UNIVERSIDADE FEDERAL DE MINAS GERAIS

MESTRADO EM MATEMÃTICA

Problema do isomorfismo para álgebras envolventes universais de álgebras de Lie

Danilo Vilela Avelar

Belo Horizonte - MG

2014

Danilo Vilela Avelar

Problema do isomorfismo para álgebras envolventes universais de álgebras de Lie

Dissertação submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática da UFMG, como requisito parcial para a obtenção do título de mestre em Matemática.

Orientador: Csaba Schneider
Coorientadora: Viviane Ribeiro Tomaz da Silva

Universidade Federal de Minas Gerais
06 de Agosto de 2014

Resumo

Sejam L e H duas álgebras de Lie e U_L e U_H suas respectivas envolventes universais. O problema do isomorfismo para álgebras envolventes universais de álgebras de Lie consiste em estudar sob quais condições o isomorfismo entre U_L e U_H implica no isomorfismo entre L e H. Nesta dissertação, faremos o estudo para álgebras de Lie simples de dimensão 3 e para álgebras de Lie nilpotentes de dimensão finita, baseado nos artigos [Mal92] de Malcolmson e [RU07] de Riley e Usefi. A fim de estudarmos o artigo [Mal92], iremos estudar as álgebras dos quatérnios, baseado no artigo [Lew06] de David W. Lewis e na dissertação de mestrado [Sha08] de Zi Yang Sham. Iremos caracterizar as álgebras dos quatérnios sobre corpos específicos, a fim de adquirir uma caracterização para as álgebras de Lie simples de dimensão 3. Além disso, mostraremos que o isomorfismo entre as envolventes universais de duas álgebras de Lie simples de dimensão 3 acontece se, e somente se, as álgebras de Lie são isomorfas. Mostraremos ainda, baseado no artigo [RU07], que a envolvente universal de uma álgebra de Lie de dimensão finita determina se a álgebra de Lie é ou não nilpotente e, no caso de ela ser nilpotente, determina também o grau de nilpotência e o número mínimo de geradores da álgebra de Lie.

Abstract

Let L and H be two Lie algebras and U_L and U_H be their respective universal enveloping algebras. The isomorphism problem for universal enveloping algebras of Lie algebras asks us to determine under what conditions the isomorphism between U_L and U_H implies the isomorphism between L and H. In this dissertation, we will investigate this problem in the context of three-dimensional simple Lie algebras and finite-dimensional nilpotent Lie algebras, based on the articles of Malcolmson [Mal92] and of Riley and Usefi [RU07]. In order to present a detailed proof of the main result of Malcolmson [Mal92], we will describe the class of quaternion algebras, based on the article [Lew06] of David W. Lewis and on masters dissertation [Sha08] of Zi Yang Sham. We will characterize the quaternion algebras over specific fields, in order to obtain a characterization of three-dimensional simple Lie algebras. Moreover, we will show that isomorphism between universal enveloping algebras of two three-dimensional simple Lie algebras occurs if and only if the Lie algebras are isomorphic. We will also show, based on the article [RU07], that the isomorphism type of the universal enveloping algebra of a finite-dimensional Lie algebra determines whether or not the Lie algebra is nilpotent and, in case it is, it also determines the nilpotency class and the minimal number of generators of the Lie algebra.

Sumário

Introdução

Em 1900, Henri Poincaré, no artigo [Poi00], introduziu o conceito de álgebra envolvente universal para uma álgebra de Lie e provou o teorema hoje conhecido como Teorema de Poincaré-Birkhoff-Witt. Entretanto, esse teorema era antes conhecido apenas como Teorema de Birkhoff-Witt, devido aos trabalhos de Birkhoff [Bir37] e Witt [Wit37] que, em 1937, de maneira independente, formularam e provaram versões desse teorema. No artigo [TTT99] de Thai-Duong Tran e Tuong Ton-That, os autores fazem uma detalhada discussão da demonstração do teorema dada por Poincaré trinta e sete anos antes dos trabalhos de Birkhoff e Witt. Em 1978, Bergman, em seu trabalho [Ber78], mostra uma aplicação do Lema do Diamante, provando o Teorema de Poincaré-Birkhoff-Witt. Ainda em seu trabalho, ele comenta que, dadas duas álgebras de Lie cujas envolventes universais são isomorfas, é um problema em aberto se isso implica no isomorfismo entre as álgebras de Lie. Esse problema é conhecido como o problema do isomorfismo para álgebras envolventes universais de álgebras de Lie, e será o foco deste nosso trabalho.

Hoje é conhecido que nem sempre o isomorfismo entre álgebras envolventes universais implica no isomorfismo entre suas respesctivas álgebras de Lie, porém sabemos que, no caso de álgebras de Lie de dimensão pequena, como por exemplo álgebras de Lie de dimensão três, se duas envolventes universais de duas álgebras de Lie de dimensão três são isomorfas, então as álgebras de Lie também são isomorfas. Mais precisamente, Malcolmson, em 1992 no artigo [Mal92], mostrou que, para o caso de álgebras de Lie simples de dimensão três, o isomorfismo entre as envolventes universais garante o isomorfismo entre as álgebras de Lie. Mais tarde, no ano de 2004, Jang-Ho Chun, Takeshi Kajiwara e Jong-Sook Lee provam no artigo [CKL04] um resultado geral para álgebras de Lie de dimensão três. Eles mostraram que sempre que estivermos trabalhando com álgebras de Lie de dimensão três, o isomorfismo entre suas envolventes universais implica no isomorfismo entre as álgebras de Lie.

Em 2007, David Riley e Hamid Usefi trabalharam, em seu artigo [RU07], quais características uma álgebra de Lie herda de sua envolvente universal. Eles mostraram que o fato de uma álgebra de Lie ser ou não nilpotente é determinado por sua envolvente universal, isto é, dadas duas álgebras de Lie cujas envolventes universais são isomorfas, então, se uma das álgebras

de Lie for nilpotente, a outra também será. Ainda nesse artigo, eles mostraram que, quando a álgebra de Lie é nilpotente, o seu grau de nilpotência e o seu número mínimo de geradores também são determinados pela envolvente universal. Outro resultado importante mostrado por eles é que a álgebra graduada associada à série central descendente de uma álgebra de Lie é determinada pela envolvente universal da álgebra de Lie, isto é, dadas duas álgebras de Lie com envolventes universais isomorfas, então suas álgebras graduadas também são isomorfas.

Uma continuação natural ao estudo do problema do isomorfismo para álgebras envolventes universais de álgebras de Lie é o estudo sobre as álgebras de Lie restritas. Hamid Usefi, no ano de 2010, mostrou no artigo [Use10], entre outros interessantes resultados, que as álgebras de Lie restritas abelianas sobre um corpo algebricamente fechado são determinadas pela sua envolvente universal, ou seja, dadas duas álgebras de Lie restritas abelianas sobre um corpo algebricamente fechado cujas envolventes universais são isomorfas, então as álgebras de Lie também são isomorfas.

Para o caso de álgebras de Lie nilpotentes, Csaba Schneider e Hamid Usefi, no ano de 2011, fizeram em seu trabalho [SU11] um estudo sobre as álgebras de Lie nilpotentes de dimensão no máximo seis sobre um corpo de característica diferente de dois. Eles mostraram que sobre um corpo de característica maior ou igual a cinco ou igual a zero o tipo de isomorfismo de uma álgebra de Lie nessas condições é determinado pelo tipo do isomorfismo de sua álgebra envolvente universal. Os exemplos tratados no artigo mostram que a restrição sobre a característica do corpo é necessária.

Nesta dissertação, temos como foco estudar o problema do isomorfismo para álgebras envolventes universais de álgebras de Lie simples de dimensão três e álgebras de Lie nilpotentes de dimensão finita. Com esse intuito, trabalharemos os artigos [Mal92] e [RU07].

A fim de trabalharmos o artigo [Mal92], faremos, no Capítulo 3, um estudo sobre as álgebras dos quatérnios, que são exemplos de álgebras associativas de dimensão quatro. Nessa parte da dissertação, usaremos como referência o artigo [Lew06] de David W. Lewis e a dissertação de mestrado [Sha08] de Zi Yang Sham. Mostraremos que as álgebras dos quatérnios são álgebras centrais simples e, assim, podemos obter, através do conhecido Teorema de Wedderburn-Artin, que as álgebras dos quatérnios ou são álgebras de divisão ou são isomorfas a uma álgebra de matrizes dois por dois. Nossa motivação para o estudo das álgebras dos quatérnios está, sobretudo, no fato de que elas possuem um subespaço de dimensão três que pode ser visto como uma álgebra de Lie e, conforme veremos, toda álgebra de Lie simples de dimensão três é isomorfa a essa subálgebra de Lie para alguma álgebra dos quatérnios. Como consequência desse resultado temos que, mediante uma caracterização das álgebras dos quatérnios, é possível caracterizar as álgebras de Lie simples de dimensão três. Mais precisamente, mostraremos que, a menos de isomorfismo, existem duas álgebras dos quatérnios sobre os reais não isomorfas e apenas uma

álgebra dos quatérnios tanto sobre os complexos como sobre um corpo finito, enquanto que sobre os racionais existem infinitas álgebras dos quatérnios não isomorfas. Consequentemente, temos que sobre os reais existem duas álgebras de Lie simples de dimensão três não isomorfas; sobre os complexos e também sobre corpos finitos existe apenas uma; e sobre os racionais existem infinitas não isomorfas.

Nosso objetivo no Capítulo 3 da dissertação é mostrar o seguinte resultado:

Teorema 1. *Sejam L e H duas álgebras de Lie simples de dimensão três e U_L e U_H suas respectivas álgebras envolventes universais. Então, U_L e U_H são isomorfas se, e somente se, L e H também são isomorfas.*

A ideia para provarmos esse teorema é mostrar dois importantes resultados: duas álgebras dos quatérnios são isomorfas se, e somente se, as álgebras de Lie simples de dimensão três referentes a elas também são isomorfas; duas álgebras dos quatérnios são isomorfas se, e somente se, as envolventes universais das álgebras de Lie simples de dimensão três referentes a elas também são isomorfas. A fim de provarmos esses dois resultados, trabalharemos com formas quadráticas de uma álgebra dos quatérnios e com a forma de Killing da álgebra de Lie simples de dimensão três. Mais precisamente, estudaremos o que acontece com a forma quadrática e com a forma de Killing quando as álgebras são isomorfas.

No Capítulo 4 da dissertação trabalharemos com as álgebras de Lie nilpotentes de dimensão finita, e para isso estudaremos o artigo [RU07]. Pretendemos provar o seguinte teorema:

Teorema 2. *Sejam L e H duas álgebras de Lie de dimensão finita e U_L e U_H suas respectivas álgebras envolventes universais tais que U_L e U_H são isomorfas. Então, se H é nilpotente, temos que L também é nilpotente. Além disso, nesse caso, o grau de nilpotência e o número mínimo de geradores de H e L serão os mesmos.*

A fim de provarmos esse teorema, iremos trabalhar com o ideal de aumento da envolvente universal. Pretendemos mostrar uma série de resultados que caminhem para um importante teorema, o qual diz que o ideal de aumento é residualmente nilpotente se, e somente se, a álgebra de Lie é nilpotente. Dessa forma, como o ideal de aumento depende da envolvente universal, temos que o fato de a álgebra de Lie ser nilpotente depende de sua envolvente universal. Nesse caso, dizemos que a envolvente universal determina se a álgebra de Lie é ou não nilpotente. Mostraremos também que existe um isomorfismo entre a envolvente universal da álgebra graduada de uma álgebra de Lie e a álgebra graduada do ideal de aumento da envolvente universal da álgebra de Lie. Através desse resultado, será possível mostrar que a álgebra envolvente universal da álgebra de Lie determina a álgebra graduada da álgebra de Lie, isto é, dadas duas álgebras de Lie cujas envolventes universais são isomorfas, então as álgebras graduadas das álgebras de Lie também são isomorfas. Caracterizada a álgebra graduada de

uma álgebra de Lie, será possível, quando a álgebra de Lie for nilpotente, determinar o grau de nilpotência e o número mínimo de geradores da álgebra de Lie. Apesar de nesta dissertação trabalharmos apenas com as álgebras de Lie de dimensão finita, os resultados de [RU07] são válidos sob álgebras de Lie de qualquer dimensão.

A fim de podermos desenvolver este trabalho, reservamos os dois primeiros capítulos para resultados gerais sobre álgebras de Lie, álgebras associativas, formas quadráticas e resíduos quadráticos, que serão ferramentas primordiais nos desenvolver dos capítulos subsequentes.

Capítulo 1

Álgebras de Lie

Neste capítulo, temos por objetivo apresentar definições e resultados interessantes da Teoria de Álgebras de Lie, a fim de usá-los nos capítulos subsequentes.

1.1 Definição e exemplos

Definição 1.1.1. Um espaço vetorial L sobre um corpo $\mathbb{F}$ com uma aplicação bilinear $[\cdot\,,\cdot]$, denominada `operação colchete`, é dito uma `álgebra de Lie` se as seguintes condições são satisfeitas:

(i) $[x, x] = 0$, para todo $x \in L$;

(ii) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$.

A propriedade (ii) é chamada de `Identidade de Jacobi`.

