes. Uma aplicação linear φ entre biálgebras B e B' é um *homomorfismo de biálgebras* se for simultaneamente homorfismo de álgebras e homomorfismo de coálgebras.

Exemplo 102 Seja G um grupo. Pelos exemplos 88 e 92 temos que (FG, μ, η) define uma álgebra e $(FG, \Delta, \varepsilon)$ define uma coalgebra. Estas duas estruturas algébricas são compatíveis já que

$$\Delta(gh) = gh \otimes gh = (g \otimes g)(h \otimes h) = \Delta(g)\Delta(h)$$

e

$$\varepsilon(gh) = 1 = \varepsilon(g)\varepsilon(h).$$

Conseqüentemente $(FG, \mu, \eta, \Delta, \varepsilon)$ é uma biálgebra. $\square$

Exemplo 103 (Álgebra Universal Envolvente) Seja$\mathfrak{g}$ uma álgebra de Lie sobre F. Sua álgebra universal envolvente $U\mathfrak{g}$ é uma álgebra associativa com unidade livremente gerada por 1 e $\mathfrak{g}$, módulo o ideal gerado por todos os elementos do tipo $xy - yx - [xy]$, onde $x, y \in \mathfrak{g}$. Vamos exibir aplicações de estrutura μ, η, Δ, e ε, tais que $(U\mathfrak{g}, \mu, \eta, \Delta, \varepsilon)$ defina uma biálgebra. As aplicações μ e η não requerem menção pois estão implícitas na definição de álgebra associativa. Devemos encontrar Δ e ε.

$\mathfrak{g} \oplus \mathfrak{g}$ é uma álgebra de Lie com produto de lie dado por $[(x_1, x_2), (y_1, y_2)] = ([x_1y_1], [x_2y_2])$, e a aplicação $\delta : \mathfrak{g} \to \mathfrak{g} \oplus \mathfrak{g}$ definida por $x \mapsto (x, x)$, chamada diagonal, é um homomorfismo de álgebras de Lie. A álgebra $U\mathfrak{g}$ é também uma álgebra de Lie com produto de Lie $[xy] = xy - yx$, para todo $x, y \in U\mathfrak{g}$. Usemos a notação $U\mathfrak{g}^-$ para denotar a álgebra universal envolvente de $\mathfrak{g}$ vista como álgebra de Lie. Devido ao Teorema PBW (cf. Teorema 82), a inclusão natural $i : \mathfrak{g} \oplus \mathfrak{g} \to U(\mathfrak{g} \oplus \mathfrak{g})^-$ é um homomorfismo de álgebras de Lie. Conseqüentemente, a composição

$$\mathfrak{g} \xrightarrow{\delta} \mathfrak{g} \oplus \mathfrak{g} \xrightarrow{i} U(\mathfrak{g} \oplus \mathfrak{g})^-$$

é um homomorfismo de álgebras de Lie. Este induz um (único) homomorfismo de álgebras $U\mathfrak{g} \to U(\mathfrak{g} \oplus \mathfrak{g})$, devido à propriedade universal de $U\mathfrak{g}$. Ademais, a aplicação $(x, y) \mapsto x \otimes 1 + 1 \otimes y$ define um isomorfismo natural entre $U(\mathfrak{g} \oplus \mathfrak{g})$ e $U\mathfrak{g} \otimes U\mathfrak{g}$, de modo que temos um homomorfismo de álgebras $\Delta : U\mathfrak{g} \to U\mathfrak{g} \otimes U\mathfrak{g}$.

Afirmamos que $(U\mathfrak{g}, \Delta, \varepsilon)$ define uma coálgebra. De fato, temos $\mathfrak{g} \oplus (\mathfrak{g} \oplus \mathfrak{g}) \cong (\mathfrak{g} \oplus \mathfrak{g}) \oplus \mathfrak{g} \cong \mathfrak{g} \oplus \mathfrak{g} \oplus \mathfrak{g}$ como álgebras de Lie, e assim as aplicações $x \mapsto (x, (x, x))$ e $x \mapsto ((x, x), x)$ se identificam a uma única aplicação $\mathfrak{g} \to \mathfrak{g} \oplus \mathfrak{g} \oplus \mathfrak{g}$. Portanto, as aplicações induzidas também se identificam a uma única aplicação $U\mathfrak{g} \longrightarrow U\mathfrak{g} \otimes U\mathfrak{g} \otimes U\mathfrak{g}$. Mas, no primeiro caso, temos $(\mathrm{id} \otimes \Delta) \circ \Delta$, e no segundo, $(\Delta \otimes \mathrm{id}) \circ \Delta$, de modo que a igualdade das aplicações induzidas se traduz na coassociatividade de Δ. De maneira similar, $\mathfrak{g} \to \mathfrak{g} \oplus \mathfrak{g} \to \mathfrak{g} \oplus 0 \to \mathfrak{g}$, dada por $x \mapsto (x, x) \mapsto (x, 0) \mapsto x$ induz $(\mathrm{id} \otimes \varepsilon) \circ \Delta : U\mathfrak{g} \to U\mathfrak{g}$. Mas, esta induz também $\mathrm{id} : U\mathfrak{g} \to U\mathfrak{g}$, logo deve ser, $(\mathrm{id} \otimes \varepsilon) \circ \Delta = \mathrm{id}$. Analogamente, $\mathrm{id} = (\varepsilon \otimes \mathrm{id}) \circ \Delta$, mostrando a afirmação.

Finalmente, como Δ e ε são homorfismos de álgebras, temos que $(U\mathfrak{g}, \mu, \eta, \Delta, \varepsilon)$ é uma biálgebra. □

Definição 104 *Um subespaço I de uma biálgebra B é dito* bi-ideal *se for simultaneamente um ideal e um coideal, i.é, se*

$$\mu(B \otimes I + I \otimes B) \subset I, \quad \Delta(I) \subset B \otimes I + I \otimes B, \quad \varepsilon(I) = 0.$$

3.3.2 Teorema Fundamental do Isomorfismo para Biálgebras

Concluímos a seção com seu principal resultado, expresso pelo seguinte teorema.

Teorema 105 (TFI para biálgebras) *Seja B uma biálgebra, D um bi-ideal e $\pi : B \to B/D$ a projeção natural de B sobre o quociente de espaços vetoriais de B/D. Então:*

(a) B/D tem uma única estrutura de biálgebra fazendo com que π seja um homomorfismo de biálgebras.

(b) Se $f : B \to B'$ é um homomorfismo qualquer entre biálgebras, então $\ker f$ é um bi-ideal de B.

(c) Se $D \subset \ker f$ então existe um único homomorfismo de biálgebras $\bar{f}$ tornando comutativo o diagrama

$$\begin{tikzcd} B \arrow[rr, "f"] \arrow[dr, "\pi"'] & & B' \\ & B/D \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Prova. O Teorema 90 nos fornece aplicações de estrutura $\bar{\mu}$ e $\bar{\eta}$ tal que $(B/D, \bar{\mu}, \bar{\eta})$ corresponda a uma álgebra associativa com unidade. O Teorema 100, por outro lado, nos fornece aplicações de estrutura $\bar{\Delta}$ e $\bar{\varepsilon}$ tal que $(B/D, \bar{\Delta}, \bar{\varepsilon})$ corresponda a uma coálgebra. Ademais, os diagramas apresentados nas provas desses dois teoremas definem π como um homomorfismo de biálgebras. Assim, precisamos apenas mostrar que $\bar{\Delta}$ e $\bar{\varepsilon}$ são homomorfismos de álgebras.

Com efeito, denotando $\pi(a)$ por $\bar{a}$ e $\mu(ab)$ por ab, vem que

$$\begin{aligned}(\bar{\Delta} \circ \bar{\mu})(\bar{a} \otimes \bar{b}) &= \bar{\Delta}(\overline{ab}) = \overline{\Delta(ab)} = \overline{(\mu \circ \Delta)(a \otimes b)} \\ &= \overline{\mu}(\overline{\Delta(a \otimes b)}) = (\bar{\mu} \circ \bar{\Delta})(\bar{a} \otimes \bar{b}),\end{aligned}$$

para todo $a, b \in B$. Como π é sobrejetora, resulta $\bar{\Delta} \circ \bar{\mu} = \bar{\mu} \circ \bar{\Delta}$. Por outro lado,

$$\begin{aligned}\bar{\Delta} \circ \bar{\eta} &= \bar{\Delta} \circ \pi \circ \eta = (\pi \otimes \pi) \circ \Delta \circ \eta \\ &= (\pi \otimes \pi)(\eta \otimes \eta) = \bar{\eta} \otimes \bar{\eta}.\end{aligned}$$

Isto mostra que $\bar{\Delta}$ é um homomorfismo de álgebras. Um argumento semelhante se aplica a $\bar{\varepsilon}$, concluindo a prova. ∎

3.4 Álgebras de Hopf

O espaço $\mathcal{F}(M)$ das funções C^{∞} sobre uma variedade diferenciável M define uma álgebra comutativa com as operações de adição e de multiplicação ponto-a-ponto usuais. Se G é um grupo de Lie, então a aplicação multiplicação μ, a aplicação unidade η, e a inversão ι de G são aplicações (infinitamente) diferenciáveis que induzem em $\mathcal{F}(G)$ aplicações de estrutura adicionais, a saber, a comultiplicação $\Delta : \mathcal{F}(G) \to \mathcal{F}(G) \otimes \mathcal{F}(G)$ (definindo o produto tensorial convenientemente), a counidade $\varepsilon : \mathcal{F}(G) \to F$ e a aplicação antípoda $S : \mathcal{F}(G) \to \mathcal{F}(G)$.

Como já vimos na seção anterior, as aplicações Δ e ε definem $\mathcal{F}(G)$ como uma bi-álgebra que, acrescida da aplicação antípoda S, representa a classe das álgebras de Hopf. Estas tiveram origem na década de 40 com a axiomatização dos trabalhos de H. Hopf sobre propriedades topológicas dos grupos de Lie, de onde provém tal denominação. Porém, apenas na década de 60 é que estas despertaram interesse como estrutura algébrica, tornando-se objeto de estudo per si. Contudo, apenas mais recentemente, é que os trabalhos de Drinfeld, motivados por aplicações da Física-Matemática, estenderam e colocaram as álgebras de Hopf numa posição de destaque. Atualmente, algumas de suas principais aplicações são:

1. Método do Espalhamento Inverso,

2. Modelos de Vértices Exatamente Solúveis (Mecânica Estatística),

3. Teoria de Nós e Invariantes de 3-variedades,

4. Teorias de Campos Conformes,

5. Abordagem geométrica não-comutativa à Física na escala de Planck,

6. Extensões da Teoria de Galois.

Conforme atesta o excelente tratado de Chari & Pressley [CP], há atualmente uma intensa interação entre a Física e a Matemática no campo das Álgebras de Hopf e, particularmente, dos Grupos Quânticos. Apesar da freqüente aparição das álgebras de Hopf e de idéias correlatas na literatura, ainda não se tem identificado precisamente o papel fundamental dessas álgebras. Há um consenso entre os especialistas de que um estudo mais detalhado de sua estrutura possa lançar alguma luz sobre pontos ainda obscuros das aplicações, gerando grande expectativa.

Nesta seção, faremos uma definição sistemática das álgebras de Hopf e apresentaremos alguns fatos elementares, preparando o contexto para a introdução dos Grupos Quânticos na próxima seção.

3.4.1 Definição e exemplos

Definição 106 (Álgebra de Hopf) *Uma* álgebra de Hopf *é uma sêxtupla* $(H, \mu, \eta, \Delta, \varepsilon, S)$, *consistindo de um espaço vetorial* H *sobre um corpo* F *e de aplicações lineares* μ, η, Δ, ε, S *satisfazendo as condições:*

(i) $(H, \mu, \eta, \Delta, \varepsilon)$ *define uma biálgebra,*

(ii) a aplicação $S : H \to H$*, chamada* antípoda*, torna comutativos os diagramas*

$$\begin{array}{ccc} H\otimes H & \xrightarrow{\mathrm{id}\otimes S} & H\otimes H \\ \Delta\uparrow & & \downarrow\mu \\ H & \xrightarrow{\eta\circ\varepsilon} & H \end{array} \qquad \begin{array}{ccc} H\otimes H & \xrightarrow{S\otimes\mathrm{id}} & H\otimes H \\ \Delta\uparrow & & \downarrow\mu \\ H & \xrightarrow{\eta\circ\varepsilon} & H \end{array}$$

ou equivalentemente, $\mu \circ (S \otimes \mathrm{id}) \circ \Delta = \eta \circ \varepsilon = \mu \circ (\mathrm{id} \otimes S) \circ \Delta$.

Um *homomorfismo de álgebras de Hopf* é um homomorfismo de biálgebras φ entre duas álgebras de Hopf H e H' tornando comutativo o diagrama

$$\begin{tikzcd} H \arrow[r, "\varphi"] \arrow[d, "S"'] & H' \arrow[d, "S'"] \\ H \arrow[r, "\varphi"] & H' \end{tikzcd}$$

ou, equivalentemente, $\varphi \circ S = S' \circ \varphi$, onde S e S' são as aplicações antípodas de H e H', respectivamente.

Um bi-ideal J de uma álgebra de Hopf H é um *Ideal de Hopf* se $S(J) \subset J$.

Teorema 107 (TFI para Álgebras de Hopf) *Sejam H e H' álgebras de Hopf, $f : H \to H'$ um homomorfismo de álgebras de Hopf, $J \subset H$ um ideal de Hopf e $\pi : H \to H/J$ a projeção natural sobre o espaço vetorial quociente H/J. Então:*

(a) $L = H/J$ admite uma única estrutura de álgebra de Hopf tal que π seja um homomorfismo de álgebras de Hopf.

(b) $\ker f$ é um ideal de Hopf.

(c) Se $J \subset \ker f$, então existe um único homomorfismo de álgebras de Hopf $\bar{f}$ tornando comutativo o diagrama

$$\begin{tikzcd} H \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H' \\ & H/J \arrow[ur, "\bar{f}"'] & \end{tikzcd} \tag{3.18}$$

Prova. A prova deste resultado é essencialmente análoga à do Teorema 105. Este nos fornece aplicações de estrutura $\bar{\mu}$, $\bar{\eta}$, $\bar{\Delta}$ e $\bar{\varepsilon}$ tais que $(L, \bar{\mu}, \bar{\eta}, \bar{\Delta}, \bar{\varepsilon})$ é uma biálgebra. Precisamos mostrar apenas os fatos relacionados à aplicação antípoda:

(a) Seja $\pi : H \to L$ a projeção natural. Pelo Teorema 100a, esta é um homomorfismo de biálgebras. Se φ é a composição

$$H \xrightarrow{S} H \xrightarrow{\pi} L,$$

então, devemos ter $J \subset \ker \varphi$, pois J é um ideal de Hopf. Logo, existe uma única aplicação linear $\bar{S}$ tornando comutativo o diagrama

$$\begin{tikzcd} H \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & L \\ & L \arrow[ur, "\bar{S}"'] & \end{tikzcd} \tag{3.19}$$

Um cálculo direto nos permite verificar que $(\bar{\mu} \circ (\mathrm{id} \otimes \bar{S}) \circ \bar{\Delta})(\pi(c)) = \bar{\eta} \circ \bar{\varepsilon}(\pi(c)) = \bar{\mu} \circ (\bar{S} \otimes \mathrm{id}) \circ \bar{\Delta})(\pi(c))$. Como π é sobrejetora, concluímos que $\bar{S}$ é uma aplicação antípoda de L. Ademais, (3.19) nos define π como um homomorfismo de álgebras de Hopf. Conseqüentemente $(L, \bar{\mu}, \bar{\eta}, \bar{\Delta}, \bar{\varepsilon}, \bar{S})$ é uma álgebra de Hopf. A unicidade desta estrutura segue da unicidade das aplicações lineares subjacentes, provando (a).

(b) Pelo Teorema 100b, $\ker f$ é um bi-ideal. Se S' é a aplicação antípoda de H' e $c \in \ker f$, temos $0 = S'(f(c)) = f(S(c))$, pois f é homomorfismo de álgebras de Hopf. Portanto, $S(c) \in \ker f$, o qual vem a ser é um ideal de Hopf.

(c) O Teorema 100b nos fornece um único homomorfismo de biálgebras tornando comutativo o diagrama (3.18). Para todo $c \in H$, temos

$$\begin{aligned} (\bar{f} \circ \bar{S})(\pi(c)) &= (\bar{f} \circ \pi)(S(c)) \\ &= f(S(c)) \\ &= (S' \circ f)(c) \\ &= (S' \circ \bar{f})(\pi(c). \end{aligned}$$

Como π é sobrejetora, segue que $\bar{f}$ é um homomorfismo de álgebras de Hopf.

3.4.2 Álgebra de Convolução

O conceito que vamos introduzir permite obter importantes propriedades da aplicação antípoda de uma álgebra de Hopf. Dada uma coálgebra (C, Δ, ε) e uma álgebra (A, μ, η) sobre F, consideremos $M = \mathrm{Hom}_F(C, A)$, o espaço vetorial das aplicações lineares de C em A. Se $f, g \in M$, então $\mu \circ (f \otimes g) \circ \Delta$ é também um elemento de M, pois é linear, como composição de aplicações lineares, e vai de C em A. Desse modo, está bem definida a aplicação $\mu_M : M \otimes M \to M$ dada por $f \otimes g \mapsto \mu \circ (f \otimes g) \circ \Delta$. Um cálculo imediato permite verificar que μ_M é linear.

Além disso, para todo $c \in C$, e toda $f, g, h \in M$,

$$\begin{aligned}
\mu_M(\mu_M(f \otimes g) \otimes h)(c) &= f(c_{(1)(1)})g(c_{(1)(2)})h(c_{(2)}) \\
&= f(c_{(1)})g(c_{(2)(1)})h(c_{(2)(2)}) \\
&= \mu_M(f \otimes \mu_M(g \otimes h))(c),
\end{aligned}$$

isto é, a aplicação μ_M é uma multiplicação associativa.

Temos ainda que, para todo $\lambda \in F$, a aplicação $\lambda\eta \circ \varepsilon$ também pertence a M, de modo que $\lambda \mapsto \lambda\eta \circ \varepsilon$ define uma aplicação linear $\eta_M : F \to M$. Para todo $\lambda \in F$ e toda $f \in M$, temos

$$\begin{aligned}
(\mu_M \circ (\eta_M \otimes \mathrm{id}))(\lambda \otimes f) &= \mu_M(\eta_M(\lambda) \otimes f) \\
&= \mu \circ ((\lambda\eta \circ \varepsilon) \otimes f) \circ \Delta \\
&= \mu \circ (\eta \otimes \mathrm{id}_C) \circ (\lambda \otimes f) \circ (\varepsilon \otimes \mathrm{id}_A) \circ \Delta \\
&= \lambda \otimes f.
\end{aligned}$$

Analogamente,

$$(\mu_M \circ (\mathrm{id} \otimes \eta_M))(f \otimes \lambda) = f \otimes \lambda = \lambda \otimes f.$$

Isto é, η_M é uma unidade e, conseqüentemente, (M, μ_M, η_M) é uma álgebra associativa com unidade $1_M = \eta \circ \varepsilon$. Esta é denominada *álgebra de convolução*.

Costuma-se denotar $\mu_M(f \otimes g)$ por $f * g$. Observemos que $f * g(c) = f(c_{(1)})g(c_{(2)})$ e, também, que $1_M(c) = (\eta \circ \varepsilon)(c) = \varepsilon(c)1_A$, de modo que podemos ver $\varepsilon(c)$ como um elemento da álgebra A (através da inclusão η), escrevendo simplesmente $1_M(c) = \varepsilon(c)$.

3.4.3 Propriedades da Aplicação Antípoda

A álgebra de convolução permite obter uma caracterização bastante precisa da aplicação antípoda de uma álgebra de Hopf, inclusive garantindo sua unicidade. Veremos isto a seguir.

Se $(H, \mu, \eta, \Delta, \varepsilon, S)$ é uma álgebra de Hopf sobre F, denotamos por H^C a coálgebra (H, Δ, ε) e por H^A a álgebra (H, μ, η). Com isto, temos que $M = \mathrm{Hom}_F(H^C, H^A)$ é uma álgebra de convolução. Por definição, a aplicação antípoda satisfaz

$$S * \mathrm{id} = \mathrm{id} * S = 1_M,$$

isto é S é o elemento inverso de id na álgebra de convolução. Uma conseqüência imediata desta propriedade é a unicidade da aplicação antípoda.

Proposição 108 *A aplicação antípoda S de uma álgebra de Hopf H tem as seguintes propriedades*

(a) $S(ab) = S(b)S(a)$, *para todo* $a, b \in H$,

(b) $S(1_H) = 1_H$,

(c) $(S \otimes S) \circ \Delta = \Delta' \circ S$,

(d) $\varepsilon \circ S = \varepsilon$,

onde $\Delta' = \tau \circ \Delta$.

Prova. (a) Basta verificar que $(S \circ \mu) * \mu = \mu * (\mu \circ (S \otimes S) \circ \tau) = 1$. De fato, para todo $a, b \in H$ temos

$$\begin{aligned}
((S \circ \mu) * \mu)(a \otimes b) &= (S \circ \mu)((a \otimes b)_{(1)})\mu((a \otimes b)_{(2)}) \\
&= (S \circ \mu)(a_{(1)} \otimes b_{(1)})\mu(a_{(2)} \otimes b_{(2)}) \\
&= S(a_{(1)}b_{(1)})a_{(2)}b_{(2)} \\
&= S((ab)_{(1)})\,(ab)_{(2)} \\
&= (S * \mathrm{id})(ab) \\
&= \varepsilon(ab) = \varepsilon(a)\varepsilon(b).
\end{aligned}$$

e

$$\begin{aligned}
(\mu * (\mu \circ (S \otimes S) \circ \tau))(a \otimes b) &= \mu((a \otimes b)_{(1)})(\mu \circ (S \otimes S) \circ \tau)((a \otimes b)_{(2)}) \\
&= \mu(a_{(1)} \otimes b_{(1)})(\mu \circ (S \otimes S) \circ \tau)(a_{(2)} \otimes b_{(2)})
\end{aligned}$$

$$\begin{aligned} &= a_{(1)}b_{(1)}S(b_{(2)})S(a_{(2)}) \\ &= a_{(1)}\varepsilon(b)S(a_{(2)}) \\ &= \varepsilon(a)\varepsilon(b). \end{aligned}$$

(b) Como $\Delta(1_H) = 1_H \otimes 1_H$, temos $1_H = \varepsilon(1_H) = (\mathrm{id} * S)(1_H) = S(1_H)$.

As demais propriedades seguem de maneira semelhante. ∎

Observação. As propriedades (a) e (b) da proposição definem S como um *anti-homomorfismo de álgebras*, enquanto que, as propriedades (c) e (d) definem S como um *anti-homomorfismo de coálgebras.*

Proposição 109 *Se H é uma álgebra de Hopf comutativa ou cocomutativa, então* $S^2 = S \circ S =$ id.

Prova. Se H é comutativa ou cocomutativa, então

$$\begin{aligned} S * (S^2)(c) &= S(c_{(1)})S^2(c_{(2)}) \\ &= S(S(c_{(2)})c_{(1)}) \\ &\overset{\text{hip.}}{=} S(c_{(1)}S(c_{(2)})) \\ &= (S \circ \varepsilon)(c) \\ &= \varepsilon(c) \\ &= (S * \mathrm{id})(c). \end{aligned}$$

Conseqüentemente, $S^2 = \mathrm{id}$. ∎

3.4.4 Conclusão

Historicamente, os exemplos mais simples de álgebras de Hopf são aqueles provenientes de grupos. De fato, muitas propriedades dos grupos se generalizam neste caso e, particularmente, no caso das álgebras de Hopf quasitriangulares, que estudaremos na próxima seção. Estas encontram-se associadas às soluções da Equação de Yang-Baxter Quântica (QYBE), as quais surgiram primeiramente nos trabalhos de Baxter sobre os Modelos de Rede (Vértices) Exatamente Solúveis.

Segundo Majid [Ma], a compreensão do verdadeiro significado da QYBE vem da Teoria das Tranças e dos Nós. A grosso modo, a cada solução da QYBE corresponde um invariante de tranças (e de nós), e também um modelo de rede exatamente solúvel. Muitas soluções da QYBE podem ser obtidas a partir de representações de álgebras de Hopf quasitriangulares (cf. Drinfeld [D]). Aliás, este é o modo como essas álgebras surgiram historicamente.

Nesta seção baseamo-nos principalmente em Abe [A], Majid [Ma], e Chari & Pressley [CP].

Capítulo 4

Grupos Quânticos

4.1 Álgebras de Hopf quasitriangulares

Seja H uma álgebra de Hopf sobre F. Como veremos, uma álgebra de Hopf quasitriangular, é simplesmente uma álgebra de Hopf cuja comultiplicação foi "perturbada" por um elemento inversível $R \in H \otimes H$. A surpreendente propriedade destas álgebras é que R satisfaz, como condição de consistência, a Equação de Yang-Baxter Quântica (QYBE) $R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}$. Esta estabelece uma conexão com a Física dos Sistemas Integráveis da Mecânica Estatística. Reciprocamente, a partir de uma solução matricial regular R da QYBE, é possível construir abstratamente uma álgebra de Hopf quasitriangular. Além disso, tais álgebras representam uma ampla classe de álgebras de Hopf que não são nem comutativas, nem cocomutativas.

4.1.1 Definição e exemplos

O elemento R pode ser escrito

$$R = \sum_{i=1}^{n} R_{1i} \otimes R_{2i} \tag{4.1}$$

para algum inteiro positivo n, e $R_{1i}, R_{2i} \in H$. Com a notação de Sweedler, escrevemos

$$R = R^{(1)} \otimes R^{(2)}. \tag{4.2}$$

onde novamente enfatizamos que $R^{(1)}$ e $R^{(2)}$ não são propriamente elementos de H.