Notemos que a condição (i) implica na anticomutatividade da álgebra de Lie e, quando a característica de $\mathbb{F}$ é diferente de 2, podemos mostrar que a anticomutatividade implica na condição (i). Dessa forma, quando a característica de $\mathbb{F}$ é diferente de 2, podemos definir a álgebra de Lie substituindo a propriedade (i) por:

(i') $[x, y] = -[y, x]$, para todos $x, y \in L$.

Exemplo 1.1.2.

1) Seja L um espaço vetorial sobre um corpo $\mathbb{F}$ munido da operação $[\cdot\,,\cdot]$ tal que $[x, y] = 0$ para todos $x, y \in L$. Dessa forma, L é uma álgebra de Lie. Dizemos que uma álgebra de Lie que satisfaz essa propriedade é uma álgebra de Lie `abeliana`.

2) Seja R uma $\mathbb{F}$-álgebra associativa qualquer. Consideremos $[\cdot\,,\cdot]$ como sendo o comutador usual induzido da operação produto de R, isto é,

$$[x, y] = xy - yx, \qquad \text{para todos } x, y \in R.$$

O comutador é uma aplicação bilinear que satisfaz as condições (i) e (ii), logo R, com a operação comutador, é uma álgebra de Lie. Neste texto, sempre que nos referirmos a uma álgebra associativa como uma álgebra de Lie, estaremos tomando sua operação colchete como sendo a operação comutador e, quando conveniente, a denotaremos por $(R, +, [\cdot\,,\cdot])$.

3) Consideremos

$$M_n(\mathbb{F}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} : a_{ij} \in \mathbb{F}, i, j = 1, \dots, n \right\}$$

com as operações usuais de soma e multiplicação de matrizes. Então, $M_n(\mathbb{F})$ é uma álgebra associativa e $gl_n(\mathbb{F}) := (M_n(\mathbb{F}), +, [\cdot\,,\cdot])$ é uma álgebra de Lie.

4) Dado $A \in gl_n(\mathbb{F})$, o traço $\mathrm{tr}(A)$ da matriz quadrada A é a soma de suas entradas diagonais. O $\mathbb{F}$-espaço vetorial $sl_n(\mathbb{F}) := \{A \in gl_n(\mathbb{F})\colon \mathrm{tr}(A) = 0\}$ também é uma álgebra de Lie com a operação comutador induzida de $gl_n(\mathbb{F})$.

5) O $\mathbb{F}$-espaço vetorial

$$su_3(\mathbb{F}) = \left\{ \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} : a, b, c \in \mathbb{F} \right\}$$

é uma álgebra de Lie com a operação comutador induzida de $gl_3(\mathbb{F})$.

6) Consideremos

$$L = \left\{ \begin{pmatrix} 0 & a & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} : a, b, c \in \mathbb{F} \right\}.$$

L é fechado sob a soma e o produto usuais de matrizes, logo L é uma álgebra associativa. Então, $(L, +, [\cdot\,,\cdot])$ é uma álgebra de Lie conhecida como `álgebra de Heisenberg`.

1.2 Conceitos básicos

Vários conceitos da álgebra e da álgebra linear podem ser transportados imediatamente para a teoria de álgebras de Lie. Como toda álgebra de Lie é um espaço vetorial, teremos que os conceitos de álgebra linear, tais como base, dimensão, e outros, são os mesmos para álgebras de Lie.

Sejam L uma $\mathbb{F}$-álgebra de Lie e $B = \{x_i \colon i \in \mathcal{I}\}$ uma base de L. Para cada $i, j \in \mathcal{I}$, temos

$$[x_i, x_j] = \sum \alpha_{ij}^{(k)} x_k,$$

e L é determinada pelo conjunto $\{\alpha_{ij}^{(k)} \colon i, j, k \in \mathcal{I}\}$. Denotaremos L por

$$L = \langle B \colon [x_i, x_j] = \sum \alpha_{ij}^{(k)} x_k, \text{ para todos } i, j \in \mathcal{I} \rangle.$$

Para simplificar a escrita, quando $[x_i, x_j] = 0$ para algum par (i, j), omitiremos esse termo na apresentação de L.

Exemplo 1.2.1.

1) O conjunto

$$\left\{ e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

é uma base da $\mathbb{F}$-álgebra de Lie $sl_2(\mathbb{F})$, e segue que

$$sl_2(\mathbb{F}) = \langle e, f, h \colon [e, f] = h, [h, e] = 2e, [h, f] = -2f \rangle.$$

2) Uma base para $su_3(\mathbb{F})$ é dada por

$$\left\{ x = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, z = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \right\}$$

e $su_3(\mathbb{F}) = \langle x, y, z \colon [y, z] = -x, [z, x] = -y, [x, y] = -z \rangle$.

3) Seja L a álgebra de Heisenberg. Então,

$$\left\{ x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, z = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$$

é uma base de L, e $L = \langle x, y, z \colon [x, y] = z \rangle$.

Definição 1.2.2. Seja K um subespaço vetorial de uma álgebra de Lie L e $[\cdot\,,\cdot]$ a operação colchete de L. Se K é fechado sob a operação colchete, isto é, se para todos $x, y \in K$ temos que $[x, y] \in K$, então K é dita uma `subálgebra` de L.

Nesta dissertação, as vezes uma álgebra A é considerada como uma álgebra associativa e como uma álgebra de Lie. Nesse caso, vamos usar as expressões subálgebra associativa e subálgebra de Lie para indicar o tipo da subálgebra.

Exemplo 1.2.3.

1) Dada uma $\mathbb{F}$-álgebra de Lie L temos que L e $\{0\}$ são subálgebras de L, e chamaremos $\{0\}$ de `subálgebra trivial` de L.

2) Dada qualquer subálgebra K de L tal que $K \neq L$, dizemos que K é uma `subálgebra própria` de L.

3) $sl_n(\mathbb{F})$ é uma subálgebra de Lie de $gl_n(\mathbb{F})$.

4) Seja $L^2 := [L, L]$ o conjunto das combinações lineares de elementos na forma $[x, y]$ tal que $x, y \in L$. Temos que L^2 é uma subálgebra de L e chamaremos L^2 de `subálgebra derivada` de L. Quando $L = \langle x, y, z \colon [x, y] = z\rangle$ é a álgebra de Heisenberg, segue que L^2 é a álgebra unidimensional gerada por z; e quando $L = su_3(\mathbb{F})$, temos que $L^2 = L$.

Definição 1.2.4. Seja J um subespaço vetorial de uma álgebra de Lie L e $[\cdot\,,\cdot]$ a operação colchete de L. Se, para todos $x \in L$ e $y \in J$, segue que $[x, y] \in J$, então J é dito um `ideal` de L.

Dada uma álgebra de Lie L e uma subálgebra K de L, definimos o `normalizador` de K em L por

$$N_L(K) := \{x \in L \colon [x, y] \in K \text{ para todo } y \in K\}.$$

Notemos que, K é um ideal de $N_L(K)$ e, quando $N_L(K) = L$, então K é um ideal de L.

Exemplo 1.2.5.

1) De forma análoga às subálgebras, dada uma $\mathbb{F}$-álgebra de Lie L temos que L e $\{0\}$ são ideais de L, e chamaremos $\{0\}$ de `ideal trivial` de L. Além disso, dado qualquer ideal J de L tal que $J \neq L$, dizemos que J é um `ideal próprio` de L.

2) $sl_n(\mathbb{F})$ é um ideal de $gl_n(\mathbb{F})$, pois dadas duas matrizes quaisquer $A, B \in M_n(\mathbb{F})$, temos que $\operatorname{tr}([A, B]) = \operatorname{tr}(AB - BA) = 0$.

3) $su_3(\mathbb{F})$ é uma subálgebra de $gl_3(\mathbb{F})$, porém não é um ideal. De fato, consideremos por exemplo

$$x = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in su_3(\mathbb{F}) \qquad \text{e} \qquad a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in gl_3(\mathbb{F}),$$

então

$$[a, x] = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin su_3(\mathbb{F}).$$

4) A subálgebra derivada L^2 de L é um ideal de L.

5) Seja L uma $\mathbb{F}$-álgebra de Lie. Definimos o *centro* de L por

$$\mathcal{Z}(L) = \{x \in L \colon [x, y] = 0, \text{ para todo } y \in L\}.$$

$\mathcal{Z}(L)$ é um ideal de L.

Definição 1.2.6. Sejam L e H duas $\mathbb{F}$-álgebras de Lie e $[\cdot\,,\cdot]_L$ e $[\cdot\,,\cdot]_H$ suas respectivas operações colchete. Um `homomorfismo de álgebras de Lie` entre L e H é uma aplicação linear $\phi \colon L \to H$ tal que

$$\phi([x, y]_L) = [\phi(x), \phi(y)]_H, \qquad \text{para todos } x, y \in L.$$

Assim, dado um homomorfismo de álgebras de Lie $\phi \colon L \to H$, temos que o `núcleo` de ϕ, dado pelo conjunto $\ker(\phi) := \{x \in L \colon \phi(x) = 0\}$, é um ideal de L, enquanto que a `imagem` de ϕ, dada pelo conjunto $\mathrm{Im}(\phi) := \{y \in H \colon \phi(x) = y \text{ para algum } x \in L\}$, é uma subálgebra de H. Um homomorfismo ϕ que é tanto sobrejetivo quanto injetivo é chamado de `isomorfismo`.

Exemplo 1.2.7.

1) Consideremos as álgebras

$$L = \langle x_1, x_2, x_3, x_4, x_5 \colon [x_1, x_2] = x_3, [x_1, x_3] = x_4, [x_1, x_4] = x_5, [x_2, x_3] = x_5 \rangle,$$

$$H = \langle x_1', x_2', x_3', x_4', x_5' \colon [x_1', x_2'] = x_3', [x_1', x_3'] = x_4', [x_1', x_4'] = x_5' \rangle.$$

Mostraremos que L e H não são isomorfas. Para isso, suponhamos que existe um isomorfismo $\phi \colon L \to H$ tal que

$$\phi(x_1) = a_1 x_1' + a_2 x_2' + a_3 x_3' + a_4 x_4' + a_5 x_5',$$

$$\phi(x_2) = b_1x'_1 + b_2x'_2 + b_3x'_3 + b_4x'_4 + b_5x'_5,$$

$$\phi(x_3) = c_1x'_1 + c_2x'_2 + c_3x'_3 + c_4x'_4 + c_5x'_5,$$

$$\phi(x_4) = d_1x'_1 + d_2x'_2 + d_3x'_3 + d_4x'_4 + d_5x'_5,$$

$$\phi(x_5) = e_1x'_1 + e_2x'_2 + e_3x'_3 + e_4x'_4 + e_5x'_5.$$

Como ϕ é um isomorfismo, temos que $[\phi(x_1), \phi(x_2)] = \phi(x_3)$, $[\phi(x_1), \phi(x_3)] = \phi(x_4)$, $[\phi(x_1), \phi(x_4)] = \phi(x_5)$ e $[\phi(x_2), \phi(x_3)] = \phi(x_5)$. Dessa forma, obtemos os seguintes sistemas:

$$\left\{\begin{array}{rcl} c_1 &=& 0 \\ c_2 &=& 0 \\ c_3 &=& a_1b_2 - a_2b_1 \\ c_4 &=& a_1b_3 - a_3b_1 \\ c_5 &=& a_1b_4 - a_4b_1 \end{array}\right., \left\{\begin{array}{rcl} d_1 &=& 0 \\ d_2 &=& 0 \\ d_3 &=& 0 \\ d_4 &=& a_1c_3 \\ d_5 &=& a_1c_4 \end{array}\right., \left\{\begin{array}{rcl} e_1 &=& 0 \\ e_2 &=& 0 \\ e_3 &=& 0 \\ e_4 &=& 0 \\ e_5 &=& a_1d_4 \end{array}\right., \left\{\begin{array}{rcl} e_1 &=& 0 \\ e_2 &=& 0 \\ e_3 &=& 0 \\ e_4 &=& b_1c_3 \\ e_5 &=& b_1c_4 \end{array}\right..$$

Assim, $b_1c_3 = 0$, então $c_3 = 0$ pois $e_5 \neq 0$ (caso contrário, $x_5 \in \ker(\phi)$ e ϕ não seria injetiva), logo b_1 não pode ser igual a zero. Mas, se $c_3 = 0$, então $d_4 = 0$, o que implica que $e_5 = 0$. Portanto, ϕ não é um isomorfismo e L e H são álgebras de Lie não isomorfas.

2) Um exemplo bastante importante de homomorfismo de álgebras de Lie é a `representação adjunta` de uma $\mathbb{F}$-álgebra de Lie L, definida pela aplicação

$$\mathrm{ad}: \begin{array}{ccc} L & \to & gl(L) \\ x & \mapsto & \mathrm{ad}_x \end{array} \quad \text{onde} \quad \mathrm{ad}_x: \begin{array}{ccc} L & \to & L \\ y & \mapsto & [x,y] \end{array}$$

e $gl(L)$ é a álgebra das transformações lineares de L em L. Como consequência da identidade de Jacobi, segue que

$$\mathrm{ad}_{[x,y]} = [\mathrm{ad}_x, \mathrm{ad}_y],$$

logo ad é um homomorfismo de álgebras de Lie.

Uma propriedade interessante é que $\ker(\mathrm{ad}) = \mathcal{Z}(L)$. Assim, quando L é abeliana, a adjunta é igual ao homomorfismo trivial; e quando $\mathcal{Z}(L) = \{0\}$, a adjunta é injetiva.