Se $m > 1$, $1 \leq i \neq j \leq m$ são inteiros positivos, definimos R_{ij} como a imagem de R pela inclusão canônica $H \otimes H \hookrightarrow H^{\otimes m}$ definida por

$$a \otimes b \mapsto 1 \otimes \cdots \otimes 1 \otimes \underset{\substack{\uparrow \\ i}}{a} \otimes 1 \otimes \cdots \otimes 1 \otimes \underset{\substack{\uparrow \\ j}}{b} \otimes 1 \otimes \cdots \otimes 1$$

para todo $a, b \in H$. Em palavras, R_{ij} é o elemento R nos fatores i e j da potência tensorial $H^{\otimes m}$ e 1 nos demais fatores. Isto nos sugere utilizar a notação de Sweedler do seguinte modo:

$$R_{ij} = 1 \otimes \cdots \otimes 1 \otimes \underset{\substack{\uparrow \\ i}}{R^{(1)}} \otimes 1 \otimes \cdots \otimes 1 \otimes \underset{\substack{\uparrow \\ j}}{R^{(2)}} \otimes 1 \otimes \cdots \otimes 1$$

Como as inclusões canônicas são claramente homomorfismos de álgebras, se R for um elemento inversível, então teremos $(R_{ij})^{-1} = (R^{-1})_{ij}$. Desse modo, podemos escrever inequivocamente R_{ij}^{-1} para o inverso do elemento R_{ij} em $H^{\otimes m}$. De fato, $R_{ij}R_{ij}^{-1} = R_{ij}(R^{-1})_{ij} = (RR^{-1})_{ij} = 1$.

Definição 110 (Álgebra de Hopf quasitriangular) *Uma* álgebra de Hopf quasitriangular *é um par (H, R) consistindo de uma álgebra de Hopf $H = (H, \mu, \eta, \Delta, \varepsilon, S)$ e de um elemento inversível $R \in H \otimes H$, chamado R-*matriz universal*, satisfazendo as condições:*

$$(\Delta \otimes \mathrm{id})(R) = R_{13}R_{23}, \qquad (\mathrm{id} \otimes \Delta)(R) = R_{13}R_{12} \tag{4.3}$$

e

$$\Delta'(h) = R\Delta(h)R^{-1}, \text{ para todo } h \in H. \tag{4.4}$$

onde $\Delta' = \tau \circ \Delta$ e τ é a aplicação transposição. Se, ademais, valer

$$R_{21}^{-1} = R_{12}, \tag{4.5}$$

então diremos que (H, R) é triangular.

Observemos que as equações (4.3) estão dadas em $H \otimes H \otimes H$.

Vamos agora ver que *a aplicação transposição τ é um isomorfismo de álgebras de Hopf.*

Com efeito, se C e D são álgebras de Hopf, temos

$$((\tau \otimes \tau) \circ \Delta)(c \otimes d) = b_{(1)} \otimes a_{(1)} \otimes b_{(2)} \otimes a_{(2)} = (\Delta \circ \tau)(c \otimes d),$$

$$\varepsilon(\tau(a \otimes b)) = \varepsilon(b)\varepsilon(a) = \varepsilon(a)\varepsilon(b) = \varepsilon(a \otimes b),$$

$$(\tau \circ \mu)(a \otimes b \otimes c \otimes d) = bd \otimes ac = \mu(b \otimes a \otimes d \otimes c) = (\mu \circ (\tau \otimes \tau))(a \otimes b \otimes c \otimes d),$$

$$\tau(1) = 1 \otimes 1 = 1,$$

$$(S \circ \tau)(a \otimes b) = S(b) \otimes S(a) = (\tau \circ S)(a \otimes b).$$

Em vista dessa observação, podemos construir uma representação importante do grupo simétrico S_m sobre uma potência tensorial $H^{\otimes m}$ de uma álgebra de Hopf H. O grupo simétrico é gerado pelas transposições $(1,2), (2,3), \ldots, (i, i+1), \ldots, (m-1, m)$. Para cada transposição $(i, i+1)$, onde $i = 1, \ldots, m-1$, definimos o valor da representação como sendo a aplicação

$$\tau_{i,i+1} = \underbrace{\mathrm{id} \otimes \cdots \otimes \mathrm{id}}_{(i-1)\text{-vezes}} \otimes \tau \otimes \underbrace{\mathrm{id} \otimes \cdots \otimes \mathrm{id}}_{(m-1-i)\text{-vezes}} \colon H^{\otimes m} \to H^{\otimes m},$$

que é claramente um isomorfismo de álgebras de Hopf. Qualquer composição destas aplicações é ainda um isomorfismo de álgebras de Hopf, logo a representação está bem-definida. Se σ é uma permutação em S_m, denotamos τ_σ a imagem de σ por essa aplicação. Como σ se decompõe (ainda que não unicamente) num produto dos geradores acima, τ_σ é simplesmente o produto das imagens desses geradores pela representação. A saber, se $\sigma = \gamma_1 \cdots \gamma_k$, onde os γ_i são transposições geradoras, então $\tau_\sigma = \tau_{\gamma_1} \cdots \tau_{\gamma_k}$. Intuitivamente, se $1 \leq i \neq j \leq m$ são dois inteiros, τ_{ij} é simplesmente a aplicação transposição τ alternando os fatores i e j da potência tensorial $H^{\otimes m}$ respectivamente. Por essa razão, continuaremos a chamar τ_{ij} de aplicação transposição.

Exemplo 111 (A álgebra $U_q\mathfrak{s}l(2,\mathbb{C})$) Consideremos, para $q \in \mathbb{C}$, a álgebra não-comutativa $U_q\mathfrak{sl}(2,\mathbb{C})$ com geradores 1, $q^{\frac{H}{2}}$, X^+, X^-, $q^{-\frac{H}{2}}$, satisfazendo as relações

$$q^{\pm \frac{H}{2}} q^{\mp \frac{H}{2}} = 1,$$

$$
\begin{aligned}
q^{\frac{H}{2}} X^{\pm} q^{-\frac{H}{2}} &= q^{\pm 1} X^{\pm}, \\
[X^{+} X^{-}] &= \frac{q^{H} - q^{-H}}{q - q^{-1}}.
\end{aligned}
$$

No limite formal quando $q \to 1$, essas relações de comutação nos fornecem

$$
\begin{aligned}
[H X^{\pm}] &= 2X^{\pm}, \\
[X^{+} X^{-}] &= H,
\end{aligned}
$$

donde vemos que, neste limite, $U_q\mathfrak{sl}(2,\mathbb{C})$ tende à álgebra universal envolvente $U\mathfrak{sl}(2,\mathbb{C})$ da álgebra de Lie $\mathfrak{sl}(2,\mathbb{C})$. Esta é uma álgebra de Hopf com estrutura de coálgebra dada por

$$
\begin{aligned}
\Delta(q^{\pm\frac{H}{2}}) &= q^{\pm\frac{H}{2}} \otimes q^{\pm\frac{H}{2}}, & \varepsilon(q^{\pm\frac{H}{2}}) &= 1, \\
\Delta(X^{\pm}) &= q^{\frac{H}{4}} \otimes X^{\pm} + X^{\pm} \otimes q^{-\frac{H}{4}}, & \varepsilon(X^{\pm}) &= 0,
\end{aligned}
$$

e aplicação antípoda é dada por

$$
S(q^{\pm\frac{H}{2}}) = q^{\mp\frac{H}{2}}, \qquad S(X^{\pm}) = -q^{\pm 1} X^{\pm}.
$$

O elemento

$$
R = q^{H\otimes H/2} \sum_{n=0}^{\infty} \frac{(1-q^{-2})^n}{[\![n]\!]_q!} (q^{\frac{H}{2}} X^{+} \otimes q^{-\frac{H}{2}} X^{-})^n q^{n(n-1)/2}
$$

onde

$$
[\![n]\!]_q = \frac{q^n - q^{-n}}{q - q^{-1}} \quad (n \geq 0)
$$

e

$$
[\![n]\!]_q! = [\![n]\!]_q \, [\![n-1]\!]_q \cdots [\![1]\!]_q \, ,
$$

satisfaz as condições para que $U_q(\mathfrak{sl}(2,\mathbb{C}))$ seja uma álgebra de Hopf quasitriangular.

Os números $[\![n]\!]_q$ e $[\![n]\!]_q!$ são denominados *q-número inteiro* e *q-fatorial*, respectivamente, e vale

$$
[\![n]\!]_q = \frac{1 - q^{-n}}{1 - q^{-1}} = 1 + q^{-1} + \cdots + q^{-n+1} \quad (n > 0),
$$

Portanto, $[\![n]\!]_1 = n$, e $[\![n]\!]_1!$ é o fatorial usual $n! = n(n-1)\cdots 1$.

O elemento R acima não é precisamente um elemento de $U_q\mathfrak{sl}(2,\mathbb{C})\otimes U_q\mathfrak{sl}(2,\mathbb{C})$, já que este contém apenas somas finitas. Isto pode ser contornado num contexto topológico (i.é, tomando-se um completamento adequado desse produto tensorial). □

Exemplo 112 (Sweedler) Seja F um corpo com característica distinta de 2. Consideremos a álgebra associativa A gerada por 1, g, x, satisfazendo as relações

$$g^2 = 1, \qquad x^2 = 0, \qquad gxg = -x,$$

estrutura de coálgebra dada por

$$\begin{aligned} \Delta(g) &= g\otimes g, & \Delta(x) &= x\otimes g + 1\otimes x, \\ \varepsilon(g) &= 1, & \varepsilon(x) &= 0, \end{aligned}$$

e aplicação antípoda dada por

$$S(g) = g, \qquad S(x) = -x.$$

Um cálculo direto permite verificar que a definição de Δ, ε, sobre os geradores se estendem a homomorfismos de álgebras, e que a definição de S sobre os geradores se estende a um anti-homomorfismo de álgebras. Além disso, o conjunto $\{1, g, x, gx\}$ forma uma base de A sobre F.

A possui as seguintes propriedades:

(a) $A^* \cong A$ como álgebras de Hopf. De fato, seja $\{1^*, g^*, x^*, x^*g^*\}$ a base de A^* dual da base $\{1, g, x, gx\}$ de A. Definindo $\alpha = 1^* - g^*$ e $\beta = x^* - x^*g^*$, temos

$$\begin{aligned} \left\langle \alpha^2, g\right\rangle &= \langle \alpha\otimes\alpha, \Delta(g)\rangle = \langle \alpha, g\rangle^2 \\ &= (\langle 1^*, g\rangle - \langle g^*, g\rangle)^2 = (0-1)^2 = 1, \end{aligned}$$

$$\begin{aligned} \left\langle \alpha^2, x\right\rangle &= \langle \alpha\otimes\alpha, \Delta(x)\rangle \\ &= \langle \alpha\otimes\alpha, x\otimes g + 1\otimes x\rangle \end{aligned}$$

$$= \quad \langle \alpha, x\rangle \langle \alpha, g\rangle + \langle \alpha, 1\rangle \langle \alpha, x\rangle = 0 \quad e$$

$$\begin{aligned}
\left\langle \alpha^2, gx \right\rangle &= \langle \alpha \otimes \alpha, \Delta(gx)\rangle \\
&= \langle \alpha \otimes \alpha, (g \otimes g)(x \otimes g + 1 \otimes x)\rangle \\
&= \langle \alpha, gx\rangle \langle \alpha, 1\rangle + \langle \alpha, g\rangle \langle \alpha, gx\rangle = 0,
\end{aligned}$$

permitindo-nos concluir que $\alpha^2 = \varepsilon$. Cálculos semelhantes conduzem a,

$$\begin{aligned}
\beta^2 &= 0, & \alpha\beta\alpha &= -\beta \\
\Delta(\alpha) &= \alpha \otimes \alpha, & \Delta(\beta) &= \beta \otimes \alpha + \varepsilon \otimes \beta \\
\alpha(1) &= 1, & \beta(1) &= 0.
\end{aligned}$$

Evidentemente, $\{\varepsilon, \alpha, \beta, \alpha\beta\}$ formam uma base de A^*, logo, as relações acima são precisamente as que definem A sobre esses geradores.

(b) A é quasitriangular. De fato, para qualquer $\lambda \in F$, o elemento

$$R = \frac{1}{2}(1 \otimes 1 + 1 \otimes g + g \otimes 1 - g \otimes g) + \frac{\lambda}{2}(x \otimes x + x \otimes gx + gx \otimes gx - gx \otimes x)$$

é uma R-matriz universal de A e toda R-matriz de A é dessa forma.

□

4.1.2 Álgebras de Hopf quasitriangulares e a QYBE

Proposição 113 *Se (H, R) é uma álgebra de Hopf quasitriangular, então*

(a) R satisfaz a QYBE: $R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}$.

(b) $(\varepsilon \otimes \mathrm{id})(R) = 1 = (\mathrm{id} \otimes \varepsilon)(R)$. *Como R é inversível, isto implica* $(\varepsilon \otimes \mathrm{id})(R^{-1}) = 1 = (\mathrm{id} \otimes \varepsilon)(R^{-1})$.

(c) $(S \otimes \mathrm{id})(R) = R^{-1}$ *e* $(\mathrm{id} \otimes S)(R^{-1}) = R$ *(donde $(S \otimes S)(R) = R$).*

Prova. (a)Aplicando τ_{12} a ambos os lados de (4.3), obtemos $(\Delta' \otimes \mathrm{id})(R) = R_{23}R_{13}$, onde $\Delta' = \tau \circ \Delta$. Logo,

$$R_{23}R_{13}R_{12} = (\Delta' \otimes \mathrm{id})(R) = R_{12}(\Delta \otimes \mathrm{id})(R)R_{12}^{-1}R_{12} = R_{12}R_{13}R_{23}.$$

(b) Aplicando $(\varepsilon \otimes \mathrm{id} \otimes \mathrm{id})$ à primeira igualdade de (4.3) obtemos

$$\begin{aligned} R &= (\varepsilon \otimes \mathrm{id} \otimes \mathrm{id})(\Delta \otimes \mathrm{id})(R) = (\varepsilon \otimes \mathrm{id} \otimes \mathrm{id})(R_{13}R_{23}) \\ &= (\varepsilon \otimes \mathrm{id})(R) \cdot R \end{aligned}$$

e aplicando $(\mathrm{id} \otimes \mathrm{id} \otimes \varepsilon)$ à segunda obtemos

$$\begin{aligned} R &= (\mathrm{id} \otimes \mathrm{id} \otimes \varepsilon)(\mathrm{id} \otimes \Delta)(R) = (\mathrm{id} \otimes \mathrm{id} \otimes \varepsilon)(R_{13}R_{12}) \\ &= R \cdot (\mathrm{id} \otimes \varepsilon)(R). \end{aligned}$$

(c) Para mostrar este item, calculamos

$$\begin{aligned} R \cdot (S \otimes \mathrm{id})(R) &= (\mu \otimes \mathrm{id})(\mathrm{id} \otimes S \otimes \mathrm{id})(R_{13}R_{23}) \\ &= (\mu \otimes \mathrm{id})(\mathrm{id} \otimes S \otimes \mathrm{id})(\Delta \otimes \mathrm{id})(R) \\ &= (\mu(\mathrm{id} \otimes S)\Delta \otimes \mathrm{id})(R) \\ &= (\varepsilon \otimes \mathrm{id})(R) = 1, \end{aligned}$$

e

$$\begin{aligned} (\mathrm{id} \otimes S)(R^{-1}) \cdot R^{-1} &= (\mathrm{id} \otimes \mu)(\mathrm{id} \otimes S \otimes \mathrm{id})(R_{12}^{-1}R_{13}^{-1}) \\ &= (\mathrm{id} \otimes \mu)\, \mathrm{id} \otimes S \otimes \mathrm{id})(\mathrm{id} \otimes \Delta)(R^{-1}) \\ &= (\mathrm{id} \otimes \mu(S \otimes \mathrm{id})\Delta)(R^{-1}) \\ &= (\mathrm{id} \otimes \varepsilon)(R^{-1}) = 1, \end{aligned}$$

e isto conclui a prova.

■

R como uma aplicação

Suponhamos que H tenha dimensão finita (de modo que H^* tenha uma estrutura de coálgebra proveniente da estrutura de álgebra de H). Definimos uma aplicação $\mathfrak{R} : H^* \to H$ por

$$\mathfrak{R}(f) = \langle \mathrm{id} \otimes f, R \rangle .$$

Mais precisamente, se $R = \sum_{i=1}^{n} R_{1i} \otimes R_{2i}$, então $\mathfrak{R}(f) = \sum_{i=1}^{n} R_{1i} \langle f, R_{2i} \rangle = R^{(1)} f(R^{(2)})$.

Mostremos que as condições (4.3) equivalem a afirmar que a aplicação $\mathfrak{R}$ é um anti-homomorfismo de álgebras e um homomorfismo de coálgebras. De fato, se $f, g \in H^*$ temos

$$\begin{aligned}
\mathfrak{R}(fg) &= \langle \mathrm{id} \otimes fg, R \rangle \\
&= \langle \mathrm{id} \otimes f \otimes g, (\mathrm{id} \otimes \Delta(R) \rangle \\
&= \langle \mathrm{id} \otimes f \otimes g, R_{13} R_{12} \rangle \\
&= \langle \mathrm{id} \otimes g, R \rangle \langle \mathrm{id} \otimes f, R \rangle = \mathfrak{R}(g) \mathfrak{R}(f),
\end{aligned}$$

e

$$\mathfrak{R}(\varepsilon) = \langle \mathrm{id} \otimes \varepsilon, R \rangle = 1.$$

Por outro lado, temos

$$\begin{aligned}
\Delta \mathfrak{R}(f) &= \Delta \langle \mathrm{id} \otimes f, R \rangle = \langle \Delta \otimes f, R \rangle \\
&= \langle \mathrm{id} \otimes \mathrm{id} \otimes f, (\Delta \otimes \mathrm{id})(R) \rangle \\
&= \langle \mathrm{id} \otimes \mathrm{id} \otimes f, R_{13} R_{23} \rangle \\
&= \langle \mathrm{id} \otimes \mathrm{id} \otimes \Delta f, R_{13} R_{24} \rangle \\
&= R^{(1)} f_{(1)}(R^{(2)}) \otimes R^{(1)} f_{(2)} R^{(2)} \\
&= (\mathfrak{R} \otimes \mathfrak{R})(\Delta f),
\end{aligned}$$

donde $\Delta \mathfrak{R} = (\mathfrak{R} \otimes \mathfrak{R}) \Delta$, e também

$$\varepsilon \mathfrak{R}(f) = \varepsilon \langle \mathrm{id} \otimes f, R \rangle = \varepsilon(R^{(1)}) f(R^{(2)})$$

$$= \quad f(\varepsilon(R^{(1)})R^{(2)}) = f(1) = \varepsilon(f),$$

logo $\mathfrak{R}$ é um homomorfismo de coálgebras.

4.2 As Álgebras de Hopf $\breve{A}(R)$ e $\breve{U}(R)$

Na seção anterior, vimos que uma álgebra de Hopf satisfaz às Equações de Yang-Baxter Quânticas. Nesta seção, a cada solução matricial regular inversível da QYBE, vamos associar uma álgebra de Hopf essencialmente quasitriangular $\breve{U}(R)$ e uma álgebra de Hopf dual $\breve{A}(R)$.

4.2.1 As biálgebras $A(R)$ e $\tilde{U}(R)$

Seja $R \in M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ uma solução inversível da QYBE. Definimos $A(R)$ como a biálgebra não-comutativa gerada por 1 e pelos n^2 elementos do conjunto $\{u^i_j\}^n_{i,j=1}$, satisfazendo as relações

$$R(u \otimes 1)(1 \otimes u) = (1 \otimes u)(u \otimes 1)R. \tag{4.6}$$

$A(R)$ admite estrutura de coálgebra dada por

$$\Delta(u^i_j) = \sum_k u^i_k \otimes u^k_j, \qquad \varepsilon(u^i_j) = \delta^i_j.$$

Aqui, as n^2 incógnitas $\{u^i_j\}$ são vistas como uma matriz $u = (u^i_j) \in M_n(A(R))$ (com índice de linha i e de coluna j) e a equação (4.6) está definida em $M_n(A(R)) \otimes M_n(A(R))$. Quando $R = 1 \otimes 1$, a álgebra $A(R)$ se reduz à álgebra simétrica (cf. Exemplo 153 na pág. 166) sobre o módulo livre gerado por $\{u^i_j\}$.

Exemplo 114 (Matrizes Quânticas) Consideremos $n = 2$ e $q \in \mathbb{C} - \{0\}$, e tomemos

$$R = q^{-\frac{1}{2}} \begin{pmatrix} q & 0 & 0 & 0 \\ 0 & 1 & q - q^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & q \end{pmatrix}.$$

Então $A(R)$ é a álgebra $M_q(2,\mathbb{C})$ das matrizes quânticas. Esta corresponde à álgebra de endomorfismos do plano quântico $\mathbb{C}_q^{2|0}$ (cf. Majid [Ma, 2.1.5]). Podemos encontrar precisamente todas as $4^2 = 16$ relações que definem essa álgebra. Para isso, consideremos $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Escrevemos explicitamente os membros da equação (4.6):

$$R(u\otimes 1)(1\otimes u) \quad = \quad q^{-\frac{1}{2}} \begin{pmatrix} qa^2 & qab & qba & qb^2 \\ ac+(q-q^{-1})ca & ad+(q-q^{-1})cb & bc+(q-q^{-1})da & bd+(q-q^{-1})db \\ ca & cb & da & db \\ qc^2 & qcd & qdc & qd^2 \end{pmatrix},$$

$$(1\otimes u)(u\otimes 1)R \quad = \quad q^{-\frac{1}{2}} \begin{pmatrix} qa^2 & ba & (q-q^{-1})ba+ab & qb^2 \\ qca & da & (q-q^{-1})da+cb & qdb \\ qac & bc & (q-q^{-1})bc+ad & qbd \\ qc^2 & dc & (q-q^{-1})dc+cd & qd^2 \end{pmatrix}.$$

Igualando estas duas expressões e cancelando o fator comum $q^{-\frac{1}{2}}$, obtemos as relações

$$\begin{gathered} ac = q^{-1}ca, \qquad bd = q^{-1}db, \qquad ab = q^{-1}ba, \qquad cd = q^{-1}dc, \\ bc = cb, \qquad ad - da = (q^{-1}-q)bc. \end{gathered} \tag{4.7}$$

□

Exemplo 115 (Matrizes Quânticas Especiais) Se, além das relações (4.7), impusermos uma condição unitária sobre o *determinante quântico*

$$\det_q u \equiv ad - q^{-1}bc = 1 \tag{4.8}$$

obteremos a álgebra de Hopf $SL_q(2,\mathbb{C})$. Com efeito, em $M_q(2,\mathbb{C})$, verificamos que

$$\Delta(ad - q^{-1}bc) = (ad - q^{-1}bc) \otimes (ad - q^{-1}bc),$$

$$\varepsilon(ad - q^{-1}bc) = 1,$$

logo a relação (4.8) está consistente com as definições de Δ e ε em $SL_q(2,\mathbb{C})$, isto é, o elemento $ad - q^{-1}bc - 1$ gera um bi-ideal em $M_q(2,\mathbb{C})$. A aplicação antípoda $S : SL_q(2,\mathbb{C}) \to SL_q(2,\mathbb{C})$ é dada por

$$S(u) = \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix}.$$

Esta álgebra é dual à álgebra $U_q\mathfrak{sl}(2,\mathbb{C})$ do Exemplo 111 (cf. Rosso [Rs1]). □

As relações de $A(R)$ em termos da base

Seja $\{e^i_j\}^n_{i,j=1}$ a base usual de $M_n(\mathbb{C})$. Com relação a essa base, temos $R = \sum_{i,j,k,l} R^{ik}_{jl} e^i_j \otimes e^k_l$ e $u = \sum_{i,j} u^i_j e^i_j$. Agora, podemos reescrever os membros esquerdo e direito de (4.6) como

$$R(1 \otimes u)(u \otimes 1) = \sum_{i,j,k,l,p,q} R^{ik}_{pq} u^p_j u^q_l e^i_j \otimes e^k_l,$$

e

$$(u \otimes 1)(1 \otimes u)R = \sum_{i,j,k,l,p,q} u^k_q u^i_p R^{pq}_{jl} e^i_j \otimes e^k_l,$$

respectivamente. Igualando essas duas expressões, obtemos as n^4 relações escalares

$$\sum_{p,q} R^{ik}_{pq} u^p_j u^q_l = \sum_{p,q} u^k_q u^i_p R^{pq}_{jl}, \tag{4.9}$$

que são úteis para se realizar cálculos explícitos.

4.2.2 Representação fundamental de $A(R)$ e a biálgebra $\tilde{U}(R)$

Consideremos a aplicação $\rho^+ : A(R) \to M_n(\mathbb{C})$, definida por $\rho^+(u^i_j)^k_l = R^{ik}_{jl}$. Esta aplicação está bem definida e é chamada *representação fundamental* de $A(R)$. Com efeito, fixando em $M_n(\mathbb{C})$ a base usual $\{e^i_j\}^n_{i,j=1}$, temos $\rho^+(u^i_j) = \sum_{k,l} R^{ik}_{jl} e^k_l$. Agora, aplicando ρ^+ a ambos os lados de (4.9), obtemos

$$\rho^+(\sum_{a,b} R^{ik}_{ab} u^a_j u^b_l) \quad = \quad \sum_{a,b} R^{ik}_{ab} \rho^+(u^a_j)\rho^+(u^b_l)$$

$$= \sum_{a,b,p,q,s} R^{ik}_{ab} R^{ap}_{jq} R^{bq}_{ls} e^p_s$$

e

$$\begin{aligned}
\rho^+(\sum_{p,q} u^k_q u^i_p R^{pq}_{jl}) &= \sum_{p,q} \rho^+(u^k_q)\rho^+(u^i_p) R^{pq}_{jl} \\
&= \sum_{a,b,p,q,s} R^{kp}_{bq} R^{iq}_{as} R^{ab}_{jl} e^p_s.
\end{aligned}$$

Igualando estas duas expressões, resulta a QYBE

$$\sum_{a,b,q} R^{ik}_{ab} R^{ap}_{jq} R^{bq}_{ls} = \sum_{a,b,q} R^{kp}_{bq} R^{iq}_{as} R^{ab}_{jl}.$$

Isto quer dizer que a condição essencial de consistência para a boa definição de ρ^+ como um homomorfismo de álgebras equivale a que R seja uma solução da QYBE.

Analogamente, definimos a *representação fundamental conjugada* $\rho^- A(R) \to M_n(\mathbb{C})$ por $\rho^-(u^i_j)^k_l = (R^{-1})^{ik}_{jl}$, cuja consistência se resume em verificar que $R_{12}R^{-1}_{31}R^{-1}_{32} = R^{-1}_{32}R^{-1}_{31}R_{12}$, isto é, $R_{31}R_{32}R_{12} = R_{12}R_{32}R_{31}$, que é a QYBE após renomear as componentes de $M_n(\mathbb{C}) \otimes M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$.

De maneira semelhante a $A(R)$, definimos a álgebra $\tilde{U}(R)$. Esta é uma biálgebra não-comutativa gerada por 1 e pelas $2n^2$ indeterminadas $l^+ = (l^{+\,i}_j)$ e $l^- = (l^{-\,i}_j)$, módulo as relações

$$\begin{aligned}
R(1 \otimes l^\pm)(l^\pm \otimes 1) &= (l^\pm \otimes 1)(1 \otimes l^\pm)R, \\
R(1 \otimes l^+)(l^- \otimes 1) &= (l^- \otimes 1)(1 \otimes l^+)R.
\end{aligned}$$

A estrutura de coálgebra de $\tilde{U}(R)$ é dada pelas aplicações

$$\Delta(l^{\pm\,i}_j) = l^{\pm\,i}_k \otimes l^{\pm\,k}_j, \qquad \varepsilon(l^{\pm\,i}_j) = \delta^i_j$$

estendidas como homomorfismos de álgebras.

Há um *emparelhamento* entre as álgebras $A(R)$ e $\tilde{U}(R)$, isto é, uma aplicação bilinear

$A(R) \times \tilde{U}(R) \to F$ definida por

$$\langle u, l^{\pm} \rangle = R^{\pm},$$

onde $R^+ = R$ e $R^- = \tau(R^{-1})$. Em termos dos geradores, temos

$$\left\langle u^i_j, l^{\pm\,k}_{l} \right\rangle = R^{\pm\,ik}_{jl}.$$

Este emparelhamento deve ser estendido adequadamente a toda $A(R) \times \tilde{U}(R)$, i.é, para cada $x \in A(R)$ e $y \in \tilde{U}(R)$ fixados, as aplicações $y\,' \mapsto \langle x, y' \rangle$ e $x\,' \mapsto \langle x', y \rangle$ são homomorfismos de álgebras. Um cálculo direto (porém trabalhoso) permite verificar que este emparelhamento está bem definido, isto é, está compatível com as relações que definem $A(R)$ e $\tilde{U}(R)$.

Além disso, as equações definidas em (3.2.2) estabelecem uma relação entre a comultiplicação e counidade de uma destas álgebras com o produto e a unidade da outra. De fato, a aplicação $u \mapsto \langle u, l^+ \rangle$ é exatamente a representação fundamental de $A(R)$, i.é $\left\langle u^i_j, l^{+\,k}_{l} \right\rangle = \rho^+(u^i_j)^k_l = R^{jk}_{il}$, logo

$$\left\langle u^i_j u^k_l, l^{+\,m}_{n} \right\rangle = \sum_p \langle u^i_j, l^{+\,m}_{p} \rangle \left\langle u^k_l, l^{+\,p}_{n} \right\rangle = \left\langle u^i_j \otimes u^k_l, \Delta l^{+\,m}_{n} \right\rangle.$$

Por outro lado, isso nos fornece também a representação fundamental de $\tilde{U}(R)$, a saber, $l^{\pm} \mapsto \langle u, l^{\pm} \rangle$. A boa definição desta representação segue analogamente à de $A(R)$, mas é preciso verificar também, que

$$\left\langle u, \sum_{m,n} l^{-\,i}_{m} l^{+\,k}_{n} R^{mn}_{jl} \right\rangle = \left\langle u, \sum_{m,n} R^{ik}_{mn} l^{+\,n}_{l} l^{-\,m}_{j} \right\rangle,$$

a qual é válida, pois equivale a $R_{12}^{-1} R_{23} R_{13} = R_{13} R_{23} R_{12}^{-1}$, isto é, novamente a QYBE.

Então, as biálgebras $A(R)$ e $\tilde{U}(R)$ definem as representações fundamentais uma em relação a outra, o que é expresso na forma de um emparelhamento. Porém, esse emparelhamento é degenerado, significando que as representações fundamentais *não* são fiéis. De fato, se R for uma solução unitária da QYBE, i.é, $R^+ = R^-$, então $\langle u, l^+ - l^- \rangle = R^+ - R^- = 0$.

A seguir, partindo de $A(R)$ e $\tilde{U}(R)$, vamos construir as álgebras $\breve{A}(R)$ e $\breve{U}(R)$ cujo emparelhamento será não-degenerado.

4.2.3 As álgebras de Hopf $\breve{A}(R)$ e $\breve{U}(R)$

O emparelhamento degenerado entre $A(R)$ e $\tilde{U}(R)$ nos fornece dois radicais (ou núcleos), não-nulos em geral, K_1 e K_2 definidos por

$$\begin{aligned} K_1 &= \left\{x \in A(R) : \langle x, y\rangle = 0,\ \forall y \in \tilde{U}(R)\right\}, \\ K_2 &= \left\{y \in \tilde{U}(R) : \langle x, y\rangle = 0,\ \forall x \in A(R)\right\}. \end{aligned}$$

Estes são claramente bi-ideais (como núcleos de homomorfismos) de $A(R)$ e $\tilde{U}(R)$, e podemos formar as biálgebras quocientes $A(R)/K_1$ e $\tilde{U}(R)/K_2$, obtendo respectivamente as biálgebras $\breve{A}(R)$ e $\breve{U}(R)$. Temos assim, um emparelhamento induzido entre $\breve{A}(R)$ e $\breve{U}(R)$, o qual agora torna-se não-degenerado. Neste sentido, podemos dizer que $\breve{A}(R)$ e $\breve{U}(R)$ são essencialmente duais uma em relação à outra (cf. Majid [Ma, 3.2.1]), i.é, existem as inclusões $\breve{A}(R) \hookrightarrow \breve{U}(R)^*$ e $\breve{U}(R) \hookrightarrow \breve{A}(R)^*$. O termo "essencialmente dual" se deve a que $\breve{U}(R)^*$ é tecnicamente maior que $A(R)$, logo tais inclusões não são sobrejetoras em geral.

$\breve{A}(R)$ e $\breve{U}(R)$ são álgebras de Hopf, com antípodas definidas respectivamente por

$$\langle Su, l^+\rangle = \langle u, Sl^+\rangle = R^{-1}, \qquad \langle Su, l^-\rangle = \langle u, Sl^-\rangle = \tau(R),$$

e estendidas como anti-homomorfismos de álgebras. Com efeito, temos

$$\begin{aligned} \left\langle u^a_b, \sum_k (Sl^{+\,i}_{k}) l^{+\,k}_{j} \right\rangle &= \sum_k \left\langle u^a_p, Sl^{+\,i}_{k}\right\rangle \left\langle u^p_b, l^{+\,k}_{j}\right\rangle \\ &= \sum_k R^{-1\,ai}_{pk} R^{pk}_{bj} = \delta^a_b \delta^i_j = \langle u^a_b, 1\rangle\, \varepsilon(l^{+\,i}_{j}), \end{aligned}$$

e similarmente para outros produtos dos u's e $l^{\pm}$'s.

A biálgebra $\breve{U}(R)$ é essencialmente quasitriangular com a aplicação $\mathfrak{R} : \breve{A}(R) \to \breve{U}(R)$ definida por $u \mapsto l^+$ estendida a $\breve{A}(R)$ como anti-homomorfismo de álgebras e homomorfismo de coálgebras. Esta está bem-definida, i.é, verifica os axiomas que definem $\breve{A}(R)$ e $\breve{U}(R)$, e satisfaz as condições (4.3) e (4.4) (cf. Majid [Ma, 3.2.3]). Por exemplo, verificamos (4.4):

$$\begin{aligned}
\langle \Delta' h \cdot \mathfrak{R}, a\rangle &= \langle \Delta' h \otimes \mathfrak{R}, \Delta a\rangle \\
&= \left\langle \Delta' h, a_{(1)}\right\rangle \mathfrak{R}(a_{(2)}) \\
&= \left\langle a_{(1)}, h_{(1)}\right\rangle h_{(2)}\mathfrak{R}(a_{(2)}) \\
&\overset{(*)}{=} \mathfrak{R}(a_{(1)})h_{(1)} \left\langle a_{(2)}, h_{(2)}\right\rangle \\
&= \langle \mathfrak{R} \otimes \Delta h, \Delta a\rangle = \langle \mathfrak{R} \cdot \Delta h, a\rangle ,
\end{aligned}$$

para todo $a \in \check{A}(R)$ e todo $h \in \check{U}(R)$. A igualdade $(*)$ se escreve em termos da base como

$$\sum_{m,n} \left\langle u^i_m, l^{\pm\, k}_n \right\rangle l^{\pm\, n}_l l^{+\, m}_j = \sum_{m,n} l^{+\, i}_m l^{\pm\, k}_n \left\langle u^m_j, l^{\pm\, n}_l \right\rangle ,$$

i.é, $R^{\pm}(1 \otimes l^{\pm})(l^{+} \otimes 1) = (l^{+} \otimes 1)(1 \otimes l^{\pm})R^{\pm}$, que é uma das relações definindo $\check{U}(R)$. Portanto, temos $\Delta' h \cdot \mathfrak{R} = \mathfrak{R} \cdot \Delta h$.

4.2.4 Famílias clássicas de Grupos Quânticos

Anteriormente construímos as álgebras de Hopf $\check{A}(R)$ e $\check{U}(R)$ inteiramente a partir das constantes de estrutura em R. Esta maneira abstrata de se construir álgebras de Hopf encontra-se em analogia direta com a maneira de se construir álgebras de Lie a partir das constantes de estrutura c^i_{jk}, tais que $[x_j x_k] = c^i_{jk} x_i$ (cf. [Hu, §1.4] e [FRT]). O análogo da restrição imposta pela Identidade de Jacobi é a QYBE. Nos seguintes exemplos, R depende de um parâmetro q, tal que, quando $q \mapsto 1$, a álgebra de Hopf $\check{A}(R)$ torna-se a álgebra de funções contínuas sobre um grupo clássico. Por essa razão, tais exemplos são conhecidos como *Grupos Quânticos Clássicos*. Estes serão grupos matriciais em $M_n(\mathbb{C})$.

Por conveniência, vamos escrever $n = 2s + 1$, onde $s \in \frac{1}{2}\mathbb{Z}_+$ e tomamos a base canônica de $M_n(\mathbb{C})$, i.é, o conjunto

$$\{e_{ij} : i, j = -s, -s + 1, \ldots , s\} ,$$

onde e_{ij} é a matriz que contém 1 na posição (i, j) e zero nas demais posições. Também, vamos precisar definir

$$\bar{i} = \begin{cases} i - 1/2, & i > 0 \\ i, & i = 0 \\ i + 1/2, & i < 0. \end{cases}$$

Visto isso, passamos a descrever três exemplos abaixo.

Exemplo 116 A_{2s} quântico, ou $SU_q(n)$.

$$R = q^{-\frac{1}{n}} \left(q \sum_{i=-s}^{s} e_{ii} \otimes e_{ii} + \sum_{i \neq j} e_{ii} \otimes e_{jj} + (q - q^{-1}) \sum_{j>i} e_{ij} \otimes e_{ji} \right)$$

□

Exemplo 117 $B_s, D_{s+1/2}$ quântico, ou $SO_q(n)$.

$$\begin{aligned} R &= q \sum_{i \neq 0} e_{ii} \otimes e_{ii} + e_{00} \otimes e_{00} + q^{-1} \sum_{i \neq 0} e_{-i,-i} \otimes e_{ii} + \sum_{i \neq j,-j} e_{ii} \otimes e_{jj} \\ &\quad + (q - q^{-1}) \sum_{j>i} e_{ij} \otimes e_{ji} - (q - q^{-1}) \sum_{j>i} q^{\bar{j} - \bar{i}} e_{ij} \otimes e_{-i-j}, \end{aligned}$$

onde o termo $e_{00} \otimes e_{00}$ existe somente quando s for inteiro, i.é, n for ímpar. □

Exemplo 118 $C_{s+1/2}$ quântico, ou $Sp_q(n)$.

$$\begin{aligned} R &= q \sum_{i=-s}^{s} e_{ii} \otimes e_{ii} + q^{-1} \sum_{i=-s}^{s} e_{-i,-i} \otimes e_{ii} + \sum_{i \neq j,-j} e_{ii} \otimes e_{jj} + (q - q^{-1}) \sum_{j>i} e_{ij} \otimes e_{ji} \\ &\quad - (q - q^{-1}) \sum_{j>i} q^{\bar{j} - \bar{i}} q^{\operatorname{sgn}(j) - \operatorname{sgn}(i)} \operatorname{sgn}(j) \operatorname{sgn}(i) e_{ij} \otimes e_{-i,-j}, \end{aligned}$$

onde $\operatorname{sgn}(i) = \pm 1$, se $i > 0$ ou $i < 0$, respectivamente. □

Os grupos quânticos associados às álgebras de Lie clássicas são usualmente dados em termos de deformações da estrutura de suas respectivas álgebras universais envolventes, como no exemplo (111). Porém, tais grupos quânticos também podem ser dados na forma dual, correspondendo a $\breve{A}(R)$ e sua dual $\breve{U}(R)$. Vamos ilustrar isto na seguinte subseção para $\mathfrak{sl}(2, \mathbb{C})$, i.é, vamos verificar que, para uma solução matricial conveniente R da QYBE, obtemos $\check{A}(R) = SL_q(2, \mathbb{C})$ e $\check{U}(R) = U_q\mathfrak{sl}(2, \mathbb{C})$.

4.2.5 Os grupos quânticos $SL_q(2, \mathbb{C})$ e $U_q\mathfrak{sl}(2, \mathbb{C})$

Consideremos novamente a matriz

$$R = q^{-\frac{1}{2}} \begin{pmatrix} q & 0 & 0 & 0 \\ 0 & 1 & q - q^{-1} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & q \end{pmatrix}$$

em $M_4(\mathbb{C})$. Esta foi obtida do Exemplo 116, com $s = \frac{1}{2}$ e $n = 2$. Podemos verificar que esta R satisfaz a QYBE e que sua inversa é

$$R^{-1} = q^{\frac{1}{2}} \begin{pmatrix} q^{-1} & 0 & 0 & 0 \\ 0 & 1 & q^{-1} - q & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & q^{-1} \end{pmatrix}.$$

Assim, fazem sentido as álgebras $A(R)$ e $\tilde{U}(R)$ construídas acima. A álgebra $A(R)$ vem a ser exatamente álgebra das matrizes quânticas do Exemplo 114, de onde obtemos as relações

$$u_1^1 u_1^2 = q^{-1} u_1^2 u_1^1, \qquad u_2^1 u_2^2 = q^{-1} u_2^2 u_2^1, \qquad u_1^1 u_2^1 = q^{-1} u_2^1 u_1^1, \qquad u_1^2 u_2^2 = q^{-1} u_2^2 u_1^2,$$
$$u_2^1 u_1^2 = u_1^2 u_2^1, \qquad u_1^1 u_2^2 - u_2^2 u_1^1 = (q^{-1} - q) u_2^1 u_1^2.$$

Vamos verificar que as relações

$$l_2^{+\,1} = 0 = l_1^{-\,2}, \quad l_1^{+\,1} l_1^{-\,1} = 1, \quad l_2^{+\,2} l_2^{-\,2} = 1, \quad \det l^+ = 1, \tag{4.10}$$

definem um bi-ideal em $\tilde{U}(R)$ e que a relação

$$\det_q u = u_1^1 u_2^2 - q^{-1} u_2^1 u_1^2 = 1,$$

define um bi-ideal em $A(R)$.

Primeiramente, observamos (cf. Sweedler [Sw, pág. 88]) que se J é um ideal gerado por um subespaço vetorial V de uma biálgebra H tal que $\Delta V \subseteq J \otimes H + H \otimes J$, então $\Delta J \subseteq J \otimes H + H \otimes J$, ou seja, J é um bi-ideal. Como conseqüência, para as relações acima, basta-nos verificar a propriedade de coideal sobre os geradores. Assim procedendo, usamos as representações fundamentais para expressar as igualdades

$$\begin{aligned}\left\langle u_1^1 u_2^2 - q^{-1} u_2^1 u_1^2, l_j^{\pm\,i} \right\rangle &= \left\langle u_1^1 \otimes u_2^2 - q^{-1} u_2^1 \otimes u_1^2, \Delta l_j^{\pm\,i} \right\rangle \\ &= R_{11}^{\pm\,i1} R_{j2}^{\pm\,12} + R_{21}^{\pm\,i1} R_{j2}^{\pm\,22} - q^{-1} \left(R_{12}^{\pm\,i1} R_{j1}^{\pm\,12} + R_{22}^{\pm\,i1} R_{j1}^{\pm\,22} \right) \\ &= \delta_j^i = \left\langle 1, l_j^{\pm\,i} \right\rangle,\end{aligned}$$

$$\begin{aligned}\Delta(u_1^1 u_2^2 - q^{-1} u_2^1 u_1^2) &= (u_j^1 \otimes u_1^j)(u_k^2 \otimes u_2^k) - q^{-1}(u_l^1 \otimes u_2^l)(u_m^2 \otimes u_1^m) \\ &= (u_1^1 u_2^2 - q^{-1} u_2^1 u_1^2) \otimes (u_1^1 u_2^2 - q^{-1} u_2^1 u_1^2).\end{aligned}$$

Logo, podemos consistentemente impor $\det_q u = 1$, obtendo a biálgebra quociente

$$\frac{A(R)}{\det_q u - 1} = SL_q(2, \mathbb{C}).$$

Voltando nossa atenção para $\tilde{U}(R)$, verificamos que

$$\left\langle u_j^i, l_2^{+\,1} \right\rangle = 0 = \left\langle u_j^i, l_1^{-\,2} \right\rangle,$$

$$\Delta l_2^{+\,1} = l_1^{+\,1} \otimes l_2^{+\,1} + l_2^{+\,1} \otimes l_2^{+\,2},$$

$$\left\langle u_j^i, l_1^{+\,1} l_1^{-\,1} \right\rangle = \left\langle \Delta u_j^i, l_1^{+\,1} \otimes l_1^{-\,1} \right\rangle = \delta_j^i = \left\langle u_j^i, 1 \right\rangle = \left\langle u_j^i, l_2^{+\,2} l_2^{-\,2} \right\rangle,$$

$$\Delta l_1^{-\,2} = l_1^{-\,2} \otimes l_1^{-\,1} + l_2^{-\,2} \otimes l_1^{-\,2},$$

$$\Delta l_1^{+\,1} l_1^{-\,1} = l_1^{+\,1} l_1^{-\,1} \otimes_1^{+\,1} l_1^{-\,1}$$

$$\left\langle u_j^i, \det l^+ \right\rangle = \left\langle \Delta u_j^i, l_1^{+\,1} \otimes_2^{+\,2} \right\rangle = \delta_j^i = \left\langle u_j^i, 1 \right\rangle,$$

$$\Delta \det l^+ = \det l^+ \otimes \det l^+,$$

donde as relações (4.10) definem um ideal em $\tilde{U}(R)$.

Fazendo as identificações

$$l^+ \equiv \begin{pmatrix} q^{\frac{H}{2}} & 0 \\ q^{-\frac{1}{2}}(q-q^{-1})X^+ & q^{-\frac{H}{2}} \end{pmatrix}, \quad l^- \equiv \begin{pmatrix} q^{-\frac{H}{2}} & q^{\frac{1}{2}}(q^{-1}-q)X^- \\ 0 & q^{\frac{H}{2}} \end{pmatrix},$$

e considerando as relações obtidas logo acima, juntamente com as relações provenientes da definição de $\tilde{U}(R)$, temos que, $R(1\otimes l^\pm)(l^\pm\otimes 1) = (l^\pm\otimes 1)(1\otimes l^\pm)R$ resulta em $q^{\frac{H}{2}}X^\pm q^{-\frac{H}{2}} = q^{\pm 1}X^\pm$, e $R(1\otimes l^+)(l^-\otimes 1) = (l^-\otimes 1)(1\otimes l^+)R$ resulta em $[X^+X^-] = \frac{q^H - q^{-H}}{q-q^{-1}}$ (em cada caso é preciso escrever todas as 16 relações, cuja maioria acaba sendo redundante).

Podemos ainda verificar que a aplicação antípoda S e a aplicação $\mathfrak{R}$ definidas acima coincidem com aquelas fornecidas nos Exemplos 111 e 115, logo, $\tilde{U}(R)$ módulo as relações (4.10) é isomorfo a $U_q\mathfrak{sl}(2,\mathbb{C})$.

Já sabemos que $U_q\mathfrak{sl}(2,\mathbb{C})$ e $SL_q(2,\mathbb{C})$ são duais, e que o emparelhamento entre $\breve{A}(R)$ e $\breve{U}(R)$ é não-degenerado. Portanto, os bi-ideais construídos devem ser radicais do emparelhamento e, conseqüentemente, $\breve{A}(R) = SL_q(2,\mathbb{C})$ e $\breve{U}(R) = U_q\mathfrak{sl}(2,\mathbb{C})$.

4.3 O análogo quântico $U_t\mathfrak{g}$ da álgebra universal envolvente $U\mathfrak{g}$ de uma álgebra de Lie simples $\mathfrak{g}$

Seja $\mathfrak{g}$ uma álgebra de Lie simples sobre $\mathbb{C}$, e seja $\mathfrak{h}$ uma subálgebra de Cartan de $\mathfrak{g}$ (i.é, uma subálgebra nilpotente que é igual ao seu normalizador em $\mathfrak{g}$). O conjunto das *raízes simples* $\{\alpha_i : i = 1,\ldots,N\}$ de $\mathfrak{g}$ geram o espaço vetorial $\mathfrak{h}^*$, o qual se identifica a $\mathfrak{h}$ mediante a forma de Killing κ de $\mathfrak{g}$ do seguinte modo: a cada $\varphi\in\mathfrak{h}^*$ corresponde o único elemento $t_\varphi\in\mathfrak{h}$ tal que $\varphi(h) = \kappa(t_\varphi, h)$, $\forall h\in\mathfrak{h}$. O conjunto $\{h_i : i = 1,\ldots,N\}$, onde $h_i = \frac{2t_{\alpha_i}}{\kappa(\alpha_i,\alpha_i)}$, é evidentemente uma base de $\mathfrak{h}$ e é chamado conjunto das *co-raízes simples* de $\mathfrak{g}$. A forma de Killing define um produto escalar invariante em $\mathfrak{h}$ (e também em $\mathfrak{h}^*$) tal que $(h_i,h_j) = \kappa(h_i,h_j) = (\alpha_i,\alpha_j)$. Como vimos, a matriz de Cartan $A = (a_{ij})$ de $\mathfrak{g}$ é não trivial (pois κ é não-degenerada em $\mathfrak{g}$) e seus elementos $a_{ij} = \langle h_i,\alpha_j\rangle = \frac{2(\alpha_j,\alpha_i)}{(\alpha_i,\alpha_i)} = \langle\alpha_j,\alpha_i\rangle$ são inteiros de Cartan. Aqui estamos adotando uma convenção um pouco diferente daquela em (2.6.5), onde a matriz de Cartan foi definida como sendo a transposta da matriz que apresentamos aqui. A álgebra universal envolvente $U\mathfrak{g}$

é a álgebra gerada por 1 e pelos elementos de $\mathfrak{g}$, módulo o ideal gerado por todos os elementos do tipo $xy - yx - [xy]$. Se $(x_1, \ldots, x_k)$ é uma base ordenada de $\mathfrak{g}$, o Teorema de PBW nos fornece uma base de $U\mathfrak{g}$, a saber, $\{1\} \cup \{x_{i_1} x_{i_2} \cdots x_{i_m} : m \in \mathbb{Z}^+, 1 \leq i_1 \leq i_2 \leq \cdots \leq i_m\}$. Esta é também conhecida como a *Base PBW* de $U\mathfrak{g}$ (cf. Corolário 85). Outro corolário desse teorema garante a injetividade da inclusão natural $\mathfrak{g} \hookrightarrow U\mathfrak{g}$ como álgebras de Lie.

Vamos agora, para $t \in \mathbb{C}$, considerar a álgebra $U_t\mathfrak{g}$ gerada por $\{k_i^{\pm 1}, e_i, f_i : i = 1, \ldots, N\}$ sobre $\mathbb{C}$ satisfazendo as relações:

(Q1) $k_i k_i^{-1} = k_i^{-1} k_i = 1, \qquad [k_i k_j] = 0,$

(Q2) $k_i e_j k_i^{-1} = t_i^{a_{ij}} e_j, \qquad k_i f_j k_i^{-1} = t_i^{-a_{ij}} f_j$

(Q3) $[e_i f_i] = \dfrac{k_i^2 - k_i^{-2}}{t_i^2 - t_i^{-2}}, \qquad [e_i f_j] = 0$, para $i \neq j$,

(Q4) $\displaystyle\sum_{l=0}^{1-a_{ij}} (-1)^l \begin{bmatrix} 1 - a_{ij} \\ l \end{bmatrix}_{t_i^2} e_i^{1-a_{ij}-l} e_j e_i^l = 0$, para $i \neq j$,

(Q5) $\displaystyle\sum_{l=0}^{1-a_{ij}} (-1)^l \begin{bmatrix} 1 - a_{ij} \\ l \end{bmatrix}_{t_i^2} f_i^{1-a_{ij}-l} f_j f_i^l = 0$, para $i \neq j$.

Nestas relações, temos $t_i = t^{\frac{(\alpha_i, \alpha_j)}{2}}$, $[m]_t = \dfrac{t^m - t^{-m}}{t - t^{-1}}$, e

$$\begin{bmatrix} m \\ n \end{bmatrix}_t = \begin{cases} \dfrac{[m]_t [m-1]_t \cdots [m-n]_t}{[n]_t [n-1]_t \cdots [1]_t} = \dfrac{(t^m - t^{-m}) \cdots (t^{m-n+1} - t^{-m+n-1})}{(t - t^{-1}) \cdots (t^n - t^{-n})} \\ 1, \text{ se } n = 0 \text{ ou } m = n. \end{cases}$$

O símbolo $\begin{bmatrix} m \\ n \end{bmatrix}_t$ corresponde ao coeficiente *t-binomial*, o qual está relacionado ao *polinômio de Gauss*

$$\left[\!\left[\begin{matrix} m \\ n \end{matrix} \right]\!\right]_q = \frac{[\![m]\!]_q \, [\![m-1]\!]_q \cdots [\![m-n+1]\!]_q}{[\![n]\!]_q \, [\![n-1]\!]_q \cdots [\![1]\!]_q} = \frac{(1 - q^m)(1 - q^{m-1}) \cdots (1 - q^{m-n+1})}{(1 - q)(1 - q^2) \cdots (1 - q^n)}$$

pela equação

$$\begin{bmatrix} m \\ n \end{bmatrix}_t = \left[\!\left[\begin{matrix} m \\ n \end{matrix} \right]\!\right]_{t^2} t^{-n(m-n)}.$$

Este polinômio aparece na Teoria das Partições. Os números $[\![m]\!]_q$ são os *q-números inteiros* do Exemplo 111. Observamos ainda que $\left[\!\left[\begin{smallmatrix} m \\ n \end{smallmatrix} \right]\!\right]_1$ é simplesmente o coeficiente binomial usual $\binom{m}{n}$.