Dado um ideal J da $\mathbb{F}$-álgebra de Lie L, podemos construir a `álgebra de Lie quociente` L/J de maneira análoga à dos anéis quocientes: L/J é um espaço vetorial e a operação colchete

em L/J é induzida naturalmente da operação colchete de L, isto é, se $x+J, y+J \in L/J$, então

$$[x+J, y+J] := [x,y] + J.$$

Temos que mostrar que essa operação está bem definida. De fato, dados $x+J = x'+J$ e $y+J = y'+J$, temos que existem $u, v \in J$ tais que $x' = x+u$ e $y' = y+v$. Logo

$$[x', y'] - [x,y] = [x,v] + [u,y] + [u,v] \in J,$$

pois J é um ideal de L e, portanto, $[x+J, y+J] = [x'+J, y'+J]$.

Agora, introduziremos os três resultados clássicos sobre homomorfismos.

Teorema 1.2.8 (Primeiro Teorema do Isomorfismo para Álgebras de Lie)**.** *Seja $\phi\colon L \to L'$ um homomorfismo entre álgebras de Lie. Então, $L/\ker(\phi)$ é isomorfa a $\phi(L)$.*

Teorema 1.2.9 (Segundo Teorema do Isomorfismo para Álgebras de Lie)**.** *Sejam I e J ideais da $\mathbb{F}$-álgebra de Lie L. Então, $(I+J)/J$ é isomorfa a $I/(I \cap J)$.*

Teorema 1.2.10 (Terceiro Teorema do Isomorfismo para Álgebras de Lie)**.** *Sejam I e J ideais da $\mathbb{F}$-álgebra de Lie L tais que $I \subseteq J$. Então, J/I é um ideal de L/I e $(L/I)/(J/I)$ é isomorfa a L/J.*

1.3 Álgebras de Lie simples

Definição 1.3.1. Seja L uma $\mathbb{F}$-álgebra de Lie. Diremos que L é `simples` se seus únicos ideais são $\{0\}$ e L e, além disso, se $L^2 = [L,L] \neq \{0\}$.

Dessa forma, se L é simples, como L^2 e $\mathcal{Z}(L)$ são ideais de L, temos que $\mathcal{Z}(L) = \{0\}$ e $L^2 = L$.

Exemplo 1.3.2.

1) Consideremos a $\mathbb{F}$-álgebra de Lie $sl_2(\mathbb{F}) = \langle e, f, h\colon [e,f] = h, [h,e] = 2e, [h,f] = -2f\rangle$.

Se a característica de $\mathbb{F}$ é diferente de 2, então $sl_2(\mathbb{F})$ é simples. De fato, se J é um ideal não trivial de $sl_2(\mathbb{F})$, então existe $a = \alpha_1 e + \alpha_2 f + \alpha_3 h \in J$ não nulo. Logo,

$$[a,e] = -\alpha_2 h + 2\alpha_3 e,\ [a,f] = \alpha_1 h - 2\alpha_3 f,\ [a,h] = -2\alpha_1 e + 2\alpha_2 f\ \in J.$$

Agora, notemos que $[e,[a,h]] = 2\alpha_2 h$, $[f,[a,h]] = 2\alpha_1 h$ e $[h,[a,e]] = 4\alpha_3 e$. Como α_1, α_2 ou α_3 é diferente de 0, temos que e ou h pertence a J. Assim, segue das relações entre os elementos da base de $sl_2(\mathbb{F})$, que $e, f, h \in J$ e, consequentemente, $J = sl_2(\mathbb{F})$.

Quando a característica de $\mathbb{F}$ é igual a 2, segue que $sl_2(\mathbb{F}) = \langle e, f, h \colon [e,f] = h, [h,e] = [h,f] = 0\rangle$ e $sl_2(\mathbb{F})$ possui um ideal não trivial, a saber, o ideal unidimensional gerado por h. Logo, $sl_2(\mathbb{F})$ não é simples nesse caso.

2) Seja $su_3(\mathbb{F}) = \langle x, y, z \colon [y,z] = -x, [z,x] = -y, [x,y] = -z\rangle$. Queremos mostrar que, se J é um ideal não trivial de $su_3(\mathbb{F})$, então $J = su_3(\mathbb{F})$ e, assim, $su_3(\mathbb{F})$ é simples. De fato, seja $a = \alpha_1 x + \alpha_2 y + \alpha_3 z \in J$ não nulo, então

$$[a,x] = \alpha_2 z - \alpha_3 x,\ [a,y] = -\alpha_1 z + \alpha_3 x,\ [a,z] = \alpha_1 y - \alpha_2 x\ \in J.$$

Agora, notemos que $[x,[a,y]] = -\alpha_1 y$, $[y,[a,z]] = -\alpha_2 z$ e $[z,[a,x]] = \alpha_3 y$ e, como α_1, α_2 ou α_3 é diferente de 0, analogamente ao exemplo anterior, temos que $J = su_3(\mathbb{F})$.

3) Como já vimos, se $L = \langle x, y, z \colon [x,y] = z\rangle$ é a álgebra de Heisenberg, então L não é simples, pois L^2 é a álgebra unidimensional gerada por z.

1.4 Álgebras de Lie solúveis e nilpotentes

Definição 1.4.1. Seja L uma $\mathbb{F}$-álgebra de Lie.

(i) A `série derivada` de L é a série definida por

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

Diremos que L é `solúvel` se existe $n \in \mathbb{N}$ tal que $L^{(n)} = \{0\}$, e chamaremos o menor n tal que $L^{(n)} = \{0\}$ de `grau de solubilidade` de L.

(ii) A `série central descendente` de L é a série definida por

$$L^1 = L\ \supseteq\ L^2 = [L,L]\ \supseteq\ L^3 = [L,L^2]\ \supseteq\ \ldots\ \supseteq\ L^i = [L,L^{i-1}]\ \supseteq\ \ldots$$

Diremos que L é `nilpotente` se existe $n \in \mathbb{N}$ tal que $L^n = \{0\}$. Se n é o menor número natural tal que $L^n = \{0\}$, então diremos que $n-1$ é o `grau de nilpotência` de L.

Lema 1.4.2. *Seja L uma $\mathbb{F}$-álgebra de Lie. Então, $[L^i, L^j] \subseteq L^{i+j}$ para todos $i, j \geq 1$.*

Demonstração. Por definição, $[L, L^j] = L^{j+1}$. Suponhamos que para todo j temos que $[L^i, L^j] \subseteq L^{i+j}$. Queremos mostrar que $[L^{i+1}, L^j] \subseteq L^{i+j+1}$. De fato,

$$[L^{i+1}, L^j] = [[L,L^i], L^j] \subseteq [L,[L^i,L^j]] + [L^i,[L^j,L]] \subseteq [L, L^{i+j}] + [L^i, L^{j+1}] \subseteq L^{i+j+1}.$$

□

Exemplo 1.4.3.

1) Toda $\mathbb{F}$-álgebra de Lie abeliana é tanto solúvel quanto nilpotente, pois $L^{(1)} = L^2 = \{0\}$ e seu grau de solubilidade e de nilpotência são ambos iguais a 1.

2) A álgebra de Heisenberg é tanto solúvel quanto nilpotente, e seus graus de solubilidade e nilpotência são ambos iguais a 2.

3) Seja L uma $\mathbb{F}$-álgebra de Lie simples. Então, L não é nem solúvel nem nilpotente. De fato, como L é simples, temos que $L^{(1)} = L^2 = L$ e, assim, $L^{(n-1)} = L^n = L$ para todo $n \in \mathbb{N}$.

4) Como consequência do item anterior, temos que a $\mathbb{F}$-álgebra de Lie $su_3(\mathbb{F})$ não é solúvel nem nilpotente, pois é simples.

5) A $\mathbb{F}$-álgebra de Lie $sl_2(\mathbb{F})$ não é nem solúvel nem nilpotente quando a característica de $\mathbb{F}$ é diferente de 2, pois, nesse caso, $sl_2(\mathbb{F})$ é simples.

Por outro lado, quando a característica de $\mathbb{F}$ é igual a 2, temos que $sl_2(\mathbb{F}) = \langle e, f, h \colon [e, f] = h, [h, e] = [h, f] = 0\rangle$ e, assim, $sl_2(\mathbb{F})$ é isomorfa à álgebra de Heisenberg. Portanto, quando a caracterítica de $\mathbb{F}$ é igual a 2, temos que $sl_2(\mathbb{F})$ é tanto solúvel quanto nilpotente, e seus graus de solubilidade e nilpotência são ambos iguais a 2.

Notemos que $L^{(n-1)} \subseteq L^n$ para todo $n \in \mathbb{N}$, logo toda álgebra de Lie nilpotente também é solúvel; porém, a volta não é válida. Por exemplo, seja L a $\mathbb{F}$-álgebra de Lie bidimensional não-abeliana dada por $L = \langle x, y \colon [x, y] = y\rangle$. Nesse caso, segue que $L^{(1)}$ é a álgebra unimensional gerada por y e $L^{(2)} = \{0\}$, logo ela é solúvel, porém $L^1 = L$, $L^2 = [L, L^1] = [L, L] = \langle y\rangle$ e $L^n = \langle y\rangle$ para todo $n \geq 3$, logo L não é nilpotente.

Em geral, se L é uma $\mathbb{F}$-álgebra de dimensão 2, temos que L pode ser abeliana ou não abeliana e, em ambos os casos, segue que L é solúvel. De igual forma, toda $\mathbb{F}$-álgebra de Lie de dimensão 1 também é solúvel e, assim, segue o seguinte lema.

Lema 1.4.4. *Toda álgebra de Lie de dimensão* 1 *ou* 2 *é solúvel.*

Dada uma $\mathbb{F}$-álgebra de Lie L, dizemos que o `número mínimo de geradores` de L é igual a cardinalidade de um menor subconjunto S de L que gera L como álgebra de Lie. Assim, quando L é uma álgebra de Lie nilpotente de dimensão finita, podemos mostrar que a dimensão de L/L^2 é igual ao número mínimo de geradores de L. Para isso, precisamos dos seguintes lemas:

Lema 1.4.5. *Sejam L uma álgebra de Lie nilpotente e K uma subálgebra própria de L. Então, K é uma subálgebra própria de $N_L(K)$.*

Demonstração. Como L é nilpotente, existe um índice n tal que $L^n \supsetneq L^{n+1} = \{0\}$. Agora, como K é uma subálgebra própria de L, existe um índice $1 \leq i < n$ tal que $L^i \nsubseteq K$ e $L^{i+1} \subseteq K$. Então,

$$[K, L^i] \subseteq [L, L^i] = L^{i+1} \subseteq K.$$

Logo, $L^i \subseteq N_L(K)$ e, assim, $K + L^i \subseteq N_L(K)$ e, como $K < K + L^i$, o lema é válido. □

Uma consequência desse lema é que, quando K é uma subálgebra maximal de L, então $N_L(K) = L$ e, assim, K é um ideal de L. Portanto, temos o seguinte corolário.

Corolário 1.4.6. *Sejam L uma álgebra de Lie nilpotente e K uma subálgebra maximal de L. Então, K é um ideal maximal de L.*

Lema 1.4.7. *Sejam L uma álgebra de Lie nilpotente e J um ideal maximal de L. Então, J contém L^2.*

Demonstração. Como J é um ideal maximal de uma álgebra de Lie nilpotente L e $L^2 + J$ é um ideal de L tal que $J \subseteq L^2 + J \subseteq L$, então $L^2 + J = J$ ou $L^2 + J = L$. Se $L^2 + J = J$, então $L^2 \subseteq J$. Assim, a fim de concluir nossa demonstração, é suficiente mostrar que o caso $L^2 + J = L$ não pode ocorrer. Assumamos então que $L^2 + J = L$. Assim,

$$L^2 = [L, L] = [L, L^2 + J] = [L, L^2] + [L, J] \subseteq L^3 + J.$$

Por um argumento indutivo segue que, para todo $n \in \mathbb{N}$, $L^n \subseteq L^{n+1} + J$. Como L é nilpotente, existe um $k \in \mathbb{N}$ tal que $L^{k-1} \neq \{0\}$ e $L^k = \{0\}$. Assim, $L^{k-1} \subseteq L^k + J = J$. Repetindo o mesmo processo um número finito de vezes, concluímos que $L^2 \subseteq J$ e, assim, $J = L$, o que não é possível desde que J é ideal maximal de L. □

Teorema 1.4.8. *Seja L é uma $\mathbb{F}$-álgebra de Lie nilpotente de dimensão finita. Então, a dimensão de L/L^2 é igual ao número mínimo de geradores de L.*

Demonstração. Como L é uma $\mathbb{F}$-álgebra de Lie, então o número mínimo de geradores de L/L^2 é menor ou igual ao número mínimo de geradores de L. Agora, como L/L^2 é abeliana, segue que o menor número de geradores possíveis de L/L^2 é igual a sua dimensão.