Para fins posteriores, é útil observar também que

$$t_i^{a_{ij}} = t^{\frac{2(\alpha_j,\alpha_i)}{(\alpha_i,\alpha_i)}\frac{(a_i,\alpha_i)}{2}} = t^{(\alpha_i,\alpha_j)} = t_j^{a_{ji}}.$$

A álgebra$U_t\mathfrak{g}$ é uma *deformação* de $U\mathfrak{g}$ com parâmetro t no sentido que $U_t\mathfrak{g} \to U\mathfrak{g}$ no limite formal $t \to 1$. Pode ser visto que (Q1)-(Q5) adquirem, neste limite, a forma das relações de comutação usuais definindo a álgebra de Lie $\mathfrak{g}$ (a extensão de (2.1) para o caso $\mathfrak{sl}(2, F)$). Para ver isso, fazemos $k_i = t_i^{h_i}$ e, quando $t \to 1$ formalmente, obtemos as seguintes relações de comutação entre os elementos h_i, e_i, f_i :

$(S1)$ $[h_i h_j] = 0$,

$(S2)$ $[e_i f_i] = \dfrac{t_i^{2h_i} - t_i^{-2h_i}}{t_i^2 - t_i^{-2}} \to h_i$, e $[e_i f_j] = 0$ se $i \neq j$,

$$\begin{aligned}
(S3) \quad [[e_i f_i]\, e_j] &= \frac{k_i^2 e_j - k_i^{-2} e_j - e_j k_i^2 + e_j k_i^{-2}}{t_i^2 - t_i^{-2}} \\
&= \frac{(1 - t_i^{-2a_{ij}}) t_i^{2h_i} + (t_i^{2a_{ij}} - 1) t_i^{-2h_i}}{t_i^2 - t_i^{-2}} e_j \to a_{ij} e_j = \langle \alpha_j, \alpha_i \rangle\, e_j, \\
[[e_i f_i]\, f_j] &= \frac{(1 - t_i^{2a_{ij}}) t_i^{2h_i} + (t_i^{-2a_{ij}} - 1) t_i^{-2h_i}}{t_i^2 - t_i^{-2}} \to -a_{ij} f_j = - \langle \alpha_j, \alpha_i \rangle\, f_j,
\end{aligned}$$

(S_{ij}^+) $(\operatorname{ad} e_i)^{-\langle \alpha_j, \alpha_i \rangle + 1}(e_j) = 0$,

(S_{ij}^-) $(\operatorname{ad} f_i)^{-\langle \alpha_j, \alpha_i \rangle + 1}(f_j) = 0$,

as quais definem abstratamente a álgebra de Lie $\mathfrak{g}$ (mais geralmente, admite-se que A seja uma matriz de Cartan generalizada, de modo que estas relações definem na verdade a álgebra de Kac-Moody $\mathfrak{g}(A)$ (cf. Apêndice de Chari & Pressley [CP])). Asduas últimas condições aparecem como os limites de (Q4) e (Q5) respectivamente, bastando observar, por simples indução e uso da regra de Leibniz, que

$$\begin{aligned}
(\operatorname{ad} e_i)^{1-a_{ij}}(e_j) &= \sum_{l=0}^{1-a_{ij}} (-1)^l \binom{1-a_{ij}}{l} e_i^{1-a_{ij}-l} e_j e_i^l, \\
(\operatorname{ad} f_i)^{1-a_{ij}}(f_j) &= \sum_{l=0}^{1-a_{ij}} (-1)^l \binom{1-a_{ij}}{l} f_i^{1-a_{ij}-l} f_j f_i^l.
\end{aligned}$$

Ademais, $U_t\mathfrak{g}$ admite estrutura de coálgebra com comultiplicação $\Delta : U_t\mathfrak{g} \to U_t\mathfrak{g} \otimes U_t\mathfrak{g}$ tal que

$$\begin{aligned}
\Delta(k_i^{\pm 1}) &= k_i^{\pm 1} \otimes k_i^{\pm 1}, \\
\Delta(e_i) &= e_i \otimes k_i^{-1} + k_i \otimes e_i, \\
\Delta(f_i) &= f_i \otimes k_i^{-1} + k_i \otimes f_i,
\end{aligned}$$

e counidade $\varepsilon : U_t\mathfrak{g} \to \mathbb{C}$ definida por

$$\varepsilon(\kappa_i^{\pm 1}) = 1, \qquad \varepsilon(e_i) = 0 = \varepsilon(f_i).$$

Estas aplicações estão definidas sobre os geradores e estendidas a toda a álgebra $U_t\mathfrak{g}$ como homomorfismos de álgebras. Pode ser mostrado (cf. Chari & Pressley[CP, 6.3]) que o modo como Δ e ε estão definidas é único, com a condição de satisfazer as propriedades de coassociatividade e counidade, respectivamente. Para ilustrar, verificamos a coassociatividade de Δ sobre os elementos e_i:

$$\begin{aligned}
(\Delta \otimes \mathrm{id})\Delta(e_i) &= (\Delta \otimes \mathrm{id})(e_i \otimes k_i^{-1} + k_i \otimes e_i) \\
&= e_i \otimes k_i^{-1} \otimes k_i^{-1} + k_i \otimes e_i \otimes k_i^{-1} + k_i \otimes k_i \otimes e_i \\
&= (\mathrm{id} \otimes \Delta)(e_i \otimes k_i^{-1} + k_i \otimes e_i) \\
&= (\mathrm{id} \otimes \Delta)\Delta(e_i).
\end{aligned}$$

A verificação da coassociatividade de Δ sobre os f_i's é análoga, e sobre os $k_i^{\pm 1}$'s é trivial. Além disso, $U_t\mathfrak{g}$ é uma álgebra de Hopf com aplicação antípoda $S : U_t\mathfrak{g} \to U_t\mathfrak{g}$ definida por

$$S(k_i) = k_i^{-1}, \qquad S(e_i) = -t_i^{-2} e_i, \qquad S(f_i) = -t_i^2 f_i.$$

De fato,

$$\begin{aligned}
\mu(\mathrm{id} \otimes S)\Delta(e_i) &= e_i S(k_i^{-1}) + k_i S(e_i) \\
&= e_i k_i - t_i^2 k_i e_i \\
&= e_i k_i - e_i k_i = 0 = \varepsilon(e_i)
\end{aligned}$$

$$= \quad \mu(S \otimes \mathrm{id})\Delta(e_i),$$

e analogamente para os f_i's e para os k_i's.

4.3.1 Sobre a estrutura de $U_t\mathfrak{g}$ quando t não é raiz da unidade

Daqui por diante, assumimos que t *não* é raiz da unidade. Seja $Q = \bigoplus_{i=1}^{N} \mathbb{Z}\alpha_i$ o reticulado das raízes de $\mathfrak{g}$ e seja $Q_+ = \bigoplus_{i=1}^{N} \mathbb{N}\alpha_i$. O objetivo principal desta subseção é mostrar que $U_t\mathfrak{g}$ é uma álgebra Q-graduada e, usando esse fato, mostrar que $U_t\mathfrak{g}$ tem uma base que desempenha um papel análogo à PBW de $U\mathfrak{g}$. Para isso, vamos precisar das seguintes notações: definimos as subálgebras $U_t\mathfrak{n}_+$ (respec. $U_t\mathfrak{n}_-$) gerada pelos e_i's (respec. f_i's) e $U_t\mathfrak{b}_+$ (respec. $U_t\mathfrak{b}_-$) gerada pelos k_i's e pelos e_i's (respec. k_i's e f_i's) de $U_t\mathfrak{g}$. Ainda, seja T o subgrupo multiplicativo de $U_t\mathfrak{g}$ formado pelos elementos inversíveis de $U_t\mathfrak{g}$ gerados pelos k_i's, e seja $\mathbb{C}[T]$ sua álgebra de grupo. Em particular, vamos mostrar que vale a decomposição triangular $U_t\mathfrak{g} \cong U_t\mathfrak{n}_- \otimes \mathbb{C}[T] \otimes U_t\mathfrak{n}_+$ (observamos a semelhança desta decomposição com o conhecido resultado para as álgebras envolventes: $U(\mathfrak{g}_1 \oplus \mathfrak{g}_2) \cong U\mathfrak{g}_1 \otimes U\mathfrak{g}_2$).

Q-graduação

Dizemos que um monômio x nos geradores e_i, f_i, k_i, é de grau $\alpha = \sum_{i=1}^{N} n_i\alpha_i \in Q$, e denotamos $\mathrm{gr}\, x = \alpha$, se

$$k_i x k_i^{-1} = t^{(\alpha_i,\alpha)}, \quad \forall i = 1, \ldots, N.$$

Proposição 119 *A ação dos k_i's por conjugação produz uma Q-graduação em $U_t\mathfrak{g}$ (respec. em $U_t\mathfrak{n}_\pm$ e $U_t\mathfrak{b}_\pm$).*

Prova. Como t não é raiz da unidade e $(\alpha_i, \alpha) \in \mathbb{Z}$, os números $t^{(\alpha_i,\alpha)} \in \mathbb{C}$ determinam unicamente os inteiros (α_i, α), os quais, por sua vez, determinam α (i.é, seus coeficientes $n_1, \ldots, n_N$) unicamente, já que o produto escalar $(\, , \,)$ é não-degenerado. Observando ainda que $k_i e_j^{n_j} k_i^{-1} = (k_i e_j k_i^{-1})^{n_j} = (t_i^{a_{ij}} e_j)^{n_j} = t_i^{n_j a_{ij}} e_j^{n_j} = t^{n_j(\alpha_i,\alpha_j)} e_j^{n_j}$, e $k_i f_j^{m_j} k_i^{-1} = t^{-m_j(\alpha_i,\alpha_j)} f_j^{m_j}$, vemos que se x é um monômio em que e_j aparece n_j vezes e f_j aparece m_j vezes, então $\mathrm{gr}\, x = \sum_{j=1}^{N}(n_j - m_j)\alpha_j = \sum_{j=1}^{N}(\mathrm{gr}\, e_j^{n_j} + \mathrm{gr}\, f_j^{m_j})$ (os k_i's não precisam ser considerados aqui pois têm grau 0). Conseqüentemente, $U_t\mathfrak{g}$ é soma direta de seus espaços de graus

$$U_\alpha = \{x \in U_t\mathfrak{g} : \operatorname{gr} x = \alpha\}.$$

■

Com isto, $(U_t\mathfrak{g})^{\otimes m}$ é Q^m-graduada, e também Q-graduada pela graduação total. Observamos que a comultiplicação Δ é claramente um homormorfismo de álgebras graduadas. De fato,

$$\begin{aligned}(k_i \otimes k_i)\Delta(e_j)(k_i^{-1} \otimes k_i^{-1}) &= (k_i e_j k_i^{-1}) \otimes k_j^{-1} + k_j \otimes (k_i e_j k_i^{-1}) \\ &= t^{(\alpha_i,\alpha_j)}\Delta(e_j),\end{aligned}$$

para todo $i = 1, \ldots, N$, i.é, o $\operatorname{gr}\Delta(e_j) = \operatorname{gr} e_j = \alpha_j$. Similarmente, concluímos que $\operatorname{gr}\Delta(f_j) = \operatorname{gr} f_j = -\alpha_j$ e que $\operatorname{gr}\Delta(k_j) = \operatorname{gr} k_j = 0$.

Lema 120 *$\forall m_1, \ldots, m_N \in \mathbb{N}$, $e_1^{m_1} \cdots e_N^{m_N}$ é não-nulo em $U_t\mathfrak{g}$.*

Prova. a) Existe sempre a representação fundamental de $U_t\mathfrak{g}$ dada pelas mesmas fórmulas da representação fundamental de $\mathfrak{g}$, na qual os e_i's têm imagem não-nula (cf. Jimbo [Ji2, Remark 1]; isto também pode ser visto seguindo-se Humphreys [Hu, §18.2]).

b) $\forall i = 1, \ldots, N$, $\forall m \in \mathbb{N}$, $e_i^m \neq 0$. Como Δ e também $\Delta^m = (\Delta \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id})\Delta^{m-1}$ são injetoras, basta mostrar que $\Delta^m(e_i^m) \neq 0$. Usando a Q^m-graduação, basta mostrar que a componente de grau $(\alpha_i, \ldots, \alpha_i)$ é não-nula. Assim, temos $\Delta^m(e_i) = u_1 + \cdots + u_m$, onde

$$u_r = k_i \otimes \cdots \otimes k_i \otimes e_i \otimes k_i^{-1} \otimes \cdots \otimes k_i^{-1}$$

i.é, o e_i está na posição r do produto tensorial, e se $r < s$, então

$$\begin{aligned}u_r u_s &= k_i^2 \otimes \cdots \otimes k_i^2 \otimes e_i k_i \otimes 1 \otimes \cdots \otimes 1 \otimes k_i^{-1} e_i \otimes k_i^{-2} \otimes \cdots \otimes k_i^{-2} \\ &= k_i^2 \otimes \cdots \otimes k_i^2 \otimes t_i^2 k_i e_i \otimes 1 \otimes \cdots \otimes 1 \otimes t_i^2 e_i k_i^{-1} \otimes k_i^{-2} \otimes \cdots \otimes k_i^{-2} \\ &= t_i^4 u_s u_r.\end{aligned}$$

Para encontrar explicitamente $\Delta^m(e_i^m)$, utilizamos a fórmula t_i^4-*multinomial*:

$$\begin{aligned}(\Delta^m(e_i))^m &= (u_1+\cdots+u_m)^m \\ &= \sum_{n_1+\cdots+n_m=m} \frac{[\![m]\!]_{t_i^4}!}{[\![n_1]\!]_{t_i^4}!\cdots[\![n_m]\!]_{t_i^4}!} u_1^{n_1}\cdots u_m^{n_m}.\end{aligned}$$

Um cálculo direto mostra que o grau de um termo deste multinomial é $(n_1\alpha_i,\ldots,n_m\alpha_i)$, de modo que, encontramos o termo de grau $(\alpha_i,\ldots,\alpha_i)$ quando $n_1=\cdots=n_m=1$, ou seja, o termo

$$\frac{[\![m]\!]_{t_i^4}!}{([\![1]\!]_{t_i^4})^m} u_1\cdots u_m =$$

$$= \frac{(t_i^2-t_i^{-2})(t_i^4-t_i^{-4})\cdots(t_i^{2m}-t_i^{-2m})}{(t_i^2-t_i^{-2})^m} e_ik_i^{m-1}\otimes e_ik_i^{m-3}\otimes\cdots\otimes e_ik_i^{-(m-1)}.$$

Este é claramente não-nulo, pois os k_i são inversíveis.

c) Sejam $m_1,\ldots,m_N\in\mathbb{N}$. Para mostrar que $e_1^{m_1}\cdots e_N^{m_N}\neq 0$, basta mostrar que a componente de grau $(m_1\alpha_1,\ldots,m_N\alpha_N)$ de $\Delta^N(e_1^{m_1}\cdots e_N^{m_N})$ é não-nula. Mas esta é

$$e_1^{m_1}k_2^{m_2}\cdots k_N^{m_N}\otimes k_1^{-m_1}e_2^{m_2}\cdots k_N^{m_N}\otimes\cdots\otimes k_1^{-m_1}\cdots k_{N-1}^{-m_{N-1}}e_N^{m_N}$$

a qual é não-nula por (b). ∎

Uma base para $\mathbb{C}[T]$

Para cada $\alpha=\sum_{i=1}^N n_i\alpha_i\in Q$, consideremos o monômio $k_\alpha=k_1^{n_1}\cdots k_N^{n_N}$. Estes claramente geram $\mathbb{C}[T]$. Mais pode ser dito. De fato, temos os seguinte lema.

Lema 121 *Os k_α's, $\alpha\in Q$, são linearmente independentes.*

Prova. Suponha que $\sum_{\text{fin.}}\lambda_\alpha k_\alpha=0$, onde $\lambda_\alpha\in\mathbb{C}-\{0\}$. Sem perda de generalidade, podemos assumir que os α que aparecem na soma estejam todos em Q_+. Assim, $(\mathrm{id}\otimes S)\Delta(\sum\lambda_\alpha k_\alpha)=\sum\lambda_\alpha k_\alpha\otimes k_\alpha^{-1}=0$ em $U_t(L)\otimes U_t(L)$. Seja $L: U_t\mathfrak{g}\to U_t\mathfrak{g}$ a representação regular à esquerda (definida por $L(x)(y)=xy$) e seja $R: U_t\mathfrak{g}\to U_t\mathfrak{g}$ a representação regular à direita (definida por $R(x)(y)=yx$). Devemos ter então $\sum\lambda_\alpha L(k_\alpha)\circ R(k_\alpha^{-1})=0$ em $\mathrm{End}(U_t\mathfrak{g})$. Aplicando esta sobre $e_1^{m_1} \cdots e_N^{m_N}$, obtemos

$$\sum \lambda_\alpha t^{(\alpha, \sum m_i \alpha_i)} = 0, \qquad \forall m_1, \ldots, m_N \in \mathbb{N}.$$

Como podemos aplicar $\sum \lambda_\alpha L(k_\alpha) \circ R(k_\alpha^{-1})$ sobre $e_1^{km_1} \cdots e_N^{km_N}$ para todo $k \in \mathbb{N}$, vemos de imediato que t e todas as suas potências t^k são raízes de um certo polinômio de Laurent. Mas t não é raiz da unidade, o que significa que todas as suas potências t^k são duas-a-duas distintas, de modo que esse polinômio de Laurent tem que ser nulo. Observando que a aplicação $\alpha \mapsto (\alpha, \sum m_i \alpha_i)$ não é necessariamente injetora, devemos agrupar os coeficientes nulos desse polinômio de Laurent, a saber,

$$\sum_{\alpha | (\alpha, \sum m_i \alpha_i) = \text{cte.}} \lambda_\alpha = 0, \qquad \forall m_1, \ldots, m_N \in \mathbb{N}.$$

Vamos concluir a prova usando indução sobre o número p de termos na soma original (lembrando que assumimos $\lambda_\alpha \in \mathbb{C} - \{0\}$). O caso $p = 1$ é óbvio. Agora, suponhamos que o resultado seja verdadeiro para todas as somas com $p \geq 1$ termos e suponhamos que seja dada uma soma com $p + 1$ termos nos índices $\alpha^{(0)}, \ldots, \alpha^{(p)} \in Q_+$. Basta mostrar que existem $m_1, \ldots, m_N \in \mathbb{N}$ tais que

$$(\alpha^{(0)}, \sum m_i \alpha_i) \notin \{(\alpha^{(k)}, \sum m_i \alpha_i) : k = 1, \ldots, p\}, \tag{4.11}$$

de modo que o argumento sobre os polinômios de Laurent nos dá $\lambda_{\alpha^{(0)}} = 0$. Ficamos assim novamente com uma soma de p termos cujos coeficientes são nulos pela hipótese de indução. Podemos refrasear (4.11) do seguinte modo:

$$\exists m_1, \ldots, m_N \in \mathbb{N}, \text{ tais que, } \forall k = 1, \ldots, p, \ \ (\alpha^{(0)} - \alpha^{(p)}, \sum m_i \alpha_i) \neq 0.$$

As aplicações $\alpha \mapsto (\alpha^{(0)} - \alpha^{(p)}, \alpha)$ são formas lineares não-nulas sobre $\mathfrak{h}^*$ as quais determinam p hiperplanos em $\mathfrak{h}^*$. Devemos mostrar que há ao menos um ponto em Q_+ que não está na reunião de todos esses hiperplanos. A prova desse fato é análoga à do caso clássico: qualquer espaço vetorial sobre um corpo de característica 0 não pode ser a reunião de uma quantidade finita de subespaços próprios (cf. Brown [Br, I, 1.14]). ∎

Uma base para $U_t\mathfrak{n}_\pm$

Há uma base em $U_t\mathfrak{n}_\pm$ cujos elementos são monômios nos e_i's (esta é gerada por tais monômios como espaço vetorial). Sem perda de generalidade, podemos assumir que os monômios básicos de um certo Q-grau formam uma base da respectiva Q-componente de $U_t\mathfrak{n}_\pm$. Seja $(E_r)_{r\in I}$ essa base.

Lema 122 *$(E_rk_\alpha)_{r\in I,\alpha\in Q}$ é uma base de $U_t\mathfrak{b}_+$. Portanto, $U_t\mathfrak{b}_+ \cong U_t\mathfrak{n}_+ \otimes \mathbb{C}[T]$ como espaços vetoriais.*

Prova. Basta mostrar que esses elementos são linearmente independentes. Suponhamos que $\sum\limits_{\text{fin.}} \lambda_r E_r k_{\alpha_r} = 0$, onde $\lambda_r \in \mathbb{C} - \{0\}$. Sem perda de generalidade, podemos assumir que todos os termos têm o mesmo Q-grau β. O termo de grau $(\beta, 0)$ em $\Delta(\sum \lambda_r E_r k_{\alpha_r})$ deve ser 0, logo

$$\begin{aligned} \sum \lambda_r E_r k_{\alpha_r} \otimes k_\beta k_{\alpha_r} &= 0, \\ \sum_\alpha \left(\left(\sum_{r|\alpha_r=\alpha} \lambda_r E_r \right) k_\alpha \otimes k_\alpha k_\beta \right) &= 0. \end{aligned}$$

Como os k_α's são linearmente independentes, segue que $\sum_{r|\alpha_r=\alpha} \lambda_r E_r = 0$, donde $\lambda_r = 0$ para todo r. ∎

Com este resultado, podemos obter facilmente uma base para $U_t\mathfrak{b}_-$. Consideremos o automorfismo φ de $U_t\mathfrak{g}$ definido por

$$\varphi(e_i) = -f_i, \quad \varphi(f_i) = -e_i, \quad \varphi(k_i) = k_i^{-1}.$$

Se $F_r = \varphi(E_r)$, então $(F_r)_{r\in I}$ é uma base de $U_t n_-$ constituída de monômios nos f_i's com as mesmas propriedades de $(E_r)_{r\in I}$ em relação a $U_t\mathfrak{b}_-$.

A decomposição triangular de $U_t\mathfrak{g}$

Proposição 123 *$(E_rF_{r'}k_\alpha)_{(r,r',\alpha)\in I\times I\times Q}$ é uma base de $U_t\mathfrak{g}$. Portanto, $U_t\mathfrak{g} \cong U_t\mathfrak{n}_- \otimes \mathbb{C}[T] \otimes U_t\mathfrak{n}_+$ como espaços vetoriais e $U_t\mathfrak{g}$ é um $U_t\mathfrak{b}_+$-módulo livre.*

Prova. Basta provar a independência linear. Suponhamos que $\sum_{\text{fin.}} \lambda_{r,r',\alpha} E_r F_{r'} k_\alpha = 0$, com $\lambda_{r,r',\alpha} \in \mathbb{C} - \{0\}$. Para cada $r \in I$, sejam α_r o grau de E_r e $-\alpha_{r'}$ o Q-grau de $F_{r'}$. Então o Q-grau de $E_r F_{r'} k_\alpha$ é $\alpha_r - \alpha_{r'}$ e podemos assumir sem perda de generalidade que os pares (r, r') ocorrendo na soma sejam tais que $\alpha_r - \alpha_{r'} =$ constante.

Vamos precisar de uma relação de ordem $\preccurlyeq$ definida em Q do seguinte modo: para $\alpha = \sum n_i \alpha_i \in Q$ sejam $m_i(\alpha) = n_i$ e $l(\alpha) = \sum m_i(\alpha) \in \mathbb{Z}$. Para cada par $\alpha \neq \alpha'$ dizemos que $\alpha \prec \alpha'$ se:

(a) $l(\alpha) < l(\alpha')$ ou

(b) $l(\alpha) = l(\alpha')$ e o menor índice i tal que $m_i(\alpha) \neq m_i(\alpha')$ verifique $m_i(\alpha) < m_i(\alpha')$.

Esta é uma relação de ordem total e é compatível com a adição.

Agora, consideremos $I_0 = \{r \in I : \operatorname{gr} E_r = \alpha_r \text{ seja maximal para } \preccurlyeq\}$. Então na equação $\Delta(\sum \lambda_{r,r',\alpha} E_r F_{r'} k_\alpha) = 0$, a componente de $Q \times Q$-grau maximal na primeira coordenada e minimal na segunda deve ser 0, isto é,

$$\sum_{r \in I_0} \lambda_{r,r',\alpha} (E_r k_{\alpha_{r'}} \otimes k_{\alpha_r}^{-1} F_{r'}) k_\alpha \otimes k_\alpha = 0.$$

Aqui α_r está fixado (pois é o grau de E_r), logo $\alpha_{r'}$ está também, e podemos cancelar os fatores $k_{\alpha_{r'}} \otimes 1$ e $1 \otimes k_{\alpha_r}^{-1}$ resultando sucessivamente

$$\sum_{r \in I_0} \lambda_{r,r',\alpha} (E_r k_\alpha \otimes F_{r'} k_\alpha) = 0,$$

$$\sum_{(r',\alpha) \text{ distintos}} \left(\sum_{r \in I_0} \lambda_{r,r',\alpha} E_r k_\alpha \right) \otimes F_{r'} k_\alpha = 0.$$

Como os $F_{r'} k_\alpha$ são linearmente independentes, para todo par (r', α) fixado, temos

$$\sum_{r \in I_0} \lambda_{r,r',\alpha} E_r k_\alpha = 0$$

e, conseqüentemente, $\lambda_{r,r',\alpha} = 0$. ∎

4.3.2 Representações de dimensão finita de $U_t\mathfrak{g}$

Seguindo Rosso [Rs2], vamos mostrar que quando t não é raiz da unidade, toda representação irredutível de $U_t\mathfrak{g}$ é obtida de uma deformação de uma representação irredutível de $\mathfrak{g}$, e que toda representação de $U_t\mathfrak{g}$ é essencialmente obtida por esse processo.

Resultados gerais

Seja V um espaço vetorial de dimensão finita sobre $\mathbb{C}$ e seja $\rho : U_t\mathfrak{g} \to \mathrm{End}(V)$ uma representação. Denotamos $\rho(a)(v)$ por $\alpha \cdot v$ para $a \in U_t\mathfrak{g}$ e $v \in V$.

Lema 124 *1. Os endomorfismos e_i, f_i, $i = 1, \ldots, N$, de V são nilpotentes.*

2. Se V é irredutível, então os endomorfismos k_i's de V são simultaneamente trigonalizáveis e $V = \bigoplus V_\mu$, onde $\mu \in \mathbb{C}[T]^* - \{0\}$ e

$$V_\mu = \{v \in V : k_i \cdot v = \mu(k_i)v,\ i = 1, \ldots, N\}$$

Prova. 1. Para $i = 1, \ldots, N$, se e_i tem um autovetor v associado ao autovalor não-nulo $\lambda \in \mathbb{C}$, então a relação

$$e_i \cdot (k_i^{-1} \cdot v) = t_i^2 k_i^{-1} e_i \cdot v = \lambda t_i^2 (k_i^{-1} \cdot v),$$

mostra-nos que e_i tem uma infinidade de autovalores não-nulos, donde e_i tem 0 como único autovalor, logo e_i é nilpotente. Idem para f_i.

2. Os endomorfismos k_i geram uma subálgebra abeliana L da álgebra de Lie $\mathfrak{gl}(V)$. Logo, pelo Teorema de Lie, V contém um autovetor v comum a todos os endomorfismos em L. Seja $E = \{W \text{ subespaço de } V : \dim W \geq 1 \text{ e } k_i|_W \text{ seja diagonalizável}\}$. O conjunto E é não-vazio pois $\mathbb{C}v \in E$. Consideremos $W \in E$ e dimensão maximal. Se W for invariante sob os e_i's e sob os f_i's, então devemos ter $W = V$ pois V é irredutível.

Suponhamos que exista $w \in W$ tal que $e_j \cdot w \notin W$ para algum $j = 1, \ldots, N$ (uma tal suposição sobre um f_j seria similar). Como $W = \bigoplus W_\mu$, onde $W_\mu = \{w : k_i \cdot w = \mu(k_i)w\}$, podemos assumir que $w \in W_\mu$ para algum $\mu \in \mathbb{C}[T]^* - \{0\}$. Desse modo, temos

$$k_i e_j \cdot w = t_i^{a_{ij}} e_j k_i \cdot w = \mu(k_i) t_i^{a_{ij}} e_j \cdot w,$$

donde $w' = e_j \cdot w$ é um autovetor comum a todos os endomorfismos k_i's e $W' = W \bigoplus \mathbb{C}w' \in E$, contrariando a maximalidade de W. ■

Observação: Os caracteres μ são chamados *pesos* da representação ρ e para cada $i = 1, \ldots, N$, como k_i é inversível, devemos ter $\mu_i = \mu(k_i) \neq 0$.

Definição 125 (Peso máximo) *Um vetor $v \in V - \{0\}$ é dito* vetor peso máximo *se existe $\lambda \in \mathbb{C}[T]^* - \{0\}$ tais que*

1. $k_i \cdot v = \lambda(k_i)v$

2. $e_i \cdot v = 0$,

para todo $i = 1, \ldots, N$.

Em outras palavras, v é vetor peso máximo se $0 \neq v \in V_\lambda$ para algum λ não-nulo e v é anulado por todos os endomorfismos e_i's.

Proposição 126 *Toda representação de dimensão finita V de $U_t\mathfrak{g}$ tem ao menos um vetor peso máximo.*

Prova. Como os k_i são simultaneamente diagonalizáveis, o conjunto de pesos $P = \{\mu \in \mathbb{C}[T]^* - \{0\} : V_\mu \neq 0\}$ é não-vazio. O subespaço vetorial não-nulo $V' = \bigoplus V_\mu$ é claramente invariante sob $U_t\mathfrak{g}$, i.é, V' é uma sub-representação de V.

Em V', consideremos $V_0 = \cap_{j=1}^N \ker e_j$. Se $v \in V_0$ então $e_j \cdot v = 0$, e $0 = k_i e_j \cdot v = t_i^{a_{ij}} e_j k_i \cdot v$, para todo $j = 1, \ldots, N$, donde $k_i \cdot v \in V_0$ e V_0 é invariante pelos k_i's. Desse modo, V_0 deve conter um autovetor comum a todos os k_i's, bastando-nos mostrar que $V_0 \neq 0$. Isto seguirá diretamente do lema abaixo. ■

Lema 127 *Sejam V, V' e P como na proposição acima. Existe um natural M tal que $\forall j_1, \ldots, j_p \in \{1, \ldots, N\}$, $e_{j_1} \cdots e_{j_p} = 0$ em $\operatorname{End} V'$ sempre que $p \geq M$.*

Prova. Basta verificar que $\forall \mu \in P$, e $\forall v \in V'$, $e_{j_1} \cdots e_{j_p} \cdot v = 0$ para p suficientemente grande. Fixemos $\mu \in P$, $v \in V_\mu$ e seja $v' = e_{j_1} \cdots e_{j_p} \cdot v$. Então, $k_i \cdot v' = \mu(k_i) t_i^{\sum_k a_{ij_k}} v'$, donde $v' \in V_{\mu'}$, com $\mu'_i = \mu_i t_i^{\sum_k a_{ij_k}}$. Se n_k é o número de vezes que e_k ocorre em $\{e_{j_1}, \ldots, e_{j_p}\}$, então podemos reescrever $\mu_i' = \mu_i t_i^{\sum_{k=1}^N n_k a_{ik}}$ (obs: $p = n_1 + \cdots + n_N$). Como V' tem dimensão finita, há apenas um número finito de pesos $\mu, \mu^{(1)}, \ldots, \mu^{(r)}$ e basta verificar que para p suficientemente grande μ' não está nesta lista (i.é, $V_{\mu'} = 0$). Para cada $i = 1, \ldots, N$ seja $x_i^{(s)} = \mu_i^{(s)}/\mu_i$; devemos encontrar um índice $i_0 \in \{1, \ldots, N\}$ tal que

$$t_{i_0}^{\sum_{k=1}^N n_k a_{i_0 k}} \notin \{1, x_{i_0}^{(1)}, \ldots, x_{i_0}^{(r)}\}.$$

Como t é não-nulo, fixamos $\xi \in \mathbb{C}$ tal que $t = e^{2\pi i \xi}$. $\xi \notin \mathbb{Q}$ pois t não é raiz da unidade. Como cada $x_i^{(s)}$ é não-nulo, fixamos também $y_i^{(s)}$ *tal* que $x_i^{(s)} = e^{2\pi i y_i^{(s)}}$. Então a igualdade $t_{i_0}^{\sum_k n_k a_{i_0 k}} = x_i^{(s)}$ se reescreve como

$$\frac{(\alpha_i, \alpha_i)}{2} \sum_{k=1}^N n_k a_{ik} = y_i^{(s)} + \frac{m}{\xi}, \text{ para algum } m,$$

e daí,

$$\sum_{k=1}^N n_k (\alpha_i, \alpha_k) = y_i^{(s)} + \frac{m}{\xi}.$$

O lado esquerdo desta igualdade está em $\mathbb{Z}$, logo o lado direito também deve estar e existe no máximo um inteiro m tal que $y_i^{(s)} + \frac{m}{\xi} \in \mathbb{Z}$. Façamos $z_i^{(s)} = y_i^{(s)} + \frac{m}{\xi}$. Suponhamos que para cada $i = 1, \ldots, N$ exista $s \in \{0, \ldots, r\}$ tal que

$$\sum_{k=1}^N n_k (\alpha_i, \alpha_k) = z_i^{(s)}$$

Isso nos dá um sistema linear nas incógnitas $n_1, \ldots, n_N$, cuja matriz é $((\alpha_i, \alpha_k))$, a qual é inversível. Assim, dados $z_1^{(s_1)}, \ldots, z_N^{(s_N)}$ há no máximo uma solução inteira para esse sistema. Como podemos formar apenas um número finito de N-uplas $(z_1^{(s_1)}, \ldots, z_N^{(s_N)})$, vemos que se $(n_1, \ldots, n_N)$ não pertencer a um certo conjunto finito (a reunião de todas as possíveis soluções para os sistemas construídos da maneira prescrita), então sempre podemos conseguir um índice i_0 tal que $t_{i_0}^{\sum_k n_k a_{i_0 k}} \notin \{1, x_{i_0}^{(1)}, \ldots, x_{i_0}^{(r)}\}$. Tomando $M = \sup\{|n_1| + \cdots + |n_N|\} + 1$ onde $(n_1, \ldots, n_N)$ percorre o tal conjunto finito, obtemos o lema. ∎

Definição 128 *Seja V um $U_t\mathfrak{g}$-módulo tal que $V = U_t\mathfrak{g} \cdot v_+$ para um vetor peso máximo v_+ de* *peso λ. Dizemos que V é um $U_t\mathfrak{g}$*-módulo cíclico.

Proposição 129 *Seja V um $U_t\mathfrak{g}$-módulo cíclico gerado por um vetor peso máximo v_+, com peso λ.*

1. *V é gerado por v_+ e por $f_{i_1}\cdots f_{i_p}\cdot v_+$, $i_1,\ldots,i_p = 1,\ldots,N$, e tal vetor, se não-nulo, é um vetor de peso μ tal que $\mu_k = \lambda_k t_k^{-\sum_j a_{ki_j}}$.*

2. *Todos os pesos de V são dessa forma.*

3. *Para cada peso μ, $\dim V_\mu$ é finita e $\dim V_\lambda = 1$.*

4. *V é um $U_t\mathfrak{g}$-módulo indecomponível, com um único submódulo próprio maximal.*

Prova. É análoga à encontrada em Humphreys [Hu, §20.2], usando a decomposição $U_t\mathfrak{g} \cong U_t\mathfrak{n}_- \otimes \mathbb{C}[T] \otimes U_t\mathfrak{n}_+$. Para (3), usamos o mesmo argumento do lema (127) que $f_{j_1}\cdots f_{j_r}\cdot v_+$ e $f_{i_1}\cdots f_{i_p}\cdot v_+$ têm o mesmo peso se, e só se, $\forall i$, f_i aparece o mesmo número de vezes em $\{f_{j_1},\ldots,f_{j_r}\}$ e $\{f_{i_1},\ldots,f_{i_p}\}$. ∎

Proposição 130 *Se ρ e ρ' são duas representações irredutíveis de mesmo peso máximo, então elas são equivalentes.*

Prova. Basta notar que se V e V' são os respectivos $U_t\mathfrak{g}$-módulos, então V e V' são ambos cíclicos. O resto segue analogamente ao Teorema A de Humphreys [Hu, §20.3]. ∎

Agora, estamos em uma condição tal que dada uma representação irredutível de dimensão finita, sabemos que esta tem peso máximo, necessariamente único. A fim de determinar os possíveis valores de λ, devemos considerar, para cada $i = 1,\ldots,N$, a restrição da representação à subálgebra gerada por $k_i^{\pm 1}$, e_i, f_i, a qual é isomorfa a $U_t\mathfrak{sl}(2,\mathbb{C})$.

Representações de dimensão finita de $U_t\mathfrak{sl}(2,\mathbb{C})$

Por simplicidade, denotaremos por $k^{\pm 1}$, e, f os geradores de $U_t\mathfrak{sl}(2,\mathbb{C})$. Observamos que, neste caso, $\mathbb{C}[T]^*$ é canonicamente isomorfo a $\mathbb{C}$, donde os pesos de uma representação de $U_t\mathfrak{sl}(2,\mathbb{C})$ são identificados a elementos de $\mathbb{C}$.

Lema 131 *1.* $C = \dfrac{(kt - k^{-1}t^{-1})^2}{(t^2 - t^{-2})^2} + fe$ *pertence ao centro de* $U_t\mathfrak{sl}(2,\mathbb{C})$ *e age como um escalar não-nulo sobre toda representação irredutível de dimensão finita.*

2. Para $\omega' \in \{1,-1,i,-i\}$*, seja* $C' = C - \dfrac{(\omega' t - \omega'^{-1}t^{-1})^2}{(t^2 - t^{-2})^2}$*. Este age como um escalar não-nulo sobre toda representação irredutível de dimensão finita, desde que esta tenha dimensão maior que* 2.

Prova. Um cálculo imediato verifica que C e C' comutam com k, e, f, donde estes encontram-se no centro da álgebra e agem como escalares sobre toda representação irredutível. O respectivo escalar é obtido avaliando-se sobre o vetor de peso máximo v_0. Para C obtemos o escalar

$$\frac{(\omega t^{m+1} - \omega^{-1}t^{-(m+1)})^2}{(t^2 - t^{-2})} \neq 0,$$

pois t não é raiz da unidade. Para C', temos o escalar

$$\frac{(\omega^2 t^{2(m+1)} + \omega^{-2}t^{-2(m+1)} - \omega'^2 t^2 - \omega'^{-2}t^{-2})^2}{(t^2 - t^{-2})^2}.$$

Notando que $\omega^2 = \omega^{-2}$ e $\omega'^2 = \omega'^{-2}$, vemos que esse escalar é nulo se, e só se,

$$\omega^2(t^{2(m+1)} + t^{-2(m+1)}) = \omega'^2(t^2 + t^{-2}),$$

ou, equivalentemente,

$$\frac{t^{2(m+1)} - t^{-2(m+1)}}{t^2 + t^{-2}} = \left(\frac{\omega'}{\omega}\right)^2 \in \{-1, 1\},$$

o que é impossível se $m \geq 1$, já que t não é raiz da unidade. ∎

Teorema 132 *1. Se* $\lambda \in \mathbb{C} - \{0\}$ *é o peso máximo de uma representação de dimensão finita de* $U_t\mathfrak{sl}(2,\mathbb{C})$*, então* $\lambda = \omega t^m$ *onde* $\omega \in \{1,-1,i,-i\}$ *e* $m \in \mathbb{N}$*.*

2. Para cada $m \in \mathbb{N}$ *e* $\omega \in \{1,-1,i,-i\}$*,* $\lambda = \omega t^m$ *é o peso máximo de uma representação irredutível de dimensão* $(m+1)$*, e os pesos dessa representação são exatamente:* $\omega t^m, \omega t^{m-2}, \ldots, \omega t^{-m}$*.*

3. Toda representação de dimensão finita de $U_t\mathfrak{sl}(2,\mathbb{C})$ *é completamente redutível.*

Prova. 1. (Compare com Humphreys [Hu, §7.2]). Seja v um vetor com peso máximo λ. Definindo $v_p = \frac{1}{p!} f^p \cdot v$, $v_0 = v$, $v_{-1} = 0$, então um cálculo direto permite-nos ver que

(a) $f \cdot v_p = (p+1)v_{p+1}$ é simplesmente a definição de v_{p+1},

(b) $k \cdot v_p = \lambda t^{-2p} v_p$,

(c) $e \cdot v_p = \dfrac{t^{2p} - t^{-2p}}{t^2 - t^{-2}} \cdot \dfrac{t^{-2(p-1)}\lambda^2 - t^{2(p-1)}\lambda^{-2}}{t^2 - t^{-2}} v_{p-1}$, $p \geq 0$.

A equação (c) segue diretamente da fórmula

$$[ef^p] = f^{p-1} \frac{t^{2p} - t^{-2p}}{t^2 - t^{-2}} \cdot \frac{k^2 t^{-2(p-1)} - k^{-2} t^{2(p-1)}}{t^2 - t^{-2}},$$

a qual é provada facilmente por indução, e do fato que $e \cdot v_0 = 0$. Como V tem dimensão finita há um primeiro inteiro m tal que $v_{m+1} = 0$. Daí, como t não é raiz da unidade, de (c) obtemos $t^{-2m}\lambda^2 - t^{2m}\lambda^{-2} = 0$, ou seja $\lambda^4 = t^{4m}$ e, conseqüentemente, $\lambda = \omega t^m$, para $\omega \in \{1, -1, i, -i\}$.

2. Seja V o espaço vetorial com base $(v_0, \ldots, v_m)$ sobre o qual k, e, f agem pelas fórmulas (a)-(c), com $\lambda = \omega t^m$. Os endomorfismos k, e, f de V satisfazem as relações que definem $U_t\mathfrak{sl}(2, \mathbb{C})$, logo V é um $U_t\mathfrak{sl}(2, \mathbb{C})$-módulo. Este é irredutível, pois os vetores pesos v_p's são únicos a menos de escalares. A segunda afirmação segue imediatamente de (b) e de $v_{-1} = v_{m+1} = 0$.

3. Imita o clássico Teorema de Weyl (cf. Teorema 50), onde $C\,'$ do Lema (1) tem papel análogo ao do elemento de Casimir da representação.

Uma discussão mais aprofundada sobre este assunto pode ser encontrada em Lusztig [Lu, 6]. ■

Corolário 133 *Se λ é o peso máximo de uma representação irredutível de dimensão finita de $U_t\mathfrak{g}$, então, necessariamente os $\lambda_j = \lambda(k_j) = \omega_j t^{m_j}$, onde $\omega_j \in \{1, -1, i, -i\}$ e $m_j \in \mathbb{N}$.*

■

Com isso, classificamos as representações irredutíveis de $U_t\mathfrak{sl}(2, \mathbb{C})$, quando t não é raiz da unidade. Embora não consideraremos este caso aqui, Roche & Arnaudon [RA] estenderam a análise para t raiz da unidade. Ao contrário daquilo que aqui obtivemos, foi mostrado que nem todas estas representações correspondem a representações de peso máximo. Encontram-se, pois, classificadas todas as representações irredutíveis de $U_t\mathfrak{sl}(2, \mathbb{C})$.

4.4 Observações Finais

Para finalizar este capítulo, vale mencionar que, conforme pode ser constatado em Chary & Pressley [CP], a teoria das representações de $U_t\mathfrak{g}$, para uma álgebra de Lie simples $\mathfrak{g}$ encontra-se atualmente em estágio bastante mais avançado que o discutido aqui. Estas serão objeto de estudo ulterior.

Também vale dizer que, além de constituir a ferramenta matemática correta que permitiu uma organização e um melhor direcionamento dos conhecimentos adquiridos no estudo dos sistemas integráveis em Mecânica Estatística, muito provavelmente a maior realização da Teoria dos Grupos Quânticos até os dias de hoje se resume na obtenção de novos invariantes de nós e de 3-variedades.

Este é um feito notável, decorrente principalmente dos trabalhos de Witten [Wi] e Drinfeld [D], e culminando na derivação da fórmula de Reshetikhin-Turaeev [RT], que efetuou um primeiro e grande passo de uma antiga busca da comunidade dos matemáticos.

Grande parte das pesquisas atuais se polarizam na compreensão dos invariantes de 3-variedades obtidos em [RT].

Apêndice A

Álgebra Linear

Neste apêndice, encontram-se alguns conceitos da Álgebra Linear que, apesar de elementares, não são completamente óbvios. Não pretendemos que este seja um estudo de revisão, mas recolhemos aqui apenas os ingredientes essenciais a este trabalho. Boa parte do material apresentado é proveniente da teoria e de exercícios propostos encontrados em Brown [Br] e Lang [La].

A.1 Módulos

A.1.1 Preliminares algébricos

Seja $1 = \{0\}$ o conjunto contendo um único elemento. Para qualquer conjunto A, temos as bijeções naturais

$$1 \times A \to A \quad \text{e} \quad A \times 1 \to A,$$

dadas respectivamente por $(0, x) \mapsto x$ e $(x, 0) \mapsto x$. Estas permitem que identifiquemos naturalmente os conjuntos A, $1 \times A$, e $A \times 1$. Observamos que, sob tais identificações, o conjunto pontual 1 tem o papel de "unidade" na construção do produto cartesiano de conjuntos. O conceito de monóide tem papel fundamental na Teoria de Categorias [Ln, pág. 2], pois é muito útil substituir o produto cartesiano de conjuntos por outras construções que têm propriedes análogas com respeito à unidade.

Um *monóide* é uma tripla (A, μ, η) consistindo de um conjunto A, uma função $\mu : A \times A \to A$, denominada *multiplicação*, e uma função $\eta : 1 \to A$, denominada *unidade*, tornando comutativos os diagramas

$$
\begin{tikzcd}
A \times A \times A \arrow[r, "\mathrm{id} \times \mu"] \arrow[d, "\mu \times \mathrm{id}"'] & A \times A \arrow[d, "\mu"] \\
A \times A \arrow[r, "\mu"] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \times A \arrow[r, "\eta \times \mathrm{id}"] \arrow[d, "\simeq"'] & A \times A \arrow[d, "\mu"] & A \times 1 \arrow[l, "\mathrm{id} \times \eta"'] \arrow[d, "\simeq"] \\
A \arrow[r, "\mathrm{id}"] & A & A \arrow[l, "\mathrm{id}"']
\end{tikzcd}
$$

Equivalentemente, denotando $\mu(x,y)$ simplesmente por xy, e denotando o único valor da função η em A por 1_A, escrevemos $(xy)z = x(yz)$ e $x1_A = 1_Ax = x$, para todo x, y, $z \in A$.

Um monóide satisfazendo a condição $\mu \circ \tau = \mu$, onde $\tau : A \times A \to A \times A$ é a bijeção natural definida por $(a,b) \mapsto (b,a)$, é dito *comutativo*.

Um *anel com unidade* é uma quádrupla $(A, +, \mu, \eta)$ consistindo de um grupo abeliano $(A, +)$, e de um monóide (A, μ, η) satisfazendo as condições de compatibilidade:

1. $\mu(x+y, z) = \mu(x,z) + \mu(y,z)$,

2. $\mu(x, y+z) = \mu(x,y) + \mu(x,z)$,

quaisquer que sejam $x, y, z \in A$.

Definição 134 (Ação de monóide) *Chama-se ação do monóide (A, μ, η) à esquerda do conjunto S uma aplicação $\varphi : A \times S \to S$ tornando comutativos os diagramas*

$$
\begin{tikzcd}
A \times A \times S \arrow[r, "\mathrm{id} \times \varphi"] \arrow[d, "\mu \times \mathrm{id}"'] & A \times S \arrow[d, "\varphi"] \\
A \times S \arrow[r, "\varphi"] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
1 \times S \arrow[r, "\eta \times \mathrm{id}"] \arrow[d, "\simeq"'] & A \times S \arrow[d, "\varphi"] \\
S \arrow[r, "\mathrm{id}"] & A
\end{tikzcd}
$$

Em termos de elementos, denotando por $a \cdot s$ o valor da ação à esquerda φ aplicada a um par arbitrário $(a,s) \in A \times S$, temos equivalentemente

$$(ab) \cdot s = a \cdot (b \cdot s) \quad e \quad 1_A \cdot s = s.$$

Similarmente, chama-se ação do monóide (A, μ, η) à direita do conjunto S uma aplicação ψ :

$S \times A \to A$ *tornando comutativos os diagramas*

$$\begin{array}{ccc} S \times A \times A & \xrightarrow{\psi \times \mathrm{id}} & S \times A \\ {\scriptstyle \mathrm{id} \times \mu}\Big\downarrow & & \Big\downarrow{\scriptstyle \psi} \\ S \times A & \xrightarrow{\psi} & A \end{array} \qquad \qquad \begin{array}{ccc} S \times 1 & \xrightarrow{\mathrm{id} \times \eta} & S \times A \\ {\scriptstyle \simeq}\Big\downarrow & & \Big\downarrow{\scriptstyle \psi} \\ S & \xrightarrow{\mathrm{id}} & A \end{array}$$

Denotando por $s \cdot a$ o valor da ação à esquerda ψ aplicada a um par arbitrário $(s, a) \in S \times A$ temos equivalentemente

$$s \cdot (ab) = (s \cdot a) \cdot b \quad e \quad s \cdot 1_A = s.$$

Definição 135 (Ação de anel) *Seja $(A, +, \mu, \eta)$ um anel com unidade, e M um grupo abeliano. Chama-se ação de A à esquerda de M uma aplicação $\varphi : A \times M \longrightarrow M$ que é uma ação do monóide (A, μ, η) sobre o conjunto M, satisfazendo as condições de compatibilidade*

1. $\varphi(a + b, m) = \varphi(a, m) + \varphi(b, m)$,

2. $\varphi(a, m + n) = \varphi(a, m) + \varphi(a, m)$,

3. $\varphi(-a, m) = -\varphi(a, m) = \varphi(a, -m)$,

para todo $a, b \in A$ e todo $m \in M$. Similarmente, define-se ação de A à direita de M.

Observamos que uma ação de anel sobre um grupo abeliano é uma ação de monóide sobre um conjunto quando ignoramos as estruturas adicionais de grupos abelianos de A e de M assim como as condições de compatibilidade acima. De modo geral, a ação de uma estrutura algébrica sobre outra é definida levando-se em consideração condições que, num certo sentido, tornem a ação compatível com tais estruturas. Freqüentemente diferentes pares de estruturas algébricas admitem múltiplas ações distintas. Muitas vezes, porém, admitem uma única ação, ou não admitem ação alguma. Este é o tema principal abordado pela Teoria de Representações.

Sobre um mesmo conjunto S pode haver ações de A à esquerda e à direita simultaneamente. Dizemos que essas ações são *compatíveis* quando comutam entre si, isto é, quando o diagrama

$$\begin{array}{ccc} S \times A \times S & \xrightarrow{\varphi \times \mathrm{id}} & A \times S \\ {\scriptstyle \mathrm{id} \times \psi}\Big\downarrow \mathrm{id} \times \psi & & \Big\downarrow{\scriptstyle \psi} \\ S \times A & \xrightarrow{\varphi} & A \end{array}$$

é comutativo. Equivalentemente, temos

$$(a \cdot m) \cdot b = a \cdot (m \cdot b),$$

para todo $a, b \in A$ e todo $m \in M$.

Um subconjunto não-vazio N de M é dito *estável* sob a ação de A à esquerda de M quando $\operatorname{Im} \varphi|_{S \times N} \subset N$, isto é, quando $a \cdot n \in N$, para todo $a \in A$ e todo $n \in N$. De maneira similar, definimos um subconjunto estável sob uma ação de A à direita de M.

Daqui por diante, não havendo confusão, vamos abandonar a notação extensa $(A, +, \mu, \eta)$, dizendo simplesmente que A é anel com unidade 1_A.

A.1.2 Definição e exemplos

Definição 136 (Módulo) *Seja A um anel com unidade 1_A. Um A-módulo à esquerda é um grupo abeliano M dotado de uma ação de A à esquerda de M. Similarmente, um A-módulo à direita é um grupo abeliano M dotado de uma ação de A à direita de M. Um módulo bilateral é um grupo abeliano M dotado simultaneamente de uma ação à esquerda e de uma ação à direita comutando entre si.*

Um subgrupo N de M estável sob a ação à esquerda é dito *A-submódulo à esquerda* de M. Analogamente, definimos *A-submódulo à direita* de um A-módulo à direita, e *A-submódulo bilateral* de um A-módulo bilateral. Todo A-módulo admite pelo menos os *A-submódulos triviais*, $0 = \{0\}$ e A.