Por outro lado, suponhamos que a dimensão de L/L^2 é igual a d e que $\{x_1 + L^2, \ldots, x_d + L^2\}$ é uma base de L/L^2. Assim, temos que L é gerada pelo conjunto $\{x_1, \ldots, x_d\}$ e por L^2. Queremos mostrar que $\{x_1, \ldots, x_d\}$ gera L. Se L não é gerado por $\{x_1, \ldots, x_d\}$, então existe uma subálgebra maximal K de L tal que K contém $\{x_1, \ldots, x_d\}$. Como L é nilpotente, pelo Corolário 1.4.6, temos que K é um ideal maximal de L e, pelo Lema 1.4.7, K contém L^2. Dessa

forma, K contém $\{x_1, \ldots, x_d\}$ e L^2, logo $K = L$, contrariando o fato de K ser um ideal maximal de L. Portanto, L é gerado por $\{x_1, \ldots, x_d\}$. □

As seguintes propriedades das $\mathbb{F}$-álgebras de Lie solúveis e nilpotentes podem ser encontradas na Seção 3 do Capítulo 1 de [Hum72]:

Proposição 1.4.9. *Seja L uma $\mathbb{F}$-álgebra de Lie.*

i) *Se L é solúvel (nilpotente), então todas suas subálgebras também o são.*

ii) *Se I é um ideal solúvel de L tal que L/I também é solúvel, então L também o é. Se $L/\mathcal{Z}(L)$ é nilpotente, então L também o é.*

iii) *Se L é nilpotente, então $\mathcal{Z}(L) \neq \{0\}$.*

iv) *Se I e J são ideais solúveis de L, então $I + J$ também é solúvel.*

1.5 Álgebra graduada

Definição 1.5.1. Seja L uma álgebra de Lie sobre o corpo $\mathbb{F}$. Definiremos a `álgebra graduada` associada à série central descendente de L por

$$\mathrm{gr}(L) = \bigoplus_{i \geq 1} \frac{L^i}{L^{i+1}},$$

com o produto em $\mathrm{gr}(L)$ induzido de L, isto é, se $\overline{x} = x + L^{i+1}$ e $\overline{y} = y + L^{j+1}$, com $x \in L^i$ e $y \in L^j$, então

$$[\overline{x}, \overline{y}] = [x, y] + L^{i+j+1}.$$

Notemos que $\mathrm{gr}(L)$ é uma álgebra de Lie. De fato, tomemos $\overline{x} = \sum_i (x_i + L^{i+1}) \in \mathrm{gr}(L)$ (notemos que as somas são finitas, então existe um número finito de índices i tal que $x_i \neq 0$), então

$$\begin{aligned}
[\overline{x}, \overline{x}] &= \left[\sum_{i_1} (x_{i_1} + L^{i_1+1}), \sum_{i_2} (x_{i_2} + L^{i_2+1})\right] \\
&= \sum_{i_1} \sum_{i_2} ([x_{i_1}, x_{i_2}] + L^{i_1+i_2+1}) \\
&= \sum_{i_1 = i_2} ([x_{i_1}, x_{i_2}] + L^{i_1+i_2+1}) + \sum_{i_1 \neq i_2} ([x_{i_1}, x_{i_2}] + L^{i_1+i_2+1}) \\
&= 0,
\end{aligned}$$

pois $[x_{i_1}, x_{i_2}] = 0$ sempre que $i_1 = i_2$ e $[x_{i_1}, x_{i_2}] = -[x_{i_2}, x_{i_1}]$ sempre que $i_1 \neq i_2$. Agora, como a identidade de Jacobi é multilinear, basta verificar que ela é válida nos geradores de $\mathrm{gr}(L)$. Assim, sejam $\overline{x} = x + L^{i+1}$, $\overline{y} = y + L^{j+1}$, $\overline{z} = z + L^{k+1} \in \mathrm{gr}(L)$, então

$$[\overline{x}, [\overline{y}, \overline{z}]] = [x, [y, z]] + L^{i+j+k+1} = (-[y, [z, x]] - [z, [x, y]]) + L^{i+j+k+1} = -[\overline{y}, [\overline{z}, \overline{x}]] - [\overline{z}, [\overline{x}, \overline{y}]].$$

Exemplo 1.5.2.

1) Seja $L = \langle x, y \colon [x, y] = y \rangle$ a álgebra de Lie bidimensional não abeliana sobre o corpo $\mathbb{F}$. Notemos que L^n é a álgebra unidimensional gerada por y para todo $n \geq 2$. Assim, $L/L^2 = \mathrm{span}\{x+L^2\}$ ($\mathrm{span}\{x+L^2\}$ significa o espaço linear gerado pelo conjunto $\{x+L^2\}$) e $L^2/L^3 = \{0\}$. Portanto, a álgebra $\mathrm{gr}(L)$ é igual a L/L^2.

2) Seja $L = \langle x, y, z \colon [x, y] = z \rangle$ a álgebra de Heisenberg. Notemos que $L^2 = \mathrm{span}\{z\}$ e $L^n = \{0\}$ para todo $n \geq 3$. Assim, $L/L^2 = \mathrm{span}\{x + L^2, y + L^2\}$, $L^2/L^3 = \mathrm{span}\{z + L^3\}$ e $L^3/L^4 = \{0\}$ e, portanto,

$$\mathrm{gr}(L) = \mathrm{span}\{x + L^2, y + L^2\} \oplus \mathrm{span}\{z + L^3\}.$$

3) Seja $L = \langle x_1, x_2, x_3, x_4, x_5 \colon [x_1, x_2] = x_3, [x_1, x_3] = x_4, [x_1, x_4] = x_5, [x_2, x_3] = x_5 \rangle$. Notemos que $L^2 = \mathrm{span}\{x_3, x_4, x_5\}$, $L^3 = \mathrm{span}\{x_4, x_5\}$, $L^4 = \{x_5\}$ e $L^5 = \{0\}$, então

$$\mathrm{gr}(L) = \mathrm{span}\{x_1 + L^2, x_2 + L^2\} \oplus \mathrm{span}\{x_3 + L^3\} \oplus \mathrm{span}\{x_4 + L^4\} \oplus \mathrm{span}\{x_5 + L^5\}.$$

4) Seja $H = \langle x_1, x_2, x_3, x_4, x_5 \colon [x_1, x_2] = x_3, [x_1, x_3] = x_4, [x_1, x_4] = x_5 \rangle$. Notemos que $H^2 = \mathrm{span}\{x_3, x_4, x_5\}$, $H^3 = \mathrm{span}\{x_4, x_5\}$, $H^4 = \{x_5\}$ e $H^5 = \{0\}$, então

$$\mathrm{gr}(H) = \mathrm{span}\{x_1 + H^2, x_2 + H^2\} \oplus \mathrm{span}\{x_3 + H^3\} \oplus \mathrm{span}\{x_4 + H^4\} \oplus \mathrm{span}\{x_5 + H^5\}.$$

Observemos que, apesar de L e H dos itens 3 e 4 do exemplo acima não serem isomorfas (ver item 1 do Exemplo 1.2.7), temos que $\mathrm{gr}(L)$ e $\mathrm{gr}(H)$ são álgebras de Lie isomorfas (basta observar que $[x_2 + L^2, x_3 + L^3] = [x_2, x_3] + L^4 = x_5 + L^4 = L^4$). Portanto, esse exemplo mostra que o isomorfismo entre duas álgebras graduadas não implica no isomorfismo entre suas respectivas álgebras de Lie associadas.

Nos lemas seguintes, a fim de facilitar notação, seja

$$L_i := \frac{L^i}{L^{i+1}}.$$

Lema 1.5.3. *Seja L uma $\mathbb{F}$-álgebra de Lie e $gr(L)$ sua álgebra graduada. Então, $L_{i+1} = [L_1, L_i]$. Em particular, $gr(L)$ é gerada por L_1 como álgebra de Lie.*

Demonstração. Primeiramente, tomemos $\overline{x} \in L_1$ e $\overline{y} \in L_i$, então $\overline{x} = x + L^2$ e $\overline{y} = y + L^{i+1}$ com $x \in L$ e $y \in L^i$. Assim, pela definição do produto em $\mathrm{gr}(L)$, temos que

$$[\overline{x}, \overline{y}] = [x + L^2, y + L^{i+1}] = [x, y] + L^{i+2} \in L_{i+1}.$$

Logo, $[L_1, L_i] \subseteq L_{i+1}$. Agora, tomemos $\overline{z} = z + L^{i+2} \in L_{i+1}$, então $z \in L^{i+1}$ e $z = \sum \alpha_{xy}[x, y]$ onde $x \in L$ e $y \in L^i$. Então,

$$\overline{z} = \sum(\alpha_{xy}[x, y] + L^{i+2}) = \sum \alpha_{xy}[x + L^2, y + L^{i+1}] \in [L_1, L_i]$$

e, assim, $L_{i+1} \subseteq [L_1, L_i]$. Portanto, $L_{i+1} = [L_1, L_i]$.

Seque por indução em i que L_i está contida na subálgebra gerada por L_1 e, assim, $\mathrm{gr}(L)$ é gerada por L_1 como álgebra de Lie. □

Lema 1.5.4. *Seja L uma $\mathbb{F}$-álgebra de Lie de dimensão finita. Então $gr(L)$ é nilpotente.*

Para mostrarmos esse lema, primeiro mostraremos o seguinte resultado:

Lema 1.5.5. *Seja L uma $\mathbb{F}$-álgebra de Lie e $gr(L)$ sua álgebra graduada. Então,*

$$gr(L)^n = \bigoplus_{i \geq n} L_i.$$

Demonstração. Provaremos esse lema usando o processo de indução. Se $n = 1$, é exatemente a definição de $\mathrm{gr}(L)$. Suponhamos que para $n - 1$ o resultado segue, isto é,

$$\mathrm{gr}(L)^{n-1} = \bigoplus_{i \geq n-1} L_i.$$

Então,

$$\begin{aligned} \mathrm{gr}(L)^n &= [\mathrm{gr}(L), \mathrm{gr}(L)^{n-1}] = \left[\bigoplus_{j \geq 1} L_j, \bigoplus_{i \geq n-1} L_i\right] \\ &= \bigoplus_{j \geq 1} \bigoplus_{i \geq n-1} [L_j, L_i]. \end{aligned}$$

Temos que $[L_j, L_i] = [L^j/L^{j+1}, L^i/L^{i+1}] = [L^j, L^i] + L^{j+i+1} \subseteq L_{j+i}$ para todos $j \geq 2$ e

$i \geq n-1$ e, pelo Lema 1.5.3, temos que $[L_1, L_i] = L_{i+1}$ para todo $i \geq 1$. Portanto,

$$\mathrm{gr}(L)^n = \bigoplus_{j\geq 1} \bigoplus_{i\geq n-1} [L_j, L_i] = \bigoplus_{k\geq n} L_k.$$

□

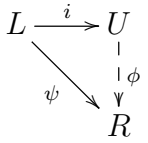
Demonstração. (Lema 1.5.4) Como L é finita, seja n tal que $L^n \supsetneq L^{n+1} = L^{n+2}$. Então,

$$\mathrm{gr}(L) = L_1 \oplus L_2 \oplus \cdots \oplus L_n.$$

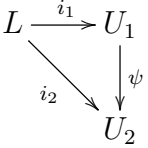
Pelo Lema 1.5.4, temos que $\mathrm{gr}(L)^{n+1} = \bigoplus_{i\geq n+1} L_i = \{0\}$ e, portanto, $\mathrm{gr}(L)$ é nilpotente com grau de nilpotência n. □

1.6 Álgebra envolvente universal

Definição 1.6.1. Seja L uma álgebra de Lie sobre um corpo $\mathbb{F}$. Uma álgebra associativa U com unidade é dita uma `álgebra envolvente universal` de L se existe um homomorfismo $i\colon L \to U$ de álgebras de Lie tal que, para qualquer $\mathbb{F}$-álgebra R associativa com unidade e para todo homomorfismo de álgebras de Lie $\phi\colon L \to R$, existe um único homomorfismo de $\mathbb{F}$-álgebras associativas $\psi\colon U \to R$ tal que $\psi \circ i = \phi$, isto é, o diagrama abaixo comuta.



A álgebra envolvente universal de L é única a menos de isomorfismo. De fato, sejam U_1 e U_2 duas álgebras envolventes universais de L. Como U_2 é uma álgebra associativa, pela propriedade universal da álgebra envolvente U_1, o diagrama



comuta, isto é, $\psi \circ i_1 = i_2$. Por outro lado, como U_1 é uma álgebra associativa e U_2 é uma

envolvente universal de L, segue também da propriedade universal de U_2 que o diagrama

$$\begin{array}{ccc} L & \xrightarrow{i_2} & U_2 \\ & \searrow^{i_1} & \downarrow \phi \\ & & U_1 \end{array}$$

comuta, isto é, $\phi \circ i_2 = i_1$. Portanto, $\psi \circ \phi = Id_{U_2}$ e $\phi \circ \psi = Id_{U_1}$ e, assim, U_1 e U_2 são isomorfas.

A fim de mostrarmos a existência, sejam $T^0L = \mathbb{F}$, $T^1L = L$ e $T^nL = \underbrace{L \otimes \cdots \otimes L}_{n \text{ vezes}}$, com $n = 2, 3, 4, \ldots$, e definimos

$$T = \bigoplus_{i=0}^{\infty} T^i L.$$

Temos que T com a operação justaposição é uma álgebra livre associativa com unidade.

Seja J o ideal de T gerado por $x \otimes y - y \otimes x - [x, y]$ para todos $x, y \in L$. A partir de agora omitiremos a operação tensor, isto é, sempre que escrevermos xy estaremos nos referindo ao elemento $x \otimes y$ em T. Mostraremos que a álgebra quociente T/J é uma álgebra envolvente universal de L e, pela unicidade, ela será única a menos de isomorfismo. Para isso, tomaremos a restrição do homomorfismo canônico $\pi \colon T \to T/J$ a L para ser a função i da definição da álgebra envolvente universal.

Sejam R uma $\mathbb{F}$-álgebra associativa qualquer e $\phi \colon L \to R$ um homomorfismo de álgebras de Lie. Então, como T é uma álgebra livre associativa com unidade, existe um homomorfismo de álgebras associativas $\psi \colon T \to R$ tal que o seguinte diagrama comuta:

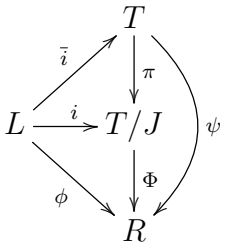
$$\begin{array}{ccc} L & \xrightarrow{\bar{i}} & T \\ & \searrow^{\phi} & \downarrow \psi \\ & & R \end{array}$$

Notemos que $J \subseteq \ker(\psi)$, pois se $x, y \in L$, então, como ψ é um homomorfismo de álgebras associativas e ϕ é um homomorfismo de álgebras de Lie, temos que

$$\begin{aligned} \psi(xy - yx - [x, y]) &= \psi(x)\psi(y) - \psi(y)\psi(x) - \phi([x, y]) \\ &= \phi(x)\phi(y) - \phi(y)\phi(x) - [\phi(x), \phi(y)] \\ &= 0. \end{aligned}$$

Dessa forma, a aplicação $\Phi \colon T/J \to R$ tal que $\Phi(x + J) = \psi(x) + J$ está bem definida e

temos o seguinte diagrama



Assim, Φ é um homomorfismo de álgebras associativas. Logo, T/J é a álgebra envolvente universal de L.

Um resultado importante na teoria das álgebras envolventes universais de uma álgebra de Lie é o Teorema de Poincaré-Birkhoff-Witt, que nos garante que toda álgebra envolvente universal possui uma base ordenada. Para podermos enunciar o Teorema de Poincaré-Birkhoff-Witt, iremos primeiro definir o que é um monômio ordenado.

Uma `base ordenada` de um espaço vetorial é uma base na qual existe uma ordenação entre seus elementos. Assim, como toda álgebra de Lie é um espaço vetorial, o conceito de base ordenada para álgebras de Lie é o mesmo empregado para espaços vetoriais.

Definição 1.6.2. Sejam $\{x_i \colon i \in \mathcal{I}\}$ uma base ordenada de L e $m = x_{i_1} \dots x_{i_t} \in T$ um monômio. Dizemos que m é um `monômio ordenado` em T se $i_1 \leq i_2 \leq \cdots \leq i_t$.

Teorema 1.6.3 (Theorem 3 (Poincaré-Birkhoff-Witt), página 159, [Jac79])**.** *Sejam L uma $\mathbb{F}$-álgebra de Lie com base ordenada $\{x_i \colon i \in \mathcal{I}\}$, $T = \bigoplus_{i=0}^{\infty} T^i L$ e J o ideal de T gerado por $xy - yx - [x, y]$. Então, as classes do 1 e dos monômios ordenados m, formam uma base para a álgebra envolvente universal $U = T/J$ de L.*

Dessa forma, chamaremos os elementos da base supracitada da envolvente universal de L de `mônomios de Poincaré-Birkhoff-Witt` ou `PBW-monômios`.

Exemplo 1.6.4.

1) Consideremos a álgebra de Lie abeliana $L = \langle x_1, \dots, x_\ell \colon [x_i, x_j] = 0$ para todos $i, j = 1, \dots, \ell \rangle$. Então, a álgebra envolvente universal de L coincide com a álgebra dos polinômios
$\mathbb{F}[x_1, \dots, x_n]$.

2) Seja $L = \langle x, y, z \colon [x, y] = z, [y, z] = x, [z, x] = y \rangle$. Então, os elementos da álgebra envolvente universal U de L serão combinações lineares de monômios em x, y e z, e poderemos ordenar cada um desses monômios através das identidades:

$$xy - yx = z, \qquad yz - zy = x \qquad \text{e} \qquad zx - xz = y.$$

Por exemplo, tomemos $zyx \in U$, então:

$$\begin{aligned} zyx &= (yz - x)x = yzx - x^2 \\ &= y(y + xz) - x^2 = y^2 + yxz - x^2 \\ &= y^2 + (xy - z)z - x^2 = -x^2 + y^2 - z^2 + xyz. \end{aligned}$$

Seguindo este mesmo processo para todo monômio, temos que $\{x^{e_1}y^{e_2}z^{e_3} : e_1, e_2, e_3 \in \mathbb{N}\}$ é uma base para a álgebra envolvente universal de L.

3) Seja $L = \langle x, y : [x, y] = y\rangle$ a álgebra bidimensional não abeliana. Então, $\{x^{e_1}y^{e_2} : e_1, e_2 \in \mathbb{N}\}$ é base da álgebra envolvente universal U de L.

4) Seja $L = \langle x, y, z : [x, y] = z\rangle$ a álgebra de Heisenberg. Então, se U é a envolvente universal de L, temos que $\{x^{e_1}y^{e_2}z^{e_3} : e_1, e_2, e_3 \in \mathbb{N}\}$ é base de U.

Observação 1.6.5. Sejam L e H duas álgebras de Lie isomorfas. Então, se U_L e U_H são as álgebras envolventes universais de L e H, respectivamente, segue que U_L e U_H são isomorfas. Porém, as envolventes universais serem isomorfas não necessariamente implica no isomorfismo entre suas respectivas álgebras de Lie. Por exemplo,

$$L = \langle x_1, x_2, x_3, x_4, x_5 : [x_1, x_2] = x_3, [x_1, x_3] = x_4, [x_1, x_4] = x_5, [x_2, x_3] = x_5\rangle,$$

$$H = \langle x_1, x_2, x_3, x_4, x_5 : [x_1, x_2] = x_3, [x_1, x_3] = x_4, [x_1, x_4] = x_5\rangle$$

são duas $\mathbb{F}$- álgebras de Lie não isomorfas (item 1 do Exemplo 1.2.7) . No Artigo [SU11], os autores mostram no Lemma 3.2 que o ideal de aumento de U_L e U_H (o ideal de aumento de uma envolvente universal será definido e estudado no Capítulo 5 desta dissertação) são isomorfos quando a característica do corpo é igual a dois, então, pelo Lemma 2.2 desse mesmo artigo, temos que U_L e U_H são isomorfas. Isso mostra que é possível obter duas álgebras de Lie não isomorfas tais que suas envolventes universais são isomorfas.

Capítulo 2

Outras definições e resultados essenciais

Neste capítulo, iremos apresentar algumas definições e resultados da teoria de álgebras associativas, da teoria de formas quadráticas e da teoria de números que serão importantes para os capítulos subsequentes.

2.1 Álgebras associativas

Nesta seção, iremos enunciar alguns resultados interessantes sobre as álgebras associativas que serão utilizados no decorrer desta dissertação. Começamos com algumas definições.

Seja A uma álgebra associativa sobre um corpo $\mathbb{F}$. De maneira análoga a definição de L^n quando L é uma álgebra Lie sobre um corpo $\mathbb{F}$, temos a definição de A^n, que será a álgebra gerada pelos produtos de n elementos de A, isto é, $A^n := \text{span}\{a_1 \cdots a_n \colon a_i \in A\}$. Notemos ainda que, assim como no caso das álgebras de Lie, A^n é um ideal de A para todo $n \geq 1$.

Definição 2.1.1. Seja A uma álgebra associativa sobre um corpo $\mathbb{F}$. Dizemos que A é `residualmente nilpotente` se $\bigcap_{n\geq 1} A^n = \{0\}$.

Agora iremos definir a álgebra graduada de uma álgebra associativa. Seja A uma álgebra associativa. Notemos que $A^iA^j = A^{i+j}$. Definimos a `álgebra graduada` de A como sendo

$$\text{gr}(A) = \mathbb{F} \oplus \left(\bigoplus_{i\geq 1} \frac{A^i}{A^{i+1}} \right),$$

com o produto em $\text{gr}(A)$ induzido por

$$(a_1 \cdots a_i + A^{i+1})(b_1 \cdots b_j + A^{j+1}) = a_1 \cdots a_i \cdot b_1 \cdots b_j + A^{i+j+1}.$$

Notemos que, $\mathrm{gr}(A)$ é uma álgebra associativa com unidade. Quando A é uma álgebra associativa com unidade, então $A^n = A$ para todo $n \in \mathbb{N}$ e, assim, $\mathrm{gr}(A) \cong \mathbb{F}$.

Lema 2.1.2. *Seja A uma $\mathbb{F}$-álgebra associativa e consideremos a álgebra graduada $gr(A)$. Então, $gr(A)$ é uma $\mathbb{F}$-álgebra associativa e é gerada como $\mathbb{F}$-álgebra associativa por A/A^2.*

Demonstração. Seja $a \in \mathrm{gr}(A)$, então $a = \sum_i \alpha_i \overline{a}_i$ com $\overline{a}_i = a_{i_1} \cdots a_{i_t} + A^{t+1}$, $a_{i_s} \in A$ e $\alpha_i \in \mathbb{F}$. Notemos que, dados $b = \sum_j \beta_j \overline{b}_j$, $c = \sum_k \gamma_k \overline{c}_k \in \mathrm{gr}(A)$, temos que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ e, assim, $\mathrm{gr}(A)$ é uma álgebra associativa. Agora, notemos que para qualquer i temos que $\overline{a}_i = (a_{i_1} + A^2) \cdots (a_{i_t} + A^2)$, logo $\mathrm{gr}(A)$ é gerada por A/A^2 como $\mathbb{F}$-álgebra associativa. □

Agora iremos definir o conceito de álgebra simples e álgebra central para álgebras associativas com unidade e enunciaremos uma série de resultados importantes para os capítulos subsequentes.

Definição 2.1.3. Seja A uma álgebra associativa com unidade 1 sobre um corpo $\mathbb{F}$.

(i) Dizemos que A é uma $\mathbb{F}$-álgebra `simples` se os únicos ideais de A são $\{0\}$ e A.

(ii) Seja $\mathcal{Z}(A) = \{x \in A \colon xy = yx \text{ para todo } y \in A\}$ o centro de A. Dizemos que A é uma $\mathbb{F}$-álgebra `central` se $\mathcal{Z}(A) = \{\alpha 1 \colon \alpha \in \mathbb{F}\}$.

Se A é uma álgebra unidimensional com multiplicação trivial, isto é, $xy = 0$ para todos $x, y \in A$, então A é tanto uma álgebra associativa quanto uma álgebra de Lie. Observemos que A, considerada como álgebra associativa, é simples, porém A não é simples quando considerada como álgebra de Lie.

Exemplo 2.1.4.

1) Seja D uma $\mathbb{F}$-álgebra de divisão, ou seja, todo elemento não nulo em D tem inverso. Consideremos a $\mathbb{F}$-álgebra associativa $M_n(D)$ e seja J um ideal não trivial de $M_n(D)$. Tomemos $A = (a_{ij}) \in J$ tal que A possui pelo menos uma entrada não nula, digamos a_{hk}. Definamos a matriz E_{ij}, com $i \neq j$, como sendo a matriz com todas as entradas nulas, exceto pela entrada ij, que é igual a 1. Então, $B_i = E_{ih} A E_{ki} = a_{hk} E_{ii}$ e $B_i \in J$, pois J é um ideal de $M_n(D)$. Assim, $B = B_1 + \cdots + B_n = a_{hk} I \in J$, onde I é a matriz identidade, e, assim, $I \in J$. Logo, $J = M_n(D)$, e, portanto, $M_n(D)$ é uma $\mathbb{F}$-álgebra simples.

2) No exemplo acima, quando D é um corpo, temos que $M_n(D)$ é uma álgebra central simples sobre D. De fato, nesse caso, $\mathcal{Z}(M_n(D)) = \{\alpha I \colon \alpha \in \mathcal{Z}(D)\} = \{\alpha I \colon \alpha \in D\}$ que é isomorfo ao corpo D.

No teorema seguinte, veremos que, a menos de isomorfismo, as únicas $\mathbb{F}$-álgebras simples são as álgebras $M_n(D)$ onde D é uma $\mathbb{F}$-álgebra de divisão.

Teorema 2.1.5 (Wedderburn-Artin, página 171, [Jac89]). *Seja A uma álgebra simples com dimensão finita sobre um corpo $\mathbb{F}$. Então, A é isomorfa a uma álgebra de matrizes $M_n(D)$, onde n é um inteiro positivo e D é uma $\mathbb{F}$-álgebra de divisão.*

Nesta dissertação, estaremos interessados no caso em que A é uma $\mathbb{F}$-álgebra central simples de dimensão 4. Assim, do teorema acima, segue o seguinte corolário.

Corolário 2.1.6. *Se A é uma álgebra simples de dimensão 4 sobre $\mathbb{F}$, então ou A é uma álgebra de divisão, ou A é uma álgebra de matrizes 2×2 sobre $\mathbb{F}$.*

Quando A for uma álgebra associativa simples, teremos os seguintes resultados:

Teorema 2.1.7 (F15 e Definição 6, página 163, [Lor08]). *Seja A uma $\mathbb{F}$-álgebra simples e $\overline{\mathbb{F}}$ o fecho algébrico do corpo $\mathbb{F}$. Então,*

$$\dim_{\overline{\mathbb{F}}}(A \otimes \overline{\mathbb{F}}) = \dim_{\mathbb{F}}(A)$$

e $A \otimes \overline{\mathbb{F}}$ é simples.