Um A-módulo M que admite apenas os A-submódulos triviais é chamado *A-módulo simples*, ou *irredutível*.

Todo anel A, visto como um grupo abeliano, é um A-módulo à esquerda, à direita e bilateral. Nesse caso, um A-submódulo à esquerda é um *ideal à esquerda*, um A-submódulo à direita é um *ideal à direita* e um A-submódulo bilateral é um *ideal bilateral* de A.

No que segue, salvo menção contrária, referir-nos-emos a um A-módulo à esquerda, à direita ou bilateral M simplesmente por módulo M, omitindo o anel A e deixando implícita a condição de lateralidade. Utilizaremos a mesma convenção para as definições derivadas de A-módulos, como A-submódulos, por exemplo.

Definição 137 *Uma aplicação $f : M \to N$ entre os módulos M e N satisfazendo as condições*

1. $f(m+n) = f(m) + f(n)$, para todo $m, n \in M$, e

2. $f(a \cdot m) = a \cdot f(m)$, para todo $m \in M$, e todo $a \in A$,

é chamada *(homo)morfismo de A-módulos*, ou *transformação A-linear.* Um homomorfismo bijetor é chamado *isomorfismo.*

Um cálculo direto nos permite verificar que que $\operatorname{Ker} f = \{m \in M : f(m) = 0\}$ e $\operatorname{Im} f$ são submódulos de M e N respectivamente, e que f é injetor se e somente se $\operatorname{Ker} f = 0$. Isto nos permite obter imediatamente o importante lema que segue.

Lema 138 (Schur) *Se $f : M \to N$ é um homomorfismo entre módulos irredutíveis, então ou f é identicamente nulo ou é isomorfismo.*

Exemplo 139 Todo grupo abeliano G é um $\mathbb{Z}$-módulo à esquerda com a ação $\varphi(n, g) = ng$, para todo $n \in \mathbb{Z}$, e todo $g \in G$. $\square$

Exemplo 140 Um espaço vetorial V sobre um corpo F é um F-módulo à esquerda com ação à esquerda dada pela multiplicação por escalar $(\lambda, v) \mapsto \lambda \cdot v$. Um F-submódulo de V é exatamente um subespaço de V. $\square$

A.1.3 Produto Direto

Seja $\{M_i\}_{i \in I}$ uma família de módulos sobre o anel A. Consideremos $x = \{x_i\}_{i \in I}$, o conjunto obtido pela escolha de exatamente um elemento x_i de cada M_i. O elemento x_i é denominado i-ésima componente de x. Seja P o conjunto de todos os x obtidos desta maneira. Então, P é um módulo sobre o anel A. Com efeito, se $x = \{x_i\}_{i \in I}$, $y = \{y_i\}_{i \in I}$, e $a \in A$, definimos

$$x + y = \{x_i + y_i\}_{i \in I}, \qquad\qquad ax = \{ax_i\}_{i \in I}.$$

Para cada $i \in I$, a aplicação $\pi_i : P \to M_i$ que assume o valor da i-ésima componente x_i de $x = \{x_i\}_{i \in I}$ é um homorfismo sobrejetor, pois

$$\pi_i(x + y) = \pi_i(\{x_i + y_i\}_{i \in I}) = x_i + y_i = \pi_i(x) + \pi_i(y),$$

e

$$\pi_i(ax) = \pi_i(\{ax_i\}_{i\in I}) = ax_i = a\pi_i(x),$$

chamado *projeção natural* de P sobre o módulo M_i. O par $(P, \{\pi_i\}_{i\in I})$, consistindo do módulo P e da família de homorfismos $\{\pi_i\}_{i\in I}$, é chamado *produto direto* da família de módulos $\{M_i\}_{i\in I}$. Este é denotado por $\prod_{i\in I} M_i$. O produto direto de uma família finita $M_1, \ldots, M_n$ é denotado por $M_1 \times \cdots \times M_n$ e, neste caso, seus elementos são escritos $(x_1, \ldots, x_n)$, para $x_i \in M_i$.

O produto direto tem a seguinte propriedade universal:

Proposição 141 *Dado um par $(N, \{\xi_i\}_{i\in I})$, consistindo de um módulo arbitrário N e uma família de homomorfismos $\xi_i : N \to M_i$, $i \in I$, existe um único homorfismo $f : N \to \prod_{i\in I} M_i$ que torna comutativo o diagrama*

$$\begin{tikzcd} N \arrow[d, "f"'] \arrow[dr, "\xi_i"] & \\ \prod_{i\in I} M_i \arrow[r, "\pi_i"'] & M_i \end{tikzcd}$$

isto é, $\xi_i = \pi_i \circ f$.

Em outras palavras a proposição nos diz que a aplicação

$$\begin{array}{rcl} \mathrm{Hom}_A(N, \prod_{i\in I} M_i) & \to & \prod_{i\in I} \mathrm{Hom}_A(N, M_i) \\ f & \mapsto & \{\pi_i \circ f\}_{i\in I} \end{array}$$

é uma bijeção. Além disso, se A for comutativo, então teremos o isomorfismo natural

$$\mathrm{Hom}_A(N, \prod_{i\in I} M_i) \cong \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$$

de módulos sobre A. O elemento de $\mathrm{Hom}_A(N, \prod_{i\in I} M_i)$, correspondente ao elemento $\{f_i\}_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(N, M_i)$, é escrito $\prod_{i\in I} f_i$ e chamado produto direto dos homomorfismos $\{f_i\}_{i\in I}$. A propriedade universal acima nos fornece uma caracterização do produto direto $\prod_{i\in I} M_i$. Recordamos que um objeto caracterizado por uma propriedade universal é único, a menos de isomorfismos.

A.1.4 A aplicação transposição

Sejam M e N dois módulos sobre um anel A com unidade 1_A, e consideremos o produto direto $(M \times N, \{\pi_1, \pi_2\})$, consistindo do módulo $M \times N$ e das projeções naturais $\pi_1 : M \times N \to M$ e $\pi_2 : M \times N \to N$, definidas respectivamente por $\pi_1(m,n) = m$ e $\pi_2(m,n) = n$, para $(m,n) \in M \times N$ arbitrário. Consideremos também o produto direto $(N \times M, \{\pi_1', \pi_2'\})$, consistindo do módulo $N \times M$ e das projeções $\pi_1' : N \times M \to N$ e $\pi_2' : N \times M \to M$, definidas respectivamente por $\pi_1'(n,m) = n$ e $\pi_2'(n,m) = m$, para $(n,m) \in N \times M$ arbitrário. A Proposição 141 acima nos fornece únicos homorfismos $f : M \times N \to N \times M$ e $g : N \times M \to M \times N$ tornando comutativos os diagramas

$$\begin{tikzcd}
M \times N \arrow[dd, "f"'] \arrow[dr, "\pi_1"] & \\
& M \\
N \times M \arrow[ur, "\pi_2'"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
M \times N \arrow[dd, "f"'] \arrow[dr, "\pi_2"] & \\
& N \\
N \times M \arrow[ur, "\pi_1'"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
N \times M \arrow[dd, "g"'] \arrow[dr, "\pi_2'"] & \\
& M \\
M \times N \arrow[ur, "\pi_1"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
N \times M \arrow[dd, "g"'] \arrow[dr, "\pi_1'"] & \\
& N \\
M \times N \arrow[ur, "\pi_2"'] &
\end{tikzcd}$$

Compondo os diagramas, no sentido vertical, obtemos respectivamente os seguintes diagramas comutativos

$$\begin{tikzcd}
M \times N \arrow[dd, "g \circ f"'] \arrow[dr, "\pi_1"] & \\
& M \\
M \times N \arrow[ur, "\pi_1"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
M \times N \arrow[dd, "g \circ f"'] \arrow[dr, "\pi_2"] & \\
& N \\
M \times N \arrow[ur, "\pi_2"'] &
\end{tikzcd}$$

Não obstante, ambos diagramas são comutativos quando consideramos a identidade id substituindo $g \circ f$. Logo, pela Proposição 141, devemos ter $g \circ f = \mathrm{id}$. Do mesmo modo, $f \circ g = \mathrm{id}$ e, conseqüentemente, f é isomorfismo com inversa g.

Temos $\pi_2' \circ f(m,n) = \pi_1(m,n) = m$ e $\pi_1' \circ f(m,n) = \pi_2(m,n) = n$, para todo (m,n) em $M \times N$. Assim, temos $f(m,n) = (n,m)$. A aplicação f é chamada de *aplicação transposição (ou aplicação twist).* Neste trabalho, ainda que apareça em um contexto mais geral, a aplicação transposição é sempre denotada por τ.

A.1.5 Soma direta

Seja S o subconjunto de $\prod_{i\in I} M_i$ consistindo dos elementos $\{\pi_i\}_{i\in I}$ tais que x_i é zero quase sempre, i.é, a menos de um número finito de componentes. Então S é um submódulo de $\prod_{i\in I} M_i$. Quando $I = \{1, 2, \ldots, n\}$, temos $S = \prod_{i\in I} M_i$. Para cada $i \in I$, a aplicação $\theta_i : M_i \to S$, que leva um elemento x_i no elemento de S cuja i-ésima coordenada é igual a x_i e as demais todas iguais a zero, é um homomorfismo injetor chamado *inclusão natural*, de M_i em S. Com isto, podemos identificar M_i à sua imagem em S. Assim, todo elemento $x = \{x_i\}_{i\in I} \in S$ pode ser escrito como $x = \sum_{i\in I} x_i$ (uma soma finita). O par $(S, \{\theta_i\}_{i\in I})$, consistindo do módulo S e da família de homomorfismos $\{\theta_i\}_{i\in I}$, é chamado *soma direta* da família de módulos $\{M_i\}_{i\in I}$. Esta é denotada por $\coprod_{i\in I} M_i$ ou por $\bigoplus_{i\in I} M_i$.

A soma direta tem a seguinte propriedade universal:

Proposição 142 *Dado um par $(N, \{\xi_i\}_{i\in I})$ consistindo de um módulo arbitrário N e de uma família de homomorfismos $\xi_i : M_i \to N$, $i \in I$, existe um único homomorfismo $f : \bigoplus_{i\in I} M_i \to N$ tornando comutativo o diagrama*

$$\begin{tikzcd} & \bigoplus_{i\in I} M_i \arrow[d, "f"] \\ M_i \arrow[ur, "\theta_i"] \arrow[r, "\xi_i"'] & N \end{tikzcd}$$

isto é, $f \circ \theta_i = \xi_i$.

Em outras palavras, a proposição acima nos diz que a aplicação

$$\begin{array}{ccc} \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N) & \to & \prod_{i\in I} \mathrm{Hom}_A(M_i, N) \\ f & \mapsto & \{f \circ \theta_i\}_{i\in I} \end{array}$$

é uma bijeção. Além disso, se A for comutativo, então teremos o isomorfismo natural

$$\mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N) \cong \prod_{i\in I} \mathrm{Hom}_A(M_i, N)$$

de módulos sobre A. O elemento de $\mathrm{Hom}_A(\bigoplus_{i\in I} M_i, N)$, correspondente ao elemento

$$\{f_i\}_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(M_i, N) \ ,$$

é escrito $\bigoplus_{i\in I} f_i$ e denominado soma direta dos homomorfismos $\{f_i\}_{i\in I}$. A propriedade universal acima caracteriza unicamente, a menos de isomorfismos, a soma direta $\bigoplus_{i\in I} M_i$.

Um módulo M, que se escreve como soma direta de uma família de submódulos irredutíveis M_i, é dito *completamente redutível*. Equivalentemente, um módulo M é *completamente redutível* quando todo submódulo N de M tiver um complementar N' em M. Isto é, quando $M = N \oplus N'$, para algum submódulo N'.

A.1.6 Módulos livres

Seja A um anel com unidade e S um conjunto. Consideremos a soma direta $F = \bigoplus_{s\in S} A$, isto é, a soma direta de cópias idênticas de A indexadas pelo conjunto S. Identificando a imagem do elemento unidade $1_A \in A$ pela inclusão natural θ_s com o símbolo $s \in S$, passamos a considerarr S como um subconjunto de F e cada elemento $x \in F$ pode ser escrito unicamente como

$$x = \sum_{s\in S} x_s s$$

onde $x_s \in A$ e $x_s = 0$ quase sempre. Neste caso, F é dito ser um *módulo livre* gerado por S.

Seja M um módulo sobre A e S um subconjunto de M, satisfazendo as condições

1. Para todo subconjunto $\{s_1, \ldots, s_n\}$ de S,

$$\sum_{i=1}^{n} a_i s_i = 0 \ \Rightarrow a_i = 0, \text{ para todo } i,$$

   isto é, S é *linearmente independente*.

2. Dado um elemento arbritrário de x de M, podemos escolher um subconjunto finito $\{s_1, \ldots, s_n\}$ de S tal que

$$x = \sum_{i=1}^{n} a_i s_i$$

onde $a_i \in A$. Em outras palavras, M é gerado pelo conjunto S ou S é um conjunto de geradores para M.

Então S é chamada de *base* de M.

Se F é o módulo livre gerado pelo conjunto S então S é uma base de F quando consideramos S como um subconjunto de M (pela inclusão natural). Reciprocamente, um módulo M que tem uma base S é isomorfo ao módulo livre gerado por S. Conseqüentemente, para que um módulo M seja livre é necessário e suficiente que M admita uma base S. Se um módulo M admite um conjunto finito de geradores, dizemos que M é um módulo livre *finitamente gerado*.

Se A é uma anel comutativo, o número de elementos numa base qualquer de um módulo finitamente gerado M é constante. Este número é chamado *posto* de M, denotado por $\operatorname{rk} M$. Dado um corpo K, um espaço vetorial sobre K admite uma base, e portanto é um módulo livre. Para um espaço vetorial finitamente gerado V, utlizamos a nomenclatura *dimensão* para nos referirmos ao seu posto, denotando-o por $\dim V$.

A.1.7 Produto Tensorial

Vimos acima que uma maneira de construir outros módulos a partir de alguns conhecidos é fazendo seu produto direto ou sua soma direta. Agora, veremos como o conceito de transformação n-linear (ou transformação multilinear) pode nos fornecer uma outra maneira de obter novos módulos. No que segue, F é um anel comutativo, porém os casos de maior interesse aqui correspondem a quando F for um corpo.

Definição 143 Sejam $V_1, \ldots, V_n, W$ módulos sobre F. Dizemos que uma função

$$f : V_1 \times \cdots \times V_n \to W$$

é uma *transformação n-linear* se

(i) $f(x_1, \ldots, x_i + x_i', \ldots x_n) = f(x_1, \ldots, x_i, \ldots x_n) + f(x_1, \ldots, x_i', \ldots x_n)$

(ii) $f(x_1, \ldots, \lambda x_i, \ldots x_n) = \lambda f(x_1, \ldots, x_i, \ldots x_n)$

para todo $\lambda \in F$ *e* $x_j, x_j' \in V_j$, com $j = 1, \ldots, n$.

Denotamos por $\mathcal{L}_n(V_1, \ldots, V_n; W)$ o módulo de todas as transformações n-lineares de $V_1 \times \cdots \times V_n$ em W. Se $f : V_1 \times \cdots \times V_n \to W$ é n-linear e $g : W \to U$ é linear, então é $g \circ f$ é claramente n-linear. Aqui podemos nos indagar se toda transformação n-linear definida em $V_1 \times \cdots \times V_n$ pode ser obtida desse modo. Isso equivale a formular a pergunta: será que existe um módulo W e uma transformação n-linear $f \in \mathcal{L}_n(V_1, \ldots, V_n; W)$ com a seguinte propriedade universal?

(PT) Dado qualquer módulo U sobre F e uma transformação n-linear $g \in \mathcal{L}_n(V_1, \ldots, V_n; U)$, existe uma única transformação linear $\varphi : W \to U$ tornando comutativo o diagrama

$$\begin{tikzcd} & W \arrow[dd, "\varphi"] \\ V_1 \times \cdots \times V_n \arrow[ur, "f"] \arrow[dr, "g"'] & \\ & U \end{tikzcd}$$

Notemos que uma resposta à essa pergunta é fornecida por um par (W, f) , consistindo de um módulo W sobre F e de uma função n-linear $f : V_1 \times \cdots \times V_n \to W$. E esse par será único, a menos de isomorfismos. De fato, se (W', h) também tem a propriedade (PT) acima, então são comutativos os seguintes diagramas

$$\begin{tikzcd} & W \arrow[dd, "\varphi_f"] \\ V_1 \times \cdots \times V_n \arrow[ur, "f"] \arrow[dr, "h"'] & \\ & W' \end{tikzcd} \qquad \begin{tikzcd} & W' \arrow[dd, "\varphi_g"] \\ V_1 \times \cdots \times V_n \arrow[ur, "h"] \arrow[dr, "f"'] & \\ & W \end{tikzcd}$$

Podemos compor estes dois diagramas obtendo respectivamente

$$\begin{tikzcd} & W \arrow[dd, "\varphi_g \circ \varphi_f"] \\ V_1 \times \cdots \times V_n \arrow[ur, "f"] \arrow[dr, "f"'] & \\ & W \end{tikzcd} \qquad \begin{tikzcd} & W' \arrow[dd, "\varphi_f \circ \varphi_g"] \\ V_1 \times \cdots \times V_n \arrow[ur, "h"] \arrow[dr, "h"'] & \\ & W' \end{tikzcd}$$

que são comutativos como composição de diagramas comutativos. Além disso, as aplicações lineares $\varphi_g \circ \varphi_f$ e $\varphi_f \circ \varphi_g$ são únicas devido à propriedade (PT). Mas esses diagramas também são comutativos para as identidades id_W e $\mathrm{id}_{W'}$. Conseqüentemente, $\varphi_g \circ \varphi_f = \mathrm{id}_W$ e $\varphi_f \circ \varphi_g = \mathrm{id}_{W'}$, i.é, φ_f é isomorfismo e φ_g é sua inversa.

Um parêntese sobre a Teoria de Categorias

Um objeto P de uma categoria (cf. Lang [La, caps. I e XVI]) $\mathcal{C}$ é dito *universalmente atrativo* se existe um único morfismo de cada objeto de $\mathcal{C}$ em P, e é dito *universalmente repulsivo* se para cada objeto de $\mathcal{C}$ existe um único morfismo de P nesse objeto. Por exemplo, se I é um conjunto de índices, o produto direto da família módulos $\{M_i\}_{i\in I}$ é um objeto universalmente atrativo na categoria cujos objetos são os pares $(M, \{\pi_i\}_{i\in I})$ consistindo de um módulo M e da família de homorfismos $\{\pi_i : M \to M_i\}_{i\in I}$. A soma direta da família de módulos $\{M_i\}_{i\in I}$ é um objeto universalmente repulsivo na categoria cujos objetos são os pares $(M, \{\theta_i\}_{i\in I})$ consistindo do módulo M e da família de homorfismos $\{\theta_i : M_i \to M\}_{i\in I}$. Quando não houver risco de confusão estes objetos são chamados de *universais*. Observando que um objeto universal P admite a identidade como um morfismo em si próprio então, se P e P' são dois objetos universais em $\mathcal{C}$, há um único isomorfismo entre eles. A prova deste fato é análoga à que foi fornecida acima sobre a unicidade do par (W, f). Observamos que estamos fazendo um uso extremamente limitado do conceito de categoria. Esta tem um caráter extremamente universal, de modo que um alto grau de arbitrariedade pesa sobre seus objetos e seus morfismos (i.é, desde que estejam satisfeitos os axiomas que definem uma categoria). Podemos ter categorias cujos objetos são grupos e cujos morfismos são homomorfismos entre esses grupos, ou categorias cujos objetos são espaços topológicos e cujos morfismos são os homeomorfismos, para falar de exemplos mais comuns. Um leitor especialmente interessado poderá encontrar material abundante no clássico trabalho de MacLane [Ln]. $\square$

Desse modo, o par (W, f) é um objeto universal da categoria cujos objetos são os pares (U, g) consistindo de um módulo U e de uma aplicação n-linear g definida sobre os módulos fixados $V_1, \ldots, V_n$ em U. Um morfismo $(U, g) \mapsto (U', g')$ nesta categoria é uma aplicação linear $\varphi : U \to U'$ que torna comutativo o diagrama

$$\begin{tikzcd} & U \arrow[dd, "\varphi"] \\ V_1 \times \cdots \times V_n \arrow[ur, "g"] \arrow[dr, "g'"'] & \\ & U' \end{tikzcd}$$

Definição 144 *O par* (W, f) *é chamado de* produto tensorial, *e* W *é denotado por* $V_1 \otimes_F \cdots \otimes_F$

V_n.

Quando não há confusão, costuma-se abandonar o subscrito F na notação. Além disso, por abuso de linguagem, o módulo $V_1 \otimes \cdots \otimes V_n$ é chamado produto tensorial dos módulos $V_1, \ldots, V_n$.

Se $v_i \in V_i$, para $i = 1, \ldots, n$, denotamos o elemento $f(v_1, \ldots, v_n) \in V_1 \otimes \cdots \otimes V_n$ por $v_1 \otimes \cdots \otimes v_n$. É imediato da multilinearidade de f que tais elementos tenham as seguintes propriedades

$$v_1 \otimes \cdots \otimes (v_i + v_i') \otimes \cdots \otimes v_n = v_1 \otimes \cdots \otimes v_i \otimes \cdots \otimes v_n + v_1 \otimes \cdots \otimes v_i' \otimes \cdots \otimes v_n,$$
$$v_1 \otimes \cdots \otimes \lambda v_i \otimes \cdots \otimes v_n = \lambda(v_1 \otimes \cdots \otimes v_i \otimes \cdots \otimes v_n)$$

para todo v_i, $v_i' \in V_i$, $i = 1, \ldots, n$, e $\lambda \in F$.

Até agora não garantimos a existência do produto tensorial $(f, V_1 \otimes \cdots \otimes V_n)$. Felizmente, é possível construir um, e de maneira natural. Seja M o módulo livremente gerado pelo conjunto de todas as n-uplas $(v_1, \ldots, v_n) \in V_1 \times \cdots \times V_n$. Este é o conjunto de todas as cadeias finitas (i.é, somas formais finitas) de elementos de $V_1 \times \cdots \times V_n$. Consideremos o submódulo livre N de M gerado por todos os elementos de M dos tipos

$$\begin{gathered}(v_1, \ldots, v_i + v_i', \ldots, v_n) - (v_1, \ldots, v_i, \ldots, v_n) - (v_1, \ldots, v_i', \ldots, v_n),\\ (v_1, \ldots, \lambda v_i, \ldots, v_n) - \lambda(v_1, \ldots, v_i, \ldots, v_n)\end{gathered} \tag{A.1}$$

para todos os v_i, $v_i' \in V_i$, $i = 1, \ldots, n$, e $\lambda \in F$. Temos a inclusão natural $\theta : V_1 \times \cdots \times V_n \to M$, do conjunto de geradores no módulo gerado por eles, a saber,

$$\theta(x_1, \ldots, x_n) = (x_1, \ldots, x_n),$$

e também a projeção natural $\pi : V \to M/N$. A composição destas é uma transformação n-linear $f : V_1 \times \cdots \times V_n \to M/N$, pois π aplicada aos elementos (A.1) é nula.

Assim podemos afirmar que $(M/N, f)$ é um produto tensorial. De fato, se P é um módulo arbitrário e $g : V_1 \times \cdots \times V_n \to P$ é uma transformação n-linear, a definição de espaço vetorial livremente gerado por $V_1 \times \cdots \times V_n$ nos fornece uma transformação linear $\varphi : V \to M$ tornando comutativo o diagrama

$$\begin{tikzcd} & M \arrow[dd, "\varphi"] \\ V_1 \times \cdots \times V_n \arrow[ur, "\theta"] \arrow[dr, "g"'] & \\ & P \end{tikzcd}$$

Como g é n-linear,

$$\begin{aligned} &\varphi((v_1, \ldots, v_i + v_i', \ldots, v_n) - (v_1, \ldots, v_i, \ldots, v_n) - (v_1, \ldots, v_i', \ldots, v_n)) = \\ &= \varphi(\theta(v_1, \ldots, v_i + v_i', \ldots, v_n)) - \varphi(\theta(v_1, \ldots, v_i, \ldots, v_n)) - \varphi(\theta(v_1, \ldots, v_i', \ldots, v_n)) \\ &= g(v_1, \ldots, v_i + v_i', \ldots, v_n) - g(v_1, \ldots, v_i, \ldots, v_n) - g(v_1, \ldots, v_i', \ldots, v_n) = 0. \end{aligned}$$

Similarmente, $\varphi((v_1, \ldots, \lambda v_i, \ldots, v_n) - \lambda(v_1, \ldots, v, \ldots, v_n)) = 0$, donde φ deve ser nula em N. O Primeiro Teorema do Isomorfismo nos garante a existência de uma única transformação linear $g_* : M/N \to P$ tornando comutativo o diagrama

$$\begin{tikzcd} & M/N \arrow[dd, "g_*"] \\ V_1 \times \cdots \times V_n \arrow[ur, "f"] \arrow[dr, "g"'] & \\ & P \end{tikzcd}$$

o que conclui nossa afirmação.

Se $x \in M/N$, então existe um elemento x' em M tal que $\pi(x') = x$, já que a projeção natural é sobrejetora. Por sua vez, x' é uma soma formal de elementos geradores de M, isto é $x' = \sum_i \theta(x_i')$. Isto nos dá

$$x = \pi(\sum_i \theta(x_i')) = \sum_i (\pi \circ \theta)(x_i') = \sum_i f(x_i'),$$

donde M/N é gerado pela imagem de f. Com a notação introduzida acima, dizemos que $V_1 \otimes \cdots \otimes V_n$ é gerado pelos elementos da forma $v_1 \otimes \cdots \otimes v_n$, onde $v_i \in V_i$. Estes são chamados *geradores homogêneos*.

Vamos agora estabelecer propriedades importantes do produto tensorial.