Teorema 2.1.8 (Teorema 6, página 158, [Lor08]). *Se $\mathbb{F}$ é algebricamente fechado, então toda $\mathbb{F}$-álgebra simples de dimensão finita A é isomorfa à álgebra de matrizes $M_n(\mathbb{F})$ para algum $n \in \mathbb{N}$. Em particular, $\mathcal{Z}(A) = \mathbb{F}$ e $\dim_{\mathbb{F}}(A) = n^2$.*

Terminamos esta seção com o seguinte resultado sobre anéis de divisão finitos.

Teorema 2.1.9 (Wedderburn, página 214, [Lam01]). *Seja D um anel de divisão finito. Então, D é um corpo finito.*

2.2 Formas Quadráticas

Nesta seção, assumiremos sempre que V é um espaço vetorial de dimensão finita sobre um corpo $\mathbb{F}$ tal que a característica de $\mathbb{F}$ é diferente de 2.

Definição 2.2.1. Seja V um espaço vetorial de dimensão finita sobre um corpo $\mathbb{F}$ de característica diferente de 2. A aplicação $Q\colon V \to \mathbb{F}$ é chamada de `forma quadrática` se Q satisfaz as seguintes condições:

(i) $Q(\alpha v) = \alpha^2 Q(v)$, para todos $v \in V$ e $\alpha \in \mathbb{F}$;

(*ii***)** A aplicação $B\colon V \times V \to \mathbb{F}$ tal que $B(v,u) = (Q(v+u) - Q(v) - Q(u))/2$ é bilinear simétrica.

Notemos que, pelo item (ii), a forma quadrática pode ser reescrita na forma

$$Q(v) = B(v,v), \qquad \text{para todo } v \in V.$$

Dados V um espaço vetorial de dimensão finita sobre $\mathbb{F}$ e $Q\colon V \to \mathbb{F}$ uma forma quadrática, diremos que o par (V,Q) é um espaço quadrático.

Sejam (V,Q) um espaço quadrático, B a forma bilinear simétrica associada a Q e $\{e_1,\ldots,e_n\}$ uma base de V. Iremos agora dar uma notação matricial para a forma quadrática Q. Definimos M_Q como a matriz cuja entrada na posição (i,j) é igual a $B(e_i,e_j)$. Consideremos $v = x_1e_1 + \cdots + x_ne_n \in V$, então podemos considerar v como uma matriz $n \times 1$ com entradas iguais a $x_1,\ldots,x_n$, ou seja,

$$v = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Assim,

$$Q(v) = v^t M_Q v,$$

onde M_Q é a matriz referente à forma quadrática Q.

Exemplo 2.2.2.

1) Sejam $V_1 = \mathbb{F}^3$ e $\{e_1,e_2,e_3\}$ uma base de V_1. Tomemos $v = x_1e_1 + x_2e_2 + x_3e_3 \in V_1$ e consideremos a aplicação

$$Q_1(v) = x_1^2 + x_2^2 + x_3^2.$$

Então, Q_1 é uma forma quadrática e (V_1,Q_1) é um espaço quadrático.

2) Sejam $V_2 = \mathbb{F}^3$ e $\{f_1,f_2,f_3\}$ uma base de V_2. Tomemos $v = x_1f_1 + x_2f_2 + x_3f_3 \in V_2$ e consideremos a aplicação

$$Q_2(v) = x_1^2 + 4x_2^2 + x_3^2.$$

Então, Q_2 é uma forma quadrática e (V_2,Q_2) é um espaço quadrático.

Definição 2.2.3. Sejam (V_1,Q_1) e (V_2,Q_2) espaços quadráticos. Diremos que (V_1,Q_1) e (V_2,Q_2) são `isométricos` se existe um isomorfismo linear $\gamma\colon V_1 \to V_2$ tal que $Q_2(\gamma(v)) = Q_1(v)$ para todo $v \in V_1$, isto é, dadas $\mathcal{B}_1$ e $\mathcal{B}_2$ bases de V_1 e V_2, respectivamente, se M_γ é a matriz referente a γ nessas bases, então $M_\gamma^t M_{Q_2} M_\gamma = M_{Q_1}$. Neste caso, γ é dita uma `isometria`.

Vale mencionar que a definição acima independe das bases fixadas.

Exemplo 2.2.4. Sejam (V_1, Q_1) e (V_2, Q_2), respectivamente, os espaços quadráticos dos items 1 e 2 do Exemplo 2.2.2. Definamos $\gamma\colon V_1 \to V_2$ tal que $\gamma(e_1) = f_1$, $\gamma(e_2) = f_2/2$ e $\gamma(e_3) = f_3$. Então, se $v = x_1e_1 + x_2e_2 + x_3e_3 \in V_1$, segue que $\gamma(v) = x_1f_1 + x_2f_2/2 + x_3f_3$. Assim,

$$Q_2(\gamma(v)) = x_1^2 + x_2^2 + x_3^2 = Q_1(v)$$

e, portanto, (V_1, Q_1) e (V_2, Q_2) são isométricos.

Vamos introduzir o conceito de soma ortogonal. Sejam (V_1, Q_1) e (V_2, Q_2) dois espaços quadráticos e definamos $V = V_1 \oplus V_2$ e $B\colon V \times V \to \mathbb{F}$ é tal que

$$B(v_1 + v_2, u_1 + u_2) \;=\; B_1(v_1, u_1) + B_2(v_2, u_2), \tag{2.1}$$

onde B_1 e B_2 são as respectivas aplicações bilineares simétricas associadas a Q_1 e Q_2. Se Q é a forma quadrática associada a B, então (V, Q) é um espaço quadrático. Pela definição de B, temos que $B(V_1, V_2) = 0$ e restrição $B|_{V_i \times V_i}$ coincide com B_i. Assim, diremos que (V, Q), satisfazendo as condições acima, é a `soma ortogonal` de (V_1, Q_1) e (V_2, Q_2), e denotaremos $V = V_1 \perp V_2$.

Exemplo 2.2.5. Sejam (V_1, Q_1) e (V_2, Q_2) os espaços quadráticos do Exemplo 2.2.2 e consideremos $V = V_1 \oplus V_2$. O espaço quadrático (V, Q), onde Q é a forma quadrática associada à aplicação bilinear simétrica B definida por (2.1), é tal que $V = V_1 \perp V_2$. Por outro lado, se definirmos $\widetilde{B}\colon V \times V \to \mathbb{F}$ tal que para todos

$$v = x_1e_1 + x_2e_2 + x_3e_3 + x_4f_1 + x_5f_2 + x_6f_3 \qquad \text{e} \qquad u = y_1e_1 + y_2e_2 + y_3e_3 + y_4f_1 + y_5f_2 + y_6f_3$$

pertencentes a V, como

$$\widetilde{B}(v, u) = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 + x_6y_6,$$

logo $(V, \widetilde{Q})$, onde $\widetilde{Q}$ é a forma quadrática referente a $\widetilde{B}$, não é a soma ortogonal de (V_1, Q_1) e (V_2, Q_2). Porém, existe uma forma quadrática $\widetilde{Q}_2$ associada ao espaço vetorial V_2 tal que $(V, \widetilde{Q})$ é a soma ortogonal de (V_1, Q_1) e $(V_2, \widetilde{Q}_2)$. A saber, $\widetilde{Q}_2$ é tal que, para todo $v = x_1f_1 + x_2f_2 + x_3f_3 \in V_2$, $\widetilde{Q}_2(v) = x_1^2 + x_2^2 + x_3^2$.

Sejam V um espaço vetorial de dimensão 1 com uma base $\{e\}$ e Q a forma quadrática definida por $Q(e) = \alpha$ com $\alpha \in \mathbb{F}^*$. Denotaremos a classe de isometria de (V, Q) por $\langle\alpha\rangle$.

Corolário 2.2.6 (Corolário 2.4, página 7, [Lam05]). *Sejam (V, Q) um espaço quadrático sobre $\mathbb{F}$ e $\{e_1, \ldots, e_n\}$ uma base de V. Então, existem $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ tal que V é isométrico a $\langle\alpha_1\rangle\perp\ldots\perp\langle\alpha_n\rangle$. Em outras palavras, se $v = x_1e_1 + \cdots + x_ne_n \in V$, então $Q(v) = \alpha_1x_1^2 + \cdots + \alpha_nx_n^2$ e denotaremos essa forma quadrática por $\langle\alpha_1, \ldots, \alpha_n\rangle$.*

Pelo corolário acima, dado um espaço quadrático (V, Q), então existe uma forma diagonal, isto é, um forma D tal que M_D é uma matriz diagonal, tal que (V, Q) e (V, D) são isométricas, então existe uma matriz invertível M tal que $M_D = M^tM_QM$.

Corolário 2.2.7. *Sejam (V, Q) um espaço quadrático e M_Q a matriz referente à forma quadrática Q. Então, existe uma matriz invertível M que diagonaliza a matriz M_Q, isto é, M^tM_QM é uma matriz diagonal.*

Seja V um $\mathbb{F}$-espaço vetorial de dimensão n e seja $\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ sua forma quadrática. Então, V é isomorfo a $\langle\alpha_1\rangle\perp V'$ tal que $V' = \langle\alpha_2\rangle\perp\ldots\perp\langle\alpha_n\rangle$ e $\langle\alpha_2, \ldots, \alpha_n\rangle$ é a forma quadrática de V restrita a V'.

Estamos interessados em saber o que podemos dizer sobre as restrição das formas quadráticas de dois espaços quadráticos isométricos.

Teorema 2.2.8 (Witt's Cancellation, página 12, [Lam05]). *Sejam V_1 e V_2 dois $\mathbb{F}$-espaços vetoriais de dimensão n e $\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ e $\langle\beta_1, \beta_2, \ldots, \beta_n\rangle$ suas respectivas formas quadráticas. Se $\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ e $\langle\beta_1, \beta_2, \ldots, \beta_n\rangle$ são isométricas e, além disso, $\alpha_1 = \beta_1$, então $\langle\alpha_2, \ldots, \alpha_n\rangle$ e $\langle\beta_2, \ldots, \beta_n\rangle$ são isométricas.*

Exemplo 2.2.9. Sejam (V_1, Q_1) e (V_2, Q_2) os espaços quadráticos do Exemplo 2.2.2. Então $\langle1, 1, 1\rangle$ e $\langle1, 4, 1\rangle$ são as formas quadráticas de V_1 e V_2, respectivamente. No Exemplo 2.2.4, já vimos que (V_1, B_1) e (V_2, B_2) são isométricos, portanto, pelo Teorema 2.2.8, $\langle1, 1\rangle$ e $\langle4, 1\rangle$ são isométricas. De fato, para verificar essa isometria, basta considerar γ, do Exemplo 2.2.4, restrito ao espaço $\text{span}_{\mathbb{F}}\{e_2, e_3\}$.

Definição 2.2.10. Seja (V, Q) um $\mathbb{F}$-espaço quadrático.

(i) Dizemos que Q é `isotrópica` se existir pelo menos um $v \in V$ com $v \neq 0$ tal que $Q(v) = 0$.

(ii) Dizemos que Q é `anisotrópica` se quando $Q(v) = 0$ implica que $v = 0$.

Exemplo 2.2.11. Sejam (V_1, Q_1) e (V_2, Q_2) os espaços quadráticos do Exemplo 2.2.2. Se $\mathbb{F} = \mathbb{R}$, então ambas as formas são anisotrópicas. Se a característica de $\mathbb{F}$ é igual a 3, então ambas as formas são isotrópicas. De fato, tomemos $v = e_1 + e_2 + e_3 \in V_1$ e $u = f_1 + f_2 + f_3 \in V_2$, então

$$Q_1(v) = 1 + 1 + 1 = 0 \qquad \text{e} \qquad Q_2(u) = 1 + 4 + 1 = 0.$$

Quando estivermos com uma $\mathbb{F}$-álgebra de Lie L de dimensão finita, temos uma importante forma bilinear associada a essa álgebra de Lie, chamada forma de Killing.

Definição 2.2.12. Seja L uma álgebra de Lie de dimensão finita sobre um corpo $\mathbb{F}$. A `forma de Killing` de L é a aplicação bilinear $K\colon L \times L \to \mathbb{F}$ tal que $K(x,y) = \mathrm{tr}(\mathrm{ad}_x \mathrm{ad}_y)$, onde ad é a representação adjunta de L (item 2 do Exemplo 1.2.7) e tr é o traço da matriz (item 4 do Exemplo 1.1.2).

Notemos que K é de fato bilinear. Sejam $x, y, z \in L$ e $\alpha \in \mathbb{F}$, então

$$\begin{aligned} K(\alpha x + y, z) &= \mathrm{tr}(\mathrm{ad}_{\alpha x+y}\mathrm{ad}_z) \;=\; \mathrm{tr}((\alpha \mathrm{ad}_x + \mathrm{ad}_y)\mathrm{ad}_z) \\ &= \alpha \mathrm{tr}(\mathrm{ad}_x \mathrm{ad}_z) + \mathrm{tr}(\mathrm{ad}_y \mathrm{ad}_z) \\ &= \alpha K(x,z) + K(y,z). \end{aligned}$$

Dessa forma, quando $\mathbb{F}$ é um corpo de característica diferente de 2, temos que a aplicação $Q\colon L \to \mathbb{F}$ tal que $Q(x) = K(x,x)$ é uma forma quadrática.

Terminamos esta seção com o seguinte resultado sobre as formas quadráticas referentes às formas de Killing de duas álgebras de Lie isomorfas.

Teorema 2.2.13. *Sejam L e H duas álgebras de Lie de dimensão finita e Q_L, Q_H as formas quadráticas referentes a suas formas de Killing, respectivamente. Se L e H são isomorfas, então (L, Q_L) e (H, Q_H) são isométricas.*

Demonstração. Sejam L e H duas álgebras de Lie isomorfas. Assim, a imagem de uma base de L pelo isomorfismo $\phi\colon L \to H$ é uma base de H, isto é, se $\{x_1, \ldots, x_m\}$ é base de L, então $\{\phi(x_1), \ldots, \phi(x_m)\}$ é uma base de H. Se $x \in L$, então a matriz da ad_x na base $\{x_1, \ldots, x_m\}$ é igual à matriz da $\mathrm{ad}_{\phi(x)}$ na base $\{\phi(x_1), \ldots, \phi(x_m)\}$.

Seja K_L a forma de Killing de L e seja K_H a forma de Killing de H. Queremos mostrar que se Q_L e Q_H são as formas quadráticas relacionadas a K_L e K_H, respectivamente, então $Q_H(\phi(x)) = Q_L(x)$ para todo $x \in L$. De fato, como $\mathrm{ad}_x = \mathrm{ad}_{\phi(x)}$ para todo $x \in L$, temos que

$$Q_H(\phi(x)) = K_H(\phi(x), \phi(x)) = \mathrm{tr}(\mathrm{ad}_{\phi(x)}\mathrm{ad}_{\phi(x)}) = \mathrm{tr}(\mathrm{ad}_x \mathrm{ad}_x) = K_L(x,x) = Q_L(x).$$

□

2.3 Resíduos quadráticos

Nesta seção, faremos um breve resumo com definições e resultados de resíduos quadráticos, que serão utilizados no Capítulo 3.

Definição 2.3.1. Sejam $a, b, n \in \mathbb{Z}$ tal que $n > 0$. Dizemos que a é `congruente` a b módulo n, e escrevemos

$$a \equiv b \,(\text{mod } n)$$

se n divide $a - b$, ou seja, se a e b deixam o mesmo resto na divisão por n.

A congruência é uma relação de equivalência, isto é, ela é reflexiva, simétrica e transitiva.

Definição 2.3.2. Seja $n \in \mathbb{Z}$ tal que $n > 0$. Definimos $\phi(n)$ como a cardinalidade do conjunto $\{m \geq 1 \colon m \leq n \text{ e } \text{mdc}(m, n) = 1\}$. Essa função é conhecida como `phi de Euler`.

Teorema 2.3.3 (Euler-Fermat, Teorema 1.40, página 50, [MMST11])**.** *Sejam $a, m \in \mathbb{Z}^*$ com $m > 0$ e $mdc(a, m) = 1$. Então,*

$$a^{\phi(m)} \equiv 1 \,(\text{mod } m).$$

Exemplo 2.3.4. Como exemplo de aplicação do teorema acima mostraremos que existem infinitos números da forma $200\ldots0013$ que são múltiplos de 2013. Notemos que, demonstrar isso é equivalente a encontrar infinitos k tais que

$$2 \cdot 10^k + 13 \equiv 0 \,(\text{mod } 2013).$$

A expressão acima pode ser reescrita na forma $2 \cdot 10^k + 13 \equiv 2013 \,(\text{mod } 2013)$, que, por sua vez, podemos reescrevê-la na forma $2 \cdot 10^k \equiv 2000 \,(\text{mod } 2013)$. Como 2000 é invertível módulo 2013, temos então a expressão

$$10^{k-3} \equiv 1 \,(\text{mod } 2013).$$

Agora, como $\text{mdc}(10, 2013) = 1$, pelo teorema acima, $10^{\phi(2013)} \equiv 1 \,(\text{mod } 2013)$, o que implica que $10^{\phi(2013)t} \equiv 1 \,(\text{mod } 2013)$ para todo $t \in \mathbb{N}$. Dessa forma, basta tomar $k = \phi(2013)t + 3$.

Definição 2.3.5. Dados $a, n \in \mathbb{Z}$ com $n > 0$, dizemos que a é um `resíduo quadrático módulo` n se existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \,(\text{mod } n)$.

Definiremos agora o símbolo de Legendre, a fim de simplificar cálculos e notações.

Definição 2.3.6. Seja p um número primo maior que 2 e $a \in \mathbb{Z}$. O símbolo de Legendre, $\left(\frac{a}{p}\right)$, é definido como

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } p \text{ não divide } a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0 & \text{se } p \text{ divide } a \\ -1 & \text{caso contrário.} \end{cases}$$

Proposição 2.3.7 (Proposição 2.8 (Critério de Euler), página 88, [MMST11]). *Seja p um primo ímpar e $a \in \mathbb{Z}$. Então,*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Corolário 2.3.8 (Corolário 2.9, página 89, [MMST11]).

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

ou seja, -1 é resíduo quadrático módulo p se, e somente se, $p \equiv 1 \pmod{4}$ ou $p = 2$.

Teorema 2.3.9 (Reciprocidade Quadrática, Teorema 2.11, página 90, [MMST11]). *Seja p e q primos ímpares distintos. Então,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)\cdot(q-1)/4}.$$

Observação 2.3.10. Se p e q são primos distintos tais que $p \equiv 3 \pmod{4}$ e $q \equiv 3 \pmod{4}$, então ou p é resíduo quadrático módulo q; ou q é resíduo quadrático módulo p.

De fato,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1,$$

pois, nesse caso, $(p-1)/2$ e $(q-1)/2$ são números ímpares. Assim, temos dois casos:

$$\text{ou} \qquad \left(\frac{p}{q}\right) = 1 \qquad \text{e} \qquad \left(\frac{q}{p}\right) = -1$$

$$\text{ou} \qquad \left(\frac{p}{q}\right) = -1 \qquad \text{e} \qquad \left(\frac{q}{p}\right) = 1.$$

Proposição 2.3.11 (Proposição 8.3.1, página 95, [IR90]). *Seja $p \in \mathbb{Z}$ tal que $p \equiv 1 \pmod{4}$. Então, existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + y^2$.*

Teorema 2.3.12 (Teorema 7.8 (Dirichlet), página 319, [MMST11]). *Sejam $a, d \in \mathbb{N}$ tais que o máximo divisor comum entre eles é igual a 1. Então, existem infinitos números primos da forma $a + dn$ (com $n \in \mathbb{N}$). Em particular, se $d = 4$ e $a = 3$, existem infinitos números primos p tais que $p \equiv 3 \pmod{4}$.*

Capítulo 3

Álgebras dos quatérnios

Neste capítulo, estudaremos as álgebras dos quatérnios sobre um corpo $\mathbb{F}$ de característica diferente de 2. Temos como objetivo caracterizar essas álgebras a menos de isomorfismo e, para isso, faremos uso do famoso Teorema de Wedderburn-Artin (Teorema 2.1.5) e da forma normal associada à álgebra dos quatérnios. Iremos também classificar as álgebras dos quatérnios sobre alguns corpos conhecidos. Mais precisamente, veremos que, a menos de isomorfismo, existe uma única álgebra dos quatérnios tanto sobre $\mathbb{C}$ como sobre o corpo finito com q elementos $\mathbb{F}_q$; enquanto que sobre $\mathbb{R}$ existem duas álgebras dos quatérnios não isomorfas. Faremos também um breve estudo sobre as $\mathbb{Q}$-álgebras dos quatérnios, mostrando que existem, nesse caso, infinitas $\mathbb{Q}$-álgebras dos quatérnios não isomorfas. Os principais resultados aqui estudados podem ser encontrados no artigo [Lew06] de David W. Lewis e na dissertação de mestrado [Sha08] de Zi Yang Sham. Vamos assumir, em todo o capítulo, que $\mathbb{F}$ é um corpo de característica diferente de 2.

3.1 Definição, características e isomorfismos

Nesta seção, definiremos a álgebra dos quatérnios sobre um corpo $\mathbb{F}$ e mostraremos que essa álgebra é central simples. Dessa forma, poderemos usar o Corolário 2.1.6 do Teorema 2.1.5 de Wedderburn-Artin, que nos garantirá que a álgebra dos quatérnios ou é uma álgebra de divisão ou é isomorfa a uma álgebra de matrizes 2×2 sobre o corpo $\mathbb{F}$. Traremos também alguns exemplos de isomorfismos entre duas álgebras dos quatérnios e a classificação dessas álgebras sobre os corpos $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{F}_q$.

Dados $\alpha, \beta \in \mathbb{F}^*$, consideremos o espaço vetorial $A_{\alpha,\beta}$ sobre o corpo $\mathbb{F}$ com base $\{1, i, j, k\}$ e introduza a seguinte tabela de multiplicação para $A_{\alpha,\beta}$:

	1	i	j	k
1	1	i	j	k
i	i	α	k	αj
j	j	$-k$	β	$-\beta i$
k	k	$-\alpha j$	βi	$-\alpha\beta$

Dessa forma, temos que $A_{\alpha,\beta}$ é uma $\mathbb{F}$-álgebra e, além disso, podemos observar que $A_{\alpha,\beta}$ é uma $\mathbb{F}$-álgebra associativa.

Lema 3.1.1. *A $\mathbb{F}$-álgebra $A_{\alpha,\beta}$ é gerada por i,j e está definida com a apresentação*

$$A_{\alpha,\beta} := \langle i, j \colon i^2 = \alpha, j^2 = \beta, ij = -ji \rangle.$$

Demonstração. Sejam $A_{\alpha,\beta}$ a $\mathbb{F}$-álgebra que satisfaz a tabela acima, $B = \langle i, j \colon i^2 = \alpha, j^2 = \beta, ij = -ji \rangle$ e denotemos $k = ij$ em B. Observemos que $A_{\alpha,\beta}$ é gerada por i, j e satisfaz as relações de B. Então, $A_{\alpha,\beta}$ é um quociente da álgebra B, logo $\dim B \geq 4$.

Por outro lado, B é gerado por $\{1, i, j, k\}$ como espaço vetorial, logo $\dim B \leq 4$ e, portanto, $\dim B = \dim A_{\alpha,\beta} = 4$ e $B = A_{\alpha,\beta}$. □

Como exemplo temos que a álgebra dos quatérnios $\mathbb{H}$ sobre o corpo $\mathbb{R}$, gerada por i, j tais que $i^2 = j^2 = -1$ e $k = ij = -ji$, está definida, pelo lema anterior, por $\mathbb{H} = \langle i, j \colon i^2 = j^2 = -1, k = ij = -ji \rangle = A_{-1,-1}$.

Agora, definindo

$$[1] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad [i] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad [j] = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{e} \qquad [k] = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

temos que $\{[1], [i], [j], [k]\}$ é uma base para $M_2(\mathbb{F})$ como espaço vetorial. Observemos que

$$[i]^2 = [j]^2 = [1] \ \text{ e } \ [k] = [i][j] = -[j][i],$$

logo $M_2(\mathbb{F})$ é gerada por $[i], [j]$ como $\mathbb{F}$-álgebra e $\phi \colon M_2(\mathbb{F}) \to A_{1,1}$ tal que $\phi([i]) = i$ e $\phi([j]) = j$ é um isomorfismo entre $M_2(\mathbb{F})$ e $A_{1,1}$.

Finalmente, vale observar que $\mathbb{H}$ é uma álgebra de divisão. De fato, dado qualquer elemento não nulo $a = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$, temos que $a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0$ e $(a_0 - a_1 i - a_2 j - a_3 k)/(a_0^2 + a_1^2 + a_2^2 + a_3^2)$ é o inverso para a. No entanto, $M_2(\mathbb{F})$ não é uma álgebra de divisão, já que existem elementos não nulos que não possuem inverso em $M_2(\mathbb{F})$, por exemplo $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Portanto, quando $\mathbb{F} = \mathbb{R}$, teremos que $M_2(\mathbb{R})$ e $\mathbb{H}$ não são isomorfas e, dessa forma, as $\mathbb{R}$-álgebras $A_{1,1}$ e $A_{-1,-1}$ não são isomorfas.

Notemos que a apresentação da álgebra $A_{\alpha,\beta}$ depende da base fixada.

Exemplo 3.1.2.

1) Seja $A_{\alpha,\beta} = \langle i, j \colon i^2 = \alpha, j^2 = \beta, ij = -ji \rangle$ uma $\mathbb{F}$-álgebra dos quatérnios e denotemos $\overline{i} = j$ e $\overline{j} = i$. Notemos que

$$\overline{i}^2 = j^2 = \beta,$$

$$\overline{j}^2 = i^2 = \alpha,$$

$$\overline{i}\,\overline{j} = ji = -ij = -\overline{j}\,\overline{i},$$

logo ϕ tal que $\phi(i) = \overline{j}$ e $\phi(j) = \overline{i}$ é um isomorfismo entre $A_{\alpha,\beta}$ e $\langle \overline{i}, \overline{j} \colon \overline{i}^2 = \beta, \overline{j}^2 = \alpha, \overline{i}\,\overline{j} = -\overline{j}\,\overline{i} \rangle = A_{\beta,\alpha}$.