Proposição 145 *Se V é um módulo sobre F então V, $F \otimes V$ e $V \otimes F$, são naturalmente* *isomorfos.*

Prova. Vamos mostrar que $F \otimes V \cong V$, pois o outro isomorfismo é análogo. Temos a ação $\alpha : F \times V \to V$ de F sobre o módulo V que é a multplicação por escalar $\alpha(\lambda, v) = \lambda v$, uma aplicação bilinear por definição. Ainda, a discussão acima nos dá uma transformação bilinear $f : F \times V \to F \otimes V$ tal que $f(\lambda, v) = \lambda \otimes v$. Obtemos da propriedade universal de $(F \otimes V, f)$ uma transformação linear $\varphi : F \otimes V \to V$ tal que $\varphi(\lambda \otimes v) = \varphi(\ f(\lambda, v)) = \alpha(\lambda, v) = \lambda v$. Por outro lado, temos a inclusão $\theta : V \to F \otimes V$ definida por $\theta(v) = 1 \otimes v$. Acontece, porém, que

$$(\varphi \circ \theta)(v) = \varphi(1 \otimes v) = 1v = v$$

e

$$(\theta \circ \varphi)(\lambda \otimes v) = \theta(\lambda v) = 1 \otimes \lambda v = \lambda \otimes v,$$

isto é, φ é isomorfismo com inversa θ. ∎

Esta proposição nos permite identificar $F \otimes V$ com $V \otimes F$ e este com V. Em termos de elementos, temos as identificações $\lambda \otimes v = v \otimes \lambda = \lambda v$. Também é muito útil a seguinte proposição.

Proposição 146 *Se V e W são módulos sobre F então $V \otimes W$ e $W \otimes V$ são naturalmente isomorfos.*

Prova. $V \times W$ e $W \times V$ são naturalmente isomorfos como módulos por meio da aplicação transposição τ (pág. 152) definida por $(v, w) \mapsto (w, v)$, a qual se estende por linearidade a um isomorfismo natural entre os módulos M e N livremente gerados por $V \times W$ e $W \times V$ respectivamente (através das inclusões). Este, por sua vez, induz um isomorfismo natural entre $V \otimes W$ e $W \otimes V$ por passagem ao quociente, que também chamado denominaremos transposição

τ. Apenas para ilustrar, temos o seguinte diagrama comutativo

$$\begin{array}{ccc} V \times W & \longrightarrow & W \times V \\ {\scriptstyle \mathrm{id} \otimes i_1}\downarrow & & \downarrow{\scriptstyle i_2} \\ M & \longrightarrow & N \\ {\scriptstyle \mathrm{id} \otimes \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_2} \\ V \otimes W & \xrightarrow{\tau} & W \otimes V \end{array}$$

Temos assim um isomorfismo $\tau : V \otimes W \to W \otimes V$ dado por $\tau(v \otimes w) = w \otimes v$. ∎

A aplicação transposição, tem um papel fundamental na teoria dos Grupos Quânticos, constituindo uma ferramenta básica para a construção de representações.

Suponhamos que $V_1, \ldots, V_n$ sejam módulos livres com respectivas bases $B_1, \ldots, B_n$. Consideremos W o módulo livremente gerado por $B_1 \times \cdots \times B_n$. Temos a inclusão natural $\theta : B_1 \times \cdots \times B_n \to W$, a qual se estende por (multi)linearidade a uma transformação n-linear $f' : V_1 \times \cdots \times V_n \to W$. Afirmamos que o par (f', W) é um produto tensorial. De fato, dado um módulo arbitrário U e uma transformação n-linear $g : V_1 \times \cdots \times V_n \to U$, a restrição g_0 de g ao conjunto $B_1 \times \cdots \times B_n$ determina, pela propriedade universal de W, uma única transformação linear $\varphi : W \to U$, tornando comutativo o diagrama

$$\begin{tikzcd} & W \arrow[dd, "\varphi"] \\ B_1 \times \cdots \times B_n \arrow[ur, "\theta"] \arrow[dr, "g_0"'] & \\ & U \end{tikzcd}$$

Agora, g é a única extensão (por linearidade) de g_0, assim como f' é a única extensão de θ ao módulo $V_1 \times \cdots \times V_n$, e conseqüentemente φ é a única transformação linear fazendo comutar o diagrama

$$\begin{tikzcd} & W \arrow[dd, "\varphi"] \\ V_1 \times \cdots \times V_n \arrow[ur, "f'"] \arrow[dr, "g"'] & \\ & U \end{tikzcd}$$

mostrando a afirmação. A unicidade do produto tensorial garante a existência de um isomorfismo $\chi : W \to V_1 \otimes \cdots \otimes V_n$ tal que

$$\begin{tikzcd}
 & W \arrow[d, "\chi"] \\
V_1 \times \cdots \times V_n \arrow[ur, "f'"] \arrow[r, "f"'] & V_1 \otimes \cdots \otimes V_n
\end{tikzcd}$$

seja comutativo. Para todo $(v_1, \ldots, v_n) \in B_1 \times \cdots \times B_n$, temos $v_1 \otimes \cdots \otimes v_n = f(v_1, \ldots, v_n) = (\chi \circ f')(v_1, \ldots, v_n) = (\chi \circ \theta)(v_1, \ldots, v_n)$. A imagem de θ é uma base para W e χ, sendo isomorfismo, leva toda base de W a uma base de $V_1 \otimes \cdots \otimes V_n$, mostrando que $B = \mathrm{Im}(\chi \circ \theta)$ é uma base para $V_1 \otimes \cdots \otimes V_n$. Resumindo, temos a seguinte

Proposição 147 *Se $B_1, \ldots, B_n$ são bases do módulos livres $V_1, \ldots, V_n$ respectivamente, então $B = \{v_1 \otimes \cdots \otimes v_n : v_i \in B_i\}$ é base de $V_1 \otimes \cdots \otimes V_n$.*

Assim, um elemento típico de $V_1 \otimes \cdots \otimes V_n$ é uma combinação linear finita de elementos da forma $v_1 \otimes \cdots \otimes v_n$, com $v_i \in B_i$. Em particular, se $V_1, \ldots, V_n$ têm posto finito, então o posto de $V_1 \otimes \cdots \otimes V_n$ é o produto dos respectivos postos de $V_1, \ldots, V_n$. Um caso especial é o de $V_i = M_{n_i}(F)$, as matrizes quadradas de ordem n_i com elementos em F, onde $n_i = \mathrm{rk}\, V_i$, $i = 1, 2$. Definimos uma transformação bilinear $f : V_1 \times V_2 \to M_{n_1 \times n_2}(F)$ por

$$f(A, B) = \begin{pmatrix} a_{11}B & \cdots & a_{1n_1}B \\ \vdots & & \vdots \\ a_{n_1 1}B & \cdots & a_{n_1 n_1}B \end{pmatrix}$$

onde pusemos $A = (a_{ij})$. Podemos mostrar por um cálculo direto que $(M_{n_1, n_2}(F), f)$ é um produto tensorial, i.é, $M_{n_1 \times n_2}(F) \cong V_1 \otimes V_2$.

Proposição 148 *Sejam $V_1, \ldots, V_n$ módulos sobre F. Então, para cada $i = 1, \ldots, n-1$, $(V_1 \otimes \cdots \otimes V_i) \otimes (V_{i+1} \otimes \cdots \otimes V_n)$ e $V_1 \otimes \cdots \otimes V_n$ são naturalmente isomorfos.*

Prova. Por comodidade sejam $V = V_1 \times \cdots \times V_i$, $W = V_{i+1} \times \cdots \times V_n$, $V' = V_1 \otimes \cdots \otimes V_i$ e $W' = V_{i+1} \otimes \cdots \otimes V_n$. Temos aplicações canônicas $f_1 : V \to V'$, $f_2 : W \to W'$ e $g : V \times W \to V \otimes W$.

$V \times W$ se identifica canonicamente com $V_1 \times \cdots \times V_n$ pela aplicação

$$((v_1, \ldots, v_i), (v_{i+1}, \ldots, v_n)) \mapsto (v_1, \ldots, v_n).$$

Usando esta identificação, definimos $h : V_1 \times \cdots \times V_n \to V' \otimes W'$, por

$$h(v_1, \ldots, v_n) = g(f_1(v_1, \ldots, v_i), f_2(v_{i+1}, \ldots, v_n)).$$

Afirmamos que $(V' \otimes W', h)$ é um produto tensorial e desse modo $V' \otimes W' \cong V_1 \otimes \cdots \otimes V_n$, como desejado.

De fato, dado um módulo arbitrário U e uma aplicação n-linear $\theta : V_1 \times \cdots \times V_n \to U$, h e θ podem ser vistas como aplicações definidas em $V \times W$, através da identificação acima. Neste caso, h coincide com g e, daí, a propriedade universal de $V \otimes W$ nos fornece uma única transformação linear $\varphi : V \otimes W \to U$ tal que $(\varphi \circ g) = \theta$. Por um argumento semelhante, temos $(\varphi \circ h) = \theta$, concluindo a prova ∎

Corolário 149 *Dados os módulos V_1, V_2, V_2, temos $(V_1 \otimes V_2) \otimes V_3 \cong V_1 \otimes (V_2 \otimes V_3)$.*

Exemplo 150 (Álgebra Tensorial) Seja V um módulo sobre F. Para cada $n \geq 0$ definimos

$$T^n(V) = \begin{cases} F & se \quad n = 0 \\ V & se \quad n = 1 \\ V \otimes \cdots \otimes V \ (n \ vezes) & se \quad n > 1 \end{cases}$$

e

$$T(V) = \bigoplus_{n=0}^{\infty} T^n(V).$$

Sabemos que $T^n(V)$ é um módulo gerado por todos os elementos da forma

$$v_1 \otimes \cdots \otimes v_n \tag{A.2}$$

para $v_i \in V \ \ (n > 0)$, e por $1 \in F \ \ (n = 0)$. Assim, $T(V)$ é gerada por 1 e por todas as cadeias finitas de elementos de V. Um elemento da forma (A.2) pertencente a $T(V)$ é chamado *tensor* *genérico.* Podemos definir aplicações de estrutura μ e η em $T(V)$ tais que $(T(V),\mu,\eta)$ seja uma álgebra associativa com unidade sobre F. A proposição acima nos garante que para todo n, $m \in \mathbb{N} \cup \{0\}$,

$$T^n(V) \otimes T^m(V) \cong T^{n+m}(V)$$

é um isomorfismo natural. Isto nos permite identificar ambos os espaços. Estes, por sua vez, encontram-se naturalmente contidos na soma direta $T(V)$, de modo que fica bem definida a aplicação $\mu : T(V) \otimes T(V) \to T(V)$ dada por

$$(v_1 \otimes \cdots \otimes v_n) \otimes (w_1 \otimes \cdots \otimes w_m) \mapsto v_1 \otimes \cdots \otimes v_n \otimes w_1 \otimes \cdots \otimes w_m,$$

onde $v_1 \otimes \cdots \otimes v_n$ e $w_1 \otimes \cdots \otimes w_m$ são elementos genéricos de $T(V)$. Note que esta aplicação é simplesmente a combinação dos isomorfismos acima. Ora, μ é claramente associativa como simples justaposição de elementos de $T(V)$ conectados pelo símbolo $\otimes$. Resta-nos apenas notar que a inclusão natural $F \hookrightarrow T(V)$ assume o papel da aplicação unidade η (agindo como identidade sobre F) e, portanto, em $T(V)$ temos uma estrutura de álgebra associativa com unidade.

Observamos que a álgebra $T(V)$ chamada *álgebra tensorial,* é graduada (cf. pág. 175) com graduação $T^n(V)$ e, em geral, é um módulo de posto infinito, mesmo quando V tem posto finito. Esta álgebra tem papel muito importante, pois seu carater de estrutura "universal" permite-nos obter uma série de outras álgebras derivadas desta por passagem ao quociente por ideais específicos de $T(V)$. Este é o caso da álgebra simetrica e álgebra exterior, introduzidas a seguir. □

A.1.8 Produtos Simétrico e Exterior

O conceito de aplicação multilinear visto acima permitiu a construção de um objeto muito importante denominado produto tensorial. Agora, veremos que uma especificação deste conceito, utilizando aplicações lineares simétricas e anti-siméticas, pode nos fornecer ainda outros tipos de objetos álgebricos muito úteis, definidos por meio de propriedade universal, e denominados produto simétrico e produto exterior respectivamente.

Produto Simétrico

Sejam V e W módulos sobre F. Denotamos $V \times \cdots \times V$ (n vezes) por V^n. Uma aplicação n-linear $f : V^n \to W$ é chamada simétrica quando $f \circ \sigma = f$, para toda permutação σ dos elementos $\{1, \ldots, n\}$. A notação $f \circ \sigma(v_1, \ldots, v_n)$ significa $f(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$, onde $v_i \in V$, para todo i. Se f é simétrica e $g : W \to U$ é linear, então claramente $g \circ f$ é simétrica. Novamente, isto nos conduz a indagação acerca da possibilidade de se construir todas as aplicações lineares simétricas desta maneira, isto é, como composição de uma aplicação linear simétrica "universal" com alguma transformação linear específica. Como veremos, a resposta é afirmativa, e está relacionada com o conceito de produto simétrico. Fixado o módulo V, seja $\mathcal{C}'$ a categoria cujos objetos são os pares (W, f), consistindo de um módulo W e de uma transformação linear simétrica $f : V^n \to W$, e cujos morfismos $(U, g) \mapsto (U', g')$ são os mesmos que já foram vistos no caso do produto tensorial. Um *produto simétrico* é simplesmente um objeto universal desta categoria, cuja existência vamos agora verificar. Seja $(T^n(V), g)$ um produto tensorial. No módulo $T^n(V)$, consideremos o submódulo $\mathfrak{a}_n$ gerado por todos os elementos da forma

$$v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$$

para toda permutação σ do conjunto $\{1, \ldots, n\}$, e todo $v_i \in V$. Seja $f = \pi \circ g$, onde π é a projeção natural $T^n(V) \to T^n(V)/\mathfrak{a}$. Por definição, f é uma aplicação linear simétrica. O par $(T^n(V)/\mathfrak{a}, f)$ é um produto simétrico. A prova desse fato é análoga à do produto tensorial. Denotamos $T^n(V)/\mathfrak{a}$ por $S^n(V)$. É fácil ver que $S^n(V)$ é gerada pela imagem de f cujos elementos são da forma $v_1 \otimes \cdots \otimes v_n + \mathfrak{a}$ para $v_i \in V$. Costuma-se denotar estes geradores homogêneos por simples justaposição tal como $v_1 \cdots v_n$.

Quando V é um módulo livre com base B, é natural indagar-se sobre a possibilidade de $S^n(V)$ ser também um módulo livre. Para isto, vamos definir em B^n a seguinte relação de equivalência: dizemos que as n-uplas $(v_1, \ldots, v_n)$ e $(w_1, \ldots, w_n)$ são equivalentes se

$$(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = (w_1, \ldots, w_n),$$

para alguma permutação σ do conjunto $\{1, \ldots, n\}$. Escolhemos um representante de cada uma das classes de de equivalência obtidas formando o conjunto denotado por $[B]$. Assim, podemos enunciar a seguinte proposição, cuja prova pode ser encontrada em Brown [Br, pág. 96].

Proposição 151 *Seja B uma base do módulo livre V. Então $\{v_1 \cdots v_n : (v_1, \ldots, v_n) \in [B]\}$ é uma base de $S_n(V)$.*

Corolário 152 *Se $\operatorname{rk} V = m$, então $\operatorname{rk} S^n(V) = \binom{m+n-1}{n}$.*

Exemplo 153 (Álgebra Simétrica) Seja V um módulo sobre F, e $T(V)$ a respectiva álgebra tensorial. Para cada n consideremos em $T_n(V)$ o submódulo $\mathfrak{a}_n$ gerado por todos elementos do tipo

$$v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$$

para toda permutação σ do conjunto $\{1, \ldots, n\}$. Definindo

$$\mathfrak{a} = \bigoplus_{n=0}^{\infty} \mathfrak{a}_n,$$

vemos que o submódulo $\mathfrak{a}$ é de fato um ideal em $T(V)$. Com isto, definimos a *álgebra simétrica* pondo

$$S(V) = \frac{T(V)}{\mathfrak{a}}.$$

Um elemento genérico de $S(V)$ é $v_1 \cdots v_p$, com $v_i \in V$. Sejam $x = v_1 \cdots v_p$ e $y = w_1 \cdots w_q$ elementos genéricos de $S(V)$. A multiplicação em $T(V)$ induz uma multiplicação em $S(V)$ dada por

$$\begin{aligned} xy &= (v_1 \otimes \cdots \otimes v_p + \mathfrak{a})(w_1 \otimes \cdots \otimes w_q + \mathfrak{a}) \\ &= v_1 \otimes \cdots \otimes v_p \otimes w_1 \otimes \cdots \otimes w_q + \mathfrak{a} = v_1 \cdots v_p w_1 \cdots w_q \end{aligned}$$

□

Observamos que $S(V)$ é naturalmente isomorfa à soma direta

$$\bigoplus_{n=0}^{\infty} S^n(V),$$

tornando $S(V)$ numa álgebra associativa graduada e comutativa com unidade.

Abstratamente, podemos dizer que $S(V)$ é a álgebra livremente gerada pelo conjunto $\{1\} \cup V$, com as relações

$$v_1 \cdots v_n = v_{\sigma(1)} \cdots v_{\sigma(n)}$$

para toda permutação σ do conjunto $\{1, \ldots, n\}$, todo $v_i \in V$, e todo $n \in \mathbb{N} \cup \{0\}$.

Consideremos a categoria $\mathcal{C}$ cujos objetos são os pares (A, ψ) consistindo de uma álgebra associativa A e de uma aplicação linear $\psi : V \to A$ satisfazendo $\psi(v)\psi(w) = \psi(w)\psi(v)$, para todo $v, w \in V$, e cujos morfismos $(A, \psi) \mapsto (A', \psi')$ são os homomorfismos de álgebras φ tornando comutativo os diagrama

$$\begin{tikzcd} & A \arrow[dd, "\varphi"] \\ V \arrow[ur, "\psi"] \arrow[dr, "\psi'"'] & \\ & A' \end{tikzcd}$$

A inclusão natural $\theta_0 : V \to T(V)$ induz uma outra inclusão natural $\theta : V \to S(V)$. Como $S(V)$ é uma álgebra comutativa temos obviamente $\theta(v)\theta(w) = \theta(w)\theta(v)$, para todo $v, w \in V$. Conseqüentemente o par $(S(V), \theta)$ pertence à categoria $\mathcal{C}$. Além disso, vale o seguinte resultado.

Proposição 154 *O par $(S(V), \theta)$ é um objeto universal na categoria $\mathcal{C}$.*

Prova. Precisamos mostrar que, dado um objeto arbitrário (A, ψ) de $\mathcal{C}$, existe um único morfismo de $(S(V), \theta)$ em (A, ψ).

Seja $\mathcal{C}'$ a categoria cujos objetos são os pares (A, ψ), consistindo de uma álgebra associativa A e de uma aplicação linear $\psi : V \to A$, e cujos morfismos são idênticos aos definidos para a categoria $\mathcal{C}$. Então, o par $(T(V), \theta_0)$ é um objeto universal em $\mathcal{C}'$, de modo que temos um único homomorfismo de álgebras $\varphi_0 : T(V) \to A$ tornando comutativo o diagrama

$$\begin{tikzcd} & T(V) \arrow[dd, "\varphi_0"] \\ V \arrow[ur, "\theta_0"] \arrow[dr, "\psi"'] & \\ & A \end{tikzcd}$$

Como $\psi(v)\psi(w) = \psi(w)\psi(v)$, temos

$$\begin{aligned}\varphi_0(v \otimes w - w \otimes v) &= \varphi_0(v)\varphi_0(w) - \varphi_0(w)\varphi_0(v) \\ &= \psi(v)\psi(w) - \psi(w)\psi(v) = 0,\end{aligned}$$

isto é, φ_0 se anula no ideal $\mathfrak{a}$ de $T(V)$. Conseqüentemente, φ_0 induz um homomorfismo de álgebras

$$\varphi : S(V) = T(V)/\mathfrak{a} \to A$$

tornando comutativo o diagrama

$$\begin{tikzcd} & S(V) \arrow[d, "\varphi"] \\ V \arrow[ur, "\theta"] \arrow[r, "\psi"'] & A \end{tikzcd}$$

A unicidade de φ é provada de modo idêntico à unicidade de φ_0. ∎

Dados os módulos V e W, com as definições e propriedades apresentadas aqui pode-se mostrar que $S(V \oplus W) \cong S(V) \otimes S(W)$ por meio da aplicação $(v, w) \mapsto v \otimes w$.

Produto Exterior

A definição e a construção do produto exterior de módulos é completamente análoga à que foi apresentada acima, para o produto simétrico. Recordamos que uma aplicação n-linear $f : V^n \to W$ é chamada anti-simétrica quando $f \circ \sigma = \varepsilon(\sigma)f$, para toda permutação σ dos elementos $\{1, \ldots, n\}$, onde $\varepsilon(\sigma) \in \{-1, 1\}$ é o sinal da permutação σ. Claramente, se f é anti-simétrica e $g : W \to U$ é linear, então $g \circ f$ é também anti-simétrica.

Fixado um módulo V sobre um corpo F, o *produto exterior* é simplesmente um objeto universal na categoria cujos objetos são os pares (W, f), consistindo de um módulo W sobre F e de uma transformação linear anti-simétrica $f : V^n \to W$, e cujos morfismos $(U, g) \mapsto (U', g')$ são os mesmos que já foram vistos no caso do produto tensorial.

Denota-se o n-ésimo produto exterior de V por $\Lambda^n V$. A construção explícita deste objeto segue os mesmos passos já descritos acima. Iniciamos com o produto tensorial $(T^n(V), g)$, onde consideramos o submódulo $\mathfrak{a}_n$ gerado por todos os elementos da forma

$$v_1 \otimes \cdots \otimes v_n - \varepsilon(\sigma) v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$$

para toda permutação σ do conjunto $\{1, \ldots, n\}$, e todo $v_i \in V$. Assim, a composição $f = \pi \circ g$, onde $\pi : T^n(V) \to T^n(V)/\mathfrak{a}$ é a projeção natural, é uma aplicação linear anti-simétrica. Com isto, o par $(T^n(V)/\mathfrak{a}, f)$ é um produto exterior, e $T^n(V)/\mathfrak{a}$ passa a ser denotado por $\Lambda^n V$. A imagem por f de um tensor homogêneo $v_1 \otimes \cdots \otimes v_n$, para $v_i \in V$, é denotada por $v_1 \wedge \cdots \wedge v_n$.

Como no caso do produto simétrico, podemos facilmente encontrar uma base e conhecer a dimensão do produto exterior, conforme enuncia o resultado abaixo. Se B é uma base do módulo livre V, formamos um conjunto $[B]$ recolhendo precisamente um elemento de cada classe de equivalência de B^n pela relação definida por

$$(v_1, \cdots, v_n) - \varepsilon(\sigma)(v_{\sigma(1)}, \cdots, v_{\sigma(n)})$$

onde σ são permutações do conjunto $\{1, \ldots, n\}$.

Proposição 155 *Seja B uma base do módulo livre V. Então $\{v_1 \wedge \cdots \wedge v_n : (v_1, \ldots, v_n) \in [B]\}$ é uma base de $S_n(V)$.*

Corolário 156 *Se $B = \{v_1, \ldots, v_m\}$, i.é,* $\operatorname{rk} V = m$, *então $\{v_{i_1} \wedge \cdots \wedge v_{i_n} : 1 \leq i_1 < \cdots < i_n \leq m\}$ é uma base de $\Lambda^n V$. Conseqüentemente,* $\operatorname{rk} \Lambda^n(V) = \binom{m}{n}$, *para $n \leq m$, e* $\operatorname{rk} \Lambda^n(V) = 0$, *para $n > m$.*

A.2 Dualidade de Espaços Vetoriais

A.2.1 Espaço Ortogonal

Definição 157 *Seja V um espaço vetorial sobre um corpo F.* $\operatorname{Hom}_F(V, F)$, *o espaço vetorial das formas lineares de V em F, é chamado* espaço dual *de V, denotado por V^*.*

Se V tem dimensão finita então $V^* \cong V$. Em particular, $\dim V = \dim V^*$, o que não vale em geral. Com efeito, tomando $V = \oplus_{i=1}^{\infty} F$, verificamos que $V^* = \operatorname{Hom}_F(\oplus_{i=1}^{\infty} F, F) \cong$

$\prod_{i=1}^{\infty} \mathrm{Hom}(F,F) \cong \prod_{i=1}^{\infty} F$. É fácil verificar que $\dim V^* = \dim \prod_{i=1}^{\infty} F > \dim V = \#\mathbb{N}$. Por outro lado, a inclusão natural

$$\begin{array}{rcl} V & \hookrightarrow & V^{**} \\ v & \mapsto & (f \mapsto f(v)) \end{array}$$

é isomorfismo quando V tem dimensão finita. Nesse caso, podemos identificar V a V^{**}.

Vejamos agora o conceito de *emparelhamento* de espaços vetoriais. Definimos uma aplicação

$$<,>: V^* \times V \to F$$

por $\langle f, v \rangle = f(v)$. Esta é claramente bilinear e satisfaz as condições:

i) Se $\langle f, v \rangle = 0$, $\forall f \in V^*$, então $v = 0$;

ii) Se $\langle f, v \rangle = 0$, $\forall v \in V$, então $f = 0$.

Uma forma bilinear que satisfazendo (i) e (ii) é dita ser *não-degenerada.*

Este conceito está relacionado ao de espaço vetorial ortogonal. Se W é um subconjunto de V, consideremos o subconjunto $W^\perp = \{f \in V^* : \langle f, W \rangle = 0\}$ de V^*. Em palavras, este é o subconjunto de todas as formas lineares de V^* que se anulam em W. Um cálculo direto permite-nos verificar que $W^\perp$ é de fato um subespaço de V^*. Este é denominado *espaço ortogonal* de W. Notemos que W não precisa ser subespaço.

Há uma definição similar para os subconjuntos U de V^*, a saber, $U^\perp = \{v \in V : \langle U, v \rangle = 0\}$. Decorre imediatamente da não-degenerecência do pareamento que $V^\perp = 0$ e $0^\perp = V^*$.

O seguinte teorema apresenta mais propriedades dos espaços ortogonais.

Teorema 158 *Sejam U e W ambos subconjuntos de V ou de V^*. Então,*

(a) $U \subseteq W \Rightarrow U^\perp \supseteq W^\perp$;

(b) $\langle U \rangle^\perp = U^\perp$;

(c) $(U \cup W)^\perp = U^\perp \cap W^\perp$;

(d) Se W for subespaço de V, então $\dim V = \dim W + \dim W^\perp$.

(e) $W \subseteq W^{\perp\perp}$. *Se W for subespaço de V então vale a igualdade.*

Prova. A prova dos ítens (a)-(d) e a primeira afirmação do item (e) é facilmente obtida por cálculo direto. Assim, vamos mostrar apenas a segunda afirmação do item (e). Isto equivale a mostrar que se $\left\langle W^{\perp}, v\right\rangle = 0$, então $v \in W$. Suponhamos que $v \notin W$. Então $V = W \oplus Fv \oplus E$, para algum subespaço E. Definimos $f \in V^*$ por $f(v) = 1$ e $f(W) = f(E) = 0$. Por definição, $f \in W^{\perp}$, mas $\langle f, v\rangle = 1 \neq 0$, contrariando a hipótese $\left\langle W^{\perp}, v\right\rangle = 0$. ■

Teorema 159 *Sejam V e W espaços vetoriais sobre F e sejam $X \subset V^*$, $Y \subset W^*$ subespaços. Considere $X \otimes Y \subset V^* \otimes W^* \subset (V \otimes W)^*$ através da inclusão natural. Então $(X \otimes Y)^{\perp} = (X^{\perp} \otimes W) + (V \otimes Y^{\perp})$.*

Prova. Definimos as aplicações

$$\begin{array}{rcl} \bar{f} : V & \to & X^* \\ \left\langle \bar{f}(v), x\right\rangle & = & \langle x, v\rangle \end{array} \qquad\qquad \begin{array}{rcl} \bar{g} : W & \to & Y^* \\ \langle \bar{g}(w), y\rangle & = & \langle y, w\rangle \end{array}$$

Claramente, temos $\ker \bar{f} = X^{\perp}$ e $\ker \bar{g} = Y^{\perp}$, logo $\bar{f}$ e $\bar{g}$ induzem aplicações lineares injetoras f e g tornando comutativos os diagramas:

$$\begin{tikzcd} V \arrow[rr, "\bar{f}"] \arrow[dr, "\pi_1"'] & & X^* \\ & V/X^{\perp} \arrow[ur, "f"'] & \end{tikzcd} \qquad\qquad \begin{tikzcd} W \arrow[rr, "\bar{g}"] \arrow[dr, "\pi_2"'] & & Y^* \\ & W/Y^{\perp} \arrow[ur, "g"'] & \end{tikzcd} \tag{A.3}$$

Assim, a composição

$$(V/X^{\perp}) \otimes (W/Y^{\perp}) \xrightarrow{f \otimes g} X^* \otimes Y^* \xrightarrow{\rho} (X \otimes Y)^*$$

é injetora.

A aplicação $T : V \otimes W \to (X \otimes Y)^*$ definida por $\langle T(v \otimes w), x \otimes y\rangle = \langle x \otimes y, v \otimes w\rangle = \langle x, v\rangle \langle y, w\rangle$ tem núcleo $(X \otimes Y)^{\perp}$, pois $T(v \otimes w) = 0 \Leftrightarrow \langle x \otimes y, v \otimes w\rangle = 0$, para todo $x \otimes y \in$

$X \otimes Y$, ou, equivalentemente, $v \otimes w \in (X \otimes Y)^{\perp}$. O diagrama

$$\begin{tikzcd}
V \otimes W \arrow[rr, "T"] \arrow[dr, "\pi_1 \otimes \pi_2"'] & & (X \otimes Y)^* \\
& (V/X^{\perp}) \otimes (W/Y^{\perp}) \arrow[ur, "\rho(f \otimes g)"'] &
\end{tikzcd}$$

é claramente comutativo, pois os diagramas (A.3) também o são. Finalmente, como $\rho(f \otimes g)$ é injetora, segue que

$$(X \otimes Y)^{\perp} = \ker T = \ker(\pi_1 \otimes \pi_2) = (X^{\perp} \otimes W) + (V \otimes Y^{\perp}).$$

$\blacksquare$

Apêndice B

Álgebra

B.1 Homomorfismos

Seja A um anel, e sejam M, N dois A-módulos à esquerda. Denotamos por $\mathrm{Hom}_A(M, N)$ o grupo aditivo de todos os homomorfismos de A-módulos de M em N.

A um homomorfismo de A-módulos $f : M \to N$ temos associados os seguintes conjuntos:

Definição 160 (Núcleo) *O* núcleo *de f é o A-submódulo* $\mathrm{Ker}\, f = \{m \in M : f(m) = 0\}$ *de M.*

Definição 161 (Imagem) *A* imagem *de f é o A-submódulo* $\mathrm{Im}\, f = \{f(m) : m \in M\} = f(M)$ *de N.*

Definição 162 (Conúcleo) *O* conúcleo *de f é o A-módulo* $\mathrm{Coker}\, f = N/f(M)$.

Uma seqüência de homomorfismos de A-módulos

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to \cdots \xrightarrow{f_{n-1}} M_n$$

é *exata em M_i* se $\mathrm{Ker}\, f_i = \mathrm{Im}\, f_{i-1}$, e a seqüência é dita *exata* se for exata em cada M_i, $2 \leq i \leq n-1$.

Uma *seqüência exata curta* é uma seqüência exata da forma

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0. \tag{B.1}$$

Equivalentemente, temos as condições: f é injetora, $\operatorname{Im} f = \operatorname{Ker} g$ e g é sobrejetora, isto é, vale o isomorfismo de A-módulos $\frac{M}{L} \cong N$.

A seqüência exata (B.1) cinde-se quando $f(L)$ é um somando direto de M.

Proposição 163 *Dada uma seqüência exata (B.1), são equivalentes:*

(a) A seqüência cinde-se.

(b) Existe $h \in \operatorname{Hom}_A(M, L)$ *tal que* $h \circ f$ *é um automorfismo de* L*.*

(c) Existe um $h' \in \operatorname{Hom}_A(N, M)$ *tal que* $g \circ h'$ *é um automorfismo de* N*.*

Um diagrama de A-módulos e A-homomorfismos

$$\begin{array}{ccc} L_1 & \xrightarrow{f_1} & L_2 \\ {\scriptstyle g_1}\downarrow & & \downarrow{\scriptstyle f_2} \\ M_1 & \xrightarrow{g_2} & M_2 \end{array}$$

é *comutativo* se $f_2 \circ f_1 = g_2 \circ g_1$.

Seja $f \in \operatorname{Hom}_A(M, N)$. Para cada A-módulo X, o homomorfismo f induz um homomorfismo aditivo

$$f^* : \operatorname{Hom}_A(N, X) \to \operatorname{Hom}_A(M, X),$$

definido por

$$f^*(g) = g \circ f, \text{ para todo } g \in \operatorname{Hom}_A(N, X).$$

Equivalentemente, a aplicação f^* pode ser definida pela seguinte condição: para cada $g \in \operatorname{Hom}_A(N, X)$, o diagrama

$$\begin{tikzcd} & N \arrow[d, "g"] \\ M \arrow[ur, "f"] \arrow[r, "f^*(g)"'] & X \end{tikzcd}$$

é comutativo. Neste caso, verifica-se facilmente que $(g \circ f)^* = f^* \circ g^*$.

Agora, sejam f e X como acima. Então F induz um homomorfismo aditivo

$$f_* : \operatorname{Hom}_A(X, M) \to \operatorname{Hom}_A(X, N),$$

definido por

$$f_*(g) = f \circ g, \text{ para todo } g \in \mathrm{Hom}_A(X, M).$$

Equivalentemente, a aplicação f_* é definida pela codição que, para cada $g \in \mathrm{Hom}_A(X, M)$, o diagrama

$$\begin{tikzcd} X \arrow[d, "g"'] \arrow[dr, "f_*(g)"] & \\ M \arrow[r, "f"'] & N \end{tikzcd}$$

seja comutativo.

B.2 Álgebras Filtradas e Álgebras Graduadas

Seja F um anel comutativo com unidade e A uma álgebra associativa com unidade sobre F. Se uma família de submódulos $\{A_i : i = 0, 1, \ldots\}$ de A satisfaz as condições:

1. $1_A \in A_0 \subset A_1 \subset A_2 \subset \cdots$,

2. $A_i A_j \subset A_{i+j}$,

3. $\cup_{i=0}^{\infty} A_i = A$,

então A é dita uma *álgebra filtrada*, e a família $\{A_i : i = 0, 1, \ldots\}$ é dita uma *filtração* sobre A.

Se uma família de submódulos $\{A_i : i = 0, 1, \ldots\}$ de A satisfaz as condições

1. $A_i A_j \subset A_{i+j}$,

2. $A = \oplus_{i=0}^{\infty} A_i$,

então A é dita uma *álgebra graduada*.

Se A e B forem duas álgebras filtradas, com respectivas filtrações $\{A_i : i = 0, 1, \ldots\}$ e $\{B_i : i = 0, 1, \ldots\}$, e $f : A \to B$ for um homomorfismo de álgebras tal que $f(A_i) \subseteq B_i$, i.é, se f conserva a filtração, então f é dito um *homomorfismo de álgebras filtradas*. Analogamente, se A e B forem álgebras graduadas e f for um homorfismo entre A e B preservando a graduação, então f é dito *homorfismo de álgebras graduadas*.

Seja $\{A_i : i = 0, 1, \ldots\}$ uma filtração sobre uma álgebra filtrada A. Definimos $B_0 = A_0$, $B_i = A_i/A_{i-1}$, $i = 1, 2, \ldots$ e $B = \oplus_{i=0}^{\infty} B_i$. Sejam $\pi_i : A_i \to B_i$ as projeções canônicas e $\mu_{ij} : B_i \times B_j \to B_{i+j}$ aplicações definidas por

$$\mu_{ij}(\pi_i(x), \pi_j(y)) = \pi_{i+j}(xy), \quad x \in B_i, \quad y \in B_j.$$

Um cálculo direto permite-nos verificar que μ_{ij} são aplicações bilineares, para todo $i, j = 0, 1, 2, \ldots$, e que, assim, induzem aplicações lineares

$$\mu_{ij} : B_i \otimes B_j \to B_{i+j}.$$

Agora, se $x = \sum_{i=0}^{\infty} \pi_i(x_i)$ e $y = \sum_{j=0}^{\infty} \pi_j(y_j)$ (somas finitas), então podemos definir

$$\mu(x \otimes y) = \sum_{i,j=0}^{\infty} \mu_{ij}(\pi_i(x_i), \pi_j(y_j)) = \sum_{i,j=0}^{\infty} \pi_{i+j}(x_i y_j).$$

Esta é um homomorfismo de espaços vetoriais $\mu : B \otimes B \to B$ tal que $\mu(\mu \otimes \mathrm{id}) = \mu(\mathrm{id} \otimes \mu)$, i.é μ define uma multiplicação associativa em B. Ainda, definimos uma aplicação $\eta : F \to B$ por $\eta(\lambda) = \lambda 1_A$. Temos $\mu(\eta \otimes \mathrm{id})(\lambda \otimes a) = \mu(\lambda 1_A \otimes a) = \lambda a = \lambda \otimes a = \mu(\mathrm{id} \otimes \eta)(\lambda \otimes a)$. Com isto (B, μ, η) é uma álgebra associativa graduada com unidade.

Apêndice C

Representações de Grupos Finitos

Neste apêndice forneceremos as definições básicas e alguns resultados elementares da Teoria das Representações dos grupos finitos.

C.1 Definição e exemplos

Nesta seção, G denota um grupo, F um corpo e V um espaço vetorial sobre F, todos arbitrários.

Definição 164 (Ação de Grupo) *Uma* ação *do grupo G sobre V é uma aplicação*

$$\varphi : G \times V \to V$$

satisfazendo as condições:

1. $\varphi(e, v) = v$,
2. $\varphi(gh, v) = \varphi(g, \varphi(h, v))$, $\forall g, h \in G$,

para todo $v \in V$, onde $e \in G$ é o elemento neutro da operação binária interna de G.

Costuma-se denotar $\varphi(g, v)$ simplesmente por $g \cdot v$.

Definição 165 (Representação de Grupo) *Uma* representação *do grupo G sobre V é um homomorfismo $\rho : G \to \mathrm{GL}(V)$ de G no grupo dos automorfismos de V.*

Verificamos que as definições acima são "equivalentes". De fato, se φ é uma ação de G sobre V, então para cada $g \in G$, a aplicação $v \mapsto g \cdot v$ define um endomorfismo ρ_g de V. Desse modo, a aplicação $\rho : G \to \mathrm{GL}(V)$, definida por $g \mapsto \rho_g$, define uma representação de grupo. Por outro lado, se ρ é uma representação do grupo G sobre V, então a aplicação $\varphi : G \times V \to V$, definida por $(g, v) \mapsto \rho(g)(v)$ define uma ação de G sobre V. Em vista dessa equivalência, escrevemos também $g \cdot v$ para denotar $\rho(g)(v)$.

Não havendo confusão, costuma-se dizer que V é um *G-módulo*, ou ainda, dizer (por abuso de linguagem) que V é uma representação.

Um *homomorfismo de representações* (ou *homomorfismo de G-módulos*) é uma aplicação linear $\varphi : V \to W$ tornando comutativo o diagrama

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ V & \xrightarrow{\varphi} & W \end{array}$$

para todo $g \in G$. Equivalentemente, $\varphi(g \cdot v) = g \cdot \varphi(v)$, $\forall g \in G$ e $\forall v \in V$. Também dizemos que φ é uma aplicação *G-linear*, para distinguir φ de uma aplicação linear ordinária.

Uma *sub-representação* (G-submódulo) é um subespaço W de V estável sob a ação de G, isto é, temos

$$G \cdot W = \{g \cdot w : \forall g \in G \text{ e } \forall w \in W\} \subset W.$$

Uma representação $V \neq 0$ que admite apenas as sub-representações triviais 0 e V é chamada *irredutível*.

Definimos o *núcleo*, a *imagem* e o *conúcleo* de φ por $\operatorname{Ker}\varphi = \{v \in V : \varphi(v) = 0\}$, $\operatorname{Im}\varphi = \varphi(V)$, e $\operatorname{Coker}\varphi = W/\operatorname{Im}\varphi$, respectivamente. Estes são claramente sub-representações de G.

Se $\{V_i\}_{i\in I}$ é uma família de representações de G então o produto direto $\prod_{i\in I} V_i$, a soma direta $\bigoplus_{i\in I} V_i$ e o produto tensorial $\bigotimes_{i\in I} V_i$ são representações de G com ação dada respectivamente por $g \cdot \prod_{i\in I} v_i = \prod_{i\in I} g \cdot v_i$, $g \cdot \bigoplus_{i\in I} v_i = \bigoplus_{i\in I} v_i$, e $g \cdot \bigotimes_{i\in I} v_i = \bigotimes_{i\in I} g \cdot v_i$. Particularmente, a n-ésima potência tensorial $V^{\otimes n} = \underbrace{V \otimes \cdots \otimes V}_{n \text{ vezes}}$ de uma representação V e o quociente V/W por uma sub-representação W de V são ainda representações de G. Conseqüentemente, o produto simétrico $S^n(V)$ e o produto exterior $\Lambda^n(V)$ são representações de G assim como as álgebras tensorial $T(V)$, simétrica $S(V)$ e exterior $\Lambda(V)$.

Menos óbvio é o caso do espaço dual V^*. É útil definir a representação V^* de modo a conservar o emparelhamento natural entre V^* e V, isto é, para todo $g \in G$, $f \in V^*$ e $v \in V$, desejamos que

$$\langle g \cdot f, g \cdot v \rangle = \langle f, v \rangle \,,$$

onde, por definição, $\langle f, v \rangle = f(v)$. Isto nos sugere definir a representação dual por

$$(g \cdot f)(v) = f(g^{-1} \cdot v).$$

Agora, se V e W são representações de dimensão finita, então $\mathrm{Hom}(V, W)$ é uma representação. Basta fazer a identificação $\mathrm{Hom}(V, W) = V^* \otimes W$. Desse modo, se $f \in \mathrm{Hom}(V, W)$, e $g \in G$, então

$$(g \cdot f)(v) = g \cdot f(g^{-1} \cdot v).$$

Posto isso, se $f \in \mathrm{Hom}(V, W)$ é G-linear, então para todo $g \in G$ e todo $v \in V$ vem que

$$f(v) = e \cdot f(v) = g \cdot g^{-1} \cdot f(v) = g \cdot f(g^{-1} \cdot v) = (g \cdot f)(v),$$

i.é, f é fixada pela ação de G sobre $\mathrm{Hom}(V, W)$. O conjunto $\mathrm{Hom}(V, W)^G$ destas é claramente um subespaço de $\mathrm{Hom}(V, W)$. Reciprocamente, se $f \in \mathrm{Hom}(V, W)$ é fixada pela ação de G então

$$f(g \cdot v) = (g \cdot f)(g \cdot v) = g \cdot f(g^{-1} \cdot g \cdot v) = g \cdot f(v),$$

i.é, f é G-linear. Assim, temos mostrado o seguinte resultado.

Proposição 166 *O espaço vetorial* $\mathrm{Hom}(V, W)^G$ *das aplicações G-lineares entre representações V e W é exatamente o subespaço de* $\mathrm{Hom}(V, W)$ *estável sob a ação de G.*

C.2 Redutibilidade Completa

Na seção anterior, vimos que é possível construir novas representações a partir de operações algébricas lineares sobre representações dadas, a saber, fazendo produtos, somas diretas e produtos tensoriais. Nesta seção, estabeleceremos um resultado que simplifica a tarefa de se classificar as representações de um grupo finito (ou compacto) G. Vamos precisar também que F seja um corpo de característica 0.

Especificamente, procuramos uma maneira de reescrever uma representação como uma soma direta de sub-representações, de maneira que, cada sub-representação não possa mais ser assim fracionada. As sub-representações com essa propriedade chamam-se *simples*. Acontece, porém, que estas correspondem exatamente às representações irredutíveis e, como veremos, toda representação se escreve "unicamente" como uma soma direta de sub-representações irredutíveis. Iniciamos com o enunciado do seguinte resultado, cuja demonstração pode ser encontrada em Fulton [FH].

Proposição 167 *Se W é uma sub-representação de uma representação V de um grupo G, então existe um subespaço complementar invariante W' tal que $V = W \oplus W'$.*

Corolário 168 (Redutibilidade completa) *Qualquer representação pode ser escrita como soma direta de sub-representações irredutíveis.*

O estudo da redutibilade completa para o caso em que o corpo F tem característica positiva constitui o objeto de estudo da *Teoria das Representações Modulares.*

Lema 169 (Schur) *Se V e W são representações irredutíveis de G, então toda aplicação G-linear $\varphi : V \to W$ é isomorfismo ou é identicamente nula. Além disso, se $V = W$, e F é algebricamente fechado, então φ age diagonalmente (com alguma constante $\lambda \in F$) sobre V.*

Prova. Basta notar que $\operatorname{Ker}\varphi$ e $\operatorname{Im}\varphi$ são sub-representações de V e W respectivamente. A segunda afirmação decorre do fato que $\varphi - \lambda I$ deve ter núcleo não-nulo para algum autovalor λ de φ. ∎

Vamos agora enunciar o resultado mais importante desta seção.

Proposição 170 *Se V é uma representação arbitrária de um grupo G, então*

$$V = V_1^{\oplus n_1} \oplus \cdots \oplus V_k^{\oplus n_k},$$

onde cada V_i é uma sub-representação distinta e irredutíveis de V. Ademais, tal decomposição de V é única (a menos da ordem dos fatores), assim como é único cada fator V_i e cada multiplicidade n_i que nela ocorre.

Prova. Se W é qualquer representação de G com decomposição $W_1^{\oplus m_1} \oplus \cdots \oplus W_j^{\oplus m_j}$, e $\varphi : V \to W$ é G-linear, o lema de Schur nos assegura que φ leva cada V_i isomorficamente sobre algum $W_{\sigma(i)}$, onde σ é alguma permutação de grupo simétrico S_j dos números $\{1, \ldots, j\}$, e conseqüentemente cada fator $V^{\oplus n_i}$ no respectivo fator $W^{\oplus m_{\sigma(i)}}$, donde $m_{\sigma(i)} \geqslant n_i$. Aplicando este resultado à aplicação G-linear $\mathrm{id} : V \to V$, obtemos $j = k$, $m_{\sigma(i)} = n_i$ e a unicidade afirmada segue-se. ∎

Bibliografia

[A] Eiichi Abe, *Hopf Algebras*, Cambridge Tracts in Mathematics 74, Cambridge University Press, Cambridge UK, 1980.

[BK] Joseph Bernstein & Tanya Khovanova, *On the Quantum Group $SL_q(2)$*, Communications in Mathematical Physics 177, 691-708, 1996.

[Bo] N. Bourbaki, *Groupes et algèbres de Lie*, Chap. 1, Hermann, Paris, 1960.

[Br] William C. Brown, *A Second Course in Linear Algebra*, John Wiley & Sons, New York, 1988.

[CC] C. Casacuberta & M. Castellet, *Mathematical Research Today And Tomorrow*, Lect. Notes in Math. 1525, Springer-Verlag, New York, 1992.

[CP] Vyjayanthi Chari & Andrew Pressley, *A Guide to Quantum Groups*, Cambridge University Press, Cambridge UK, 1995.

[CR] Charles W. Curtis & Irving Reiner, *Methods of Representation Theory*, Wiley Classics Library Edition, John Wiley & Sons, New York, 1990.

[D] V. G. Drinfeld, *Quantum Groups*, Proceedings of the International Conference on Mathematics, Berkeley, 798-820, 1986.

[FRT] L. Fadeev, N. Reshetikhin & L. Takhatajan, *Quantization of Lie Groups and Lie Algebras*, in *Algebraic Analysis*, Vol. 1, 129-139, M. Kashiwara & T. Kawai (eds.), Academic Press, New York, 1988.

[FK] Jürg Fröhlich & Thomas Kerler, *Quantum Groups, Quantum Categories and Quantum Field Theory*, Lect. Notes in Math. 1542, Springer-Verlag, Berlin, 1993

[FH] William Fulton & Joe Harris, *Representation Theory*, Readings in Math, Springer-Verlag, New York, 1991.

[G] A. Guichardet, *Introduction aux Groupes Quantiques (point de vue formel)*, Notas de Aula, École Polytechnique, 1992.

[HK] Kenneth Hoffman & Ray Kunze, *Álgebra Linear*, EDUSP, São Paulo, 1961.

[Hu] James E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.

[IT] Mikio Ise & Masaru Takeuchi, *Lie Groups I and II*, Trans. Math. Monographs 85, 1991.

[Ja] Nathan Jacobson, *Lie Algebras*, Dover Publications, New York, 1979.

[FQ] Arthur Jaffe & Frank Quinn, *Theoretical Mathematics: toward a cultural synthesis of mathematics and theoretical physics*, Bull. of the AMS 29, 1-13, 1993.

[Ji1] Michio Jimbo, *A q-Difference Analogue of* $U(\mathfrak{g})$ *and the Yang-Baxter Equation*, Letters in Mathematical Physics 10, 63-69, 1985.

[Ji2] Michio Jimbo, *A q-Analogue of* $U(\mathfrak{gl}(N+1))$*, Heche Algebra, and the Yang-Baxter Equation*, Letters in Mathematical Physics 11, 247-252, 1986.

[Ji3] Michio Jimbo, *Yang-Baxter Equations in Integrable Systems*, Advanced Series in Mathematics 10, World Scientific, Singapore 1989.

[K] P. P. Kulish, *Quantum Groups*, Lect. Notes in Math. 1510, Springer-Verlag, New York, 1992. Translation of the Proceedings of Workshops in the Euler International Mathematical Institute, Leningrad, 1990.

[La] Serge Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1972.

[Ln] Saunders Mac Lane, *Categories for the Working Matematician*, Springer-Verlag, New York, 1988.

[Lu] George Lusztig, *Introduction to Quantum Groups*, Birkhäuser, Boston, 1993.

[Ma] Shahn Majid, *Quasitriangular Hopf Algebras and Yang-Baxter Equations*, Intl. Journal of Modern Physics 5, 1-91, 1990.

[Ms] Tetsuya Masuda et al, *Representations of the Quantum Group $SU_q(2)$ and the Little q-Jacobi Polynomials*, Journal of Functional Analysis 99, 357-386, 1991.

[Re1] N. Reshetikhin et al, *Quantization of Lie Groups and Lie Algebras*, Leningrad Math. Journal, Vol. 1, No. 1, 193-225, 1990.

[Re2] N. Reshetikhin, *Quasitriangularity of Quantum Groups at Roots of* 1, Communications in Mathematical Physics, 1995.

[RT] N. Reshetikhin & V. G. Turaeev, *Invariants of 3-manifolds via link polynomials and quantum groups*, Invent. Math. 103, 547-597, 1991.

[RA] Philippe Roche & D. Arnaudon, *Irreducible Representations of the Quantum Analogue of $SU(2)$*, Letters in Mathematical Physics 17, 295-300, 1989.

[Ro1] Philippe Roche, *Structures Algébriques liées à des modèles de méchanique statistique bidimensionnels*, Thèse de Doctorat, École Polytechnique, Paris, 1991.

[Ro2] Philippe Roche, *Introduction to Quantum Groups and Applications to Mathematical Physics*, Notas de Aula, Curso de Verão, ICMSC-USP, São Carlos, 1994.

[Rs1] Marc Rosso, *Comparaision des groupes de Drinfeld et de Woronowicz*, C. R. Acad. Sci. Paris 304, 323-326, 1987.

[Rs2] Marc Rosso, *Finite Dimensional Representations of the Quantum Analogue of the Enveloping Algebra of a Complex Lie Algebra*, Communications in Mathematical Physics 117, 581-593, 1988.

[Sc] Rudolf Schmid, *Strings, Knots and Quantum Groups: a glimpse at three 1990 fields medalists*, Soc. for Industrial and Applied Math. 34, 406-425, 1992.

[Se] Jean-Pierre Serre, *Lie Algebras and Lie Groups*, W. A. Benjamin Inc, New York, 1965.

[Sm] S. P. Smith, *Quantum Groups: An Introduction and Survey for Ring Theorists*, in Noncomutative rings, S. Montgomery & L. W. Small (eds), Mathematical Sciences Research Institute Publications 24, 131-178, Springer-Verlag, Berlin, 1992.

[Sw] Moss E. Sweedler, *Hopf Algebras*, W. A. Benjamin Inc, New York, 1969.

[Wi] Edward Witten, *Quantum Field Theory and The Jones Polynomials*, Comm. Math. Physics 121, 351-399, 1989.

[Wy] Brian G. Wybourne, *Classical Groups for Physicists*, John Wiley & Sons, New York, 1974.