2) Podemos escrever a $\mathbb{F}$-álgebra $A_{\alpha,\beta}$ na forma $A_{\alpha,-\alpha\beta}$ através de uma mudança de base. De fato, denotemos $\overline{i} = i$ e $\overline{j} = k$, então

$$\overline{i}^2 = i^2 = \alpha,$$

$$\overline{j}^2 = k^2 = -\alpha\beta,$$

$$\overline{i}\,\overline{j} = ik = -ki = -\overline{j}\,\overline{i},$$

logo ϕ tal que $\phi(i) = \overline{i}$ e $\phi(j) = \dfrac{1}{\alpha}\overline{i}\,\overline{j}$ é um isomorfismo entre $A_{\alpha,\beta}$ e $\langle \overline{i}, \overline{j} \colon \overline{i}^2 = \alpha, \overline{j}^2 = -\alpha\beta, \overline{i}\,\overline{j} = -\overline{j}\,\overline{i} \rangle = A_{\alpha,-\alpha\beta}$.

3) Sejam $x, y \in \mathbb{F}$ tal que $x^2+y^2 \neq 0$ e $A_{-1,-(x^2+y^2)} = \langle i, j \colon i^2 = -1, j^2 = -(x^2+y^2), ij = -ji \rangle$. Denotemos $\overline{i} = i$ e $\overline{j} = (xj + yk)/(x^2 + y^2)$, então

$$\overline{i}^2 = i^2 = -1,$$

$$\overline{j}^2 = \frac{(xj+yk)^2}{(x^2+y^2)^2} = \frac{x^2j^2 + y^2k^2}{(x^2+y^2)^2} = \frac{-x^2(x^2+y^2) - y^2(x^2+y^2)}{(x^2+y^2)^2} = -\frac{x^2+y^2}{x^2+y^2} = -1,$$

$$\overline{i}\,\overline{j} = i\left(\frac{xj+yk}{x^2+y^2}\right) = \frac{xij + yik}{x^2+y^2} = \frac{-xji - yki}{x^2+y^2} = -\left(\frac{xj+yk}{x^2+y^2}\right) i = -\overline{j}\,\overline{i}.$$

Logo, ϕ tal que $\phi(i) = \overline{i}$ e $\phi(j) = x\overline{i} + y\overline{j}$ é um isomorfismo entre $A_{-1,-(x^2+y^2)}$ e $\langle \overline{i}, \overline{j} \colon \overline{i}^2 = -1, \overline{j}^2 = -1, \overline{i}\,\overline{j} = -\overline{j}\,\overline{i} \rangle = A_{-1,-1}$.

4) Dados $x, y \in \mathbb{F}$ não nulos, denotemos $\overline{i} = xi$ e $\overline{j} = yj$, então

$$\overline{i}^2 = x^2i^2 = \alpha x^2,$$

$$\overline{j}^2 = y^2 j^2 = \beta y^2,$$

$$\overline{i}\,\overline{j} = xiyj = -yjxi = -\overline{j}\,\overline{i},$$

logo ϕ tal que $\phi(i) = \frac{1}{x}\overline{i}$ e $\phi(j) = \frac{1}{y}\overline{j}$ é um isomorfismo entre $A_{\alpha,\beta}$ e $\langle \overline{i}, \overline{j} \colon \overline{i}^2 = \alpha x^2, \overline{j}^2 = \beta y^2, \overline{i}\,\overline{j} = -\overline{j}\,\overline{i} \rangle = A_{\alpha x^2, \beta y^2}$.

Um caso particular deste exemplo é quando $\sqrt{\alpha}, \sqrt{\beta} \in \mathbb{F}$. Nesse caso, tomamos $x = \frac{1}{\sqrt{\alpha}}$ e $y = \frac{1}{\sqrt{\beta}}$ e, dessa forma, $A_{\alpha,\beta}$ pode também ser escrito na forma $A_{1,1}$ através da mudança de base ϕ.

Dados $\alpha, \beta \in \mathbb{F}^*$, podemos concluir do último exemplo que, em geral, sempre que $\mathbb{F}$ é um corpo algebricamente fechado, $A_{\alpha,\beta}$ é isomorfa a $A_{1,1}$, que por sua vez é isomorfa à $\mathbb{F}$-álgebra $M_2(\mathbb{F})$. Temos, assim, a seguinte proposição.

Proposição 3.1.3. *Dados $\alpha, \beta \in \mathbb{F}^*$, se $\mathbb{F}$ é um corpo algebricamente fechado, então $A_{\alpha,\beta}$ é isomorfo a $M_2(\mathbb{F})$. Em particular, a menos de isomorfismo, $M_2(\mathbb{C})$ é a única álgebra dos quatérnios sobre $\mathbb{C}$.*

Consideremos agora $\mathbb{F}$ um corpo finito com q elementos. Denotamos, nesse caso, $\mathbb{F}$ por $\mathbb{F}_q$. Então, a $\mathbb{F}_q$-álgebra $A_{\alpha,\beta}$ é finita. Se $A_{\alpha,\beta}$ fosse uma álgebra de divisão, pelo Teorema 2.1.9, $A_{\alpha,\beta}$ seria um corpo finito. Porém, $A_{\alpha,\beta}$ é não comutativa, logo $A_{\alpha,\beta}$ não é uma álgebra de divisão. Segue, do Corolário 2.1.6, o seguinte resultado.

Proposição 3.1.4. *A álgebra $M_2(\mathbb{F}_q)$ é, a menos de isomorfismo, a única álgebra dos quatérnios sobre $\mathbb{F}_q$.*

Já vimos que sobre $\mathbb{R}$ temos pelo menos duas álgebras dos quatérnios, $\mathbb{H}$ e $M_2(\mathbb{R})$. Na próxima proposição veremos que, de fato, sobre $\mathbb{R}$ existem apenas dois casos de álgebras dos quatérnios $A_{\alpha,\beta}$: $A_{-1,-1} = \mathbb{H}$ e $A_{1,1}$ que é isomorfa a $M_2(\mathbb{R})$.

Proposição 3.1.5. *As álgebras $\mathbb{H}$ e $M_2(\mathbb{R})$ são, a menos de isomorfismo, as únicas álgebras dos quatérnios sobre $\mathbb{R}$.*

Demonstração. Sobre $\mathbb{R}$, podemos separar as escolhas de α, β em quatro casos:

Caso 1 - $\alpha, \beta > 0$**:**

Nesse caso, temos que $\sqrt{\alpha}, \sqrt{\beta} \in \mathbb{R}$, então, pelo item 4 do Exemplo 3.1.2, $A_{\alpha,\beta}$ é isomorfa a $A_{1,1}$, que por sua vez é isomorfa a $M_2(\mathbb{R})$.

Caso 2 - $\alpha, \beta < 0$**:**

Nesse caso, temos que $\sqrt{-\alpha}, \sqrt{-\beta} \in \mathbb{R}$, então, novamente pelo item 4 do Exemplo 3.1.2 e denotando $x = \dfrac{1}{\sqrt{-\alpha}}$ e $y = \dfrac{1}{\sqrt{-\beta}}$, concluímos que $A_{\alpha,\beta}$ é isomorfa a $A_{-1,-1}$, que por sua vez coincide com $\mathbb{H}$.

Caso 3 - $\alpha > 0$, $\beta < 0$**:**

Nesse caso, temos que $\sqrt{\alpha}, \sqrt{-\beta} \in \mathbb{R}$, então, pelo item 4 do Exemplo 3.1.2 e denotando $x = \dfrac{1}{\sqrt{\alpha}}$ e $y = \dfrac{1}{\sqrt{-\beta}}$, concluímos que $A_{\alpha,\beta}$ é isomorfa a $A_{1,-1}$. Agora, usando o item 2 do Exemplo 3.1.2, temos que $A_{1,-1}$ é isomorfa a $A_{1,1}$. Logo, nessas condições de α e β, $A_{\alpha,\beta}$ também é isomorfa a $A_{1,1}$, que, por sua vez, é isomorfa a $M_2(\mathbb{R})$.

Caso 4 - $\alpha < 0$, $\beta > 0$**:**

Pelo item 1 do Exemplo 3.1.2, temos que $A_{\alpha,\beta}$ é isomorfa a $A_{\beta,\alpha}$. Logo, pelo Caso 3 acima, segue que $A_{\alpha,\beta}$ é isomorfa a $M_2(\mathbb{R})$.

□

A fim de estudar o caso geral, mostraremos que $A_{\alpha,\beta}$ é uma álgebra central simples.

Lema 3.1.6. *A álgebra dos quatérnios $A_{\alpha,\beta}$ é uma $\mathbb{F}$-álgebra central simples.*

Demonstração. A fim de mostrarmos que $A_{\alpha,\beta}$ é central, notemos que $\mathbb{F} \subseteq \mathcal{Z}(A_{\alpha,\beta})$. Agora, tomemos $a = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{Z}(A_{\alpha,\beta})$. Como $a_0 \in \mathcal{Z}(A_{\alpha,\beta})$, temos que $b = a_1 i + a_2 j + a_3 k \in \mathcal{Z}(A_{\alpha,\beta})$.

Por um lado,

$$ib = i(a_1 i + a_2 j + a_3 k) = \alpha a_1 + a_2 k + \alpha a_3 j$$

e, por outro,

$$bi = (a_1 i + a_2 j + a_3 k)i = \alpha a_1 - a_2 k - \alpha a_3 j.$$

Como $ib = bi$,

$$a_2 k + \alpha a_3 j = -a_2 k - \alpha a_3 j,$$

o que implica que $a_2 = a_3 = 0$ e $b = a_1 i$.

Notemos que $jb = -a_1 k$ e $bj = a_1 k$, logo $a_1 = 0$ e $b = 0$. Portanto, $\mathcal{Z}(A_{\alpha,\beta}) = \mathbb{F}$ e $A_{\alpha,\beta}$ é central.

Agora, tomemos I um ideal não nulo de $A_{\alpha,\beta}$ e $a = a_0 + a_1 i + a_2 j + a_3 k$ um elemento não nulo de I. Queremos mostrar que $I = A_{\alpha,\beta}$, e para isso mostraremos que existe um elemento de $\mathbb{F}^*$ em I. Se $a_1 = a_2 = a_3 = 0$, então $a_0 \in I \cap \mathbb{F}^*$, pois $a \neq 0$, e temos $I = A_{\alpha,\beta}$. Assim, assumamos que algum a_1, a_2, a_3 é não nulo.

Notemos que

$$aj - ja = 2\beta a_3 i + 2a_1 k \in I,$$

$$ia - ai = 2\alpha a_3 j + 2a_2 k \in I.$$

Multiplicando ambos elementos pelo inverso de $2k$ à direita e à esquerda obtemos

$$(2k)^{-1}(2\beta a_3 i + 2a_1 k) = a_3 j + a_1 \in I,$$

$$(2\beta a_3 i + 2a_1 k)(2k)^{-1} = -a_3 j + a_1 \in I,$$

$$(2k)^{-1}(2\alpha a_3 j + 2a_2 k) = -a_3 i + a_2 \in I,$$

$$(2\alpha a_3 j + 2a_2 k)(2k)^{-1} = a_3 i + a_2 \in I.$$

Então,

$$(a_3 j + a_1) + (-a_3 j + a_1) = 2a_1 \in I,$$

$$(-a_3 i + a_2) + (a_3 i + a_2) = 2a_2 \in I,$$

e $a_1, a_2 \in I$ e $I = A_{\alpha,\beta}$ se $a_1 \neq 0$ ou $a_2 \neq 0$. Então, suponhamos que $a_1 = a_2 = 0$, o que implica $a_3 \neq 0$ e, assim, $a_3 j \in I$. Logo $(a_3 j)j = a_3\beta \in I$ e $a_3 \in I \cap \mathbb{F}^*$, portanto, $I = A_{\alpha,\beta}$ e $A_{\alpha,\beta}$ é simples. □

Temos assim que $A_{\alpha,\beta}$ é uma $\mathbb{F}$-álgebra associativa central simples de dimensão 4. Logo, segue do Corolário 2.1.6 que ou $A_{\alpha,\beta}$ é uma álgebra de divisão ou $A_{\alpha,\beta}$ é isomorfa a uma álgebra de matrizes 2×2 sobre $\mathbb{F}$.

Conforme vimos, se $\mathbb{F} = \mathbb{C}$ ou $\mathbb{F} = \mathbb{F}_q$, então $A_{\alpha,\beta}$ é isomorfa a $M_2(\mathbb{F})$ (Proposições 3.1.3 e 3.1.4), e se $\mathbb{F} = \mathbb{R}$, então $A_{\alpha,\beta}$ ou coincide com $\mathbb{H}$ ou é isomorfa a $M_2(\mathbb{R})$ (Proposição 3.1.5). Por outro lado, conforme veremos na Seção 3.4, se $\mathbb{F} = \mathbb{Q}$, então existem infinitas álgebras dos quatérnios não isomorfas.

3.2 Álgebras dos quatérnios e formas normais

Estaremos interessados em saber, em geral, quando $A_{\alpha,\beta}$ é uma álgebra de divisão ou é isomorfa a uma álgebra de matrizes 2×2 sobre $\mathbb{F}$. Para isso, veremos quais informações obtemos da álgebra $A_{\alpha,\beta}$ através de sua forma normal.

Definição 3.2.1. Seja $A_{\alpha,\beta}$ uma álgebra dos quatérnios sobre o corpo $\mathbb{F}$ e $a = a_0 + a_1 i + a_2 j + a_3 k \in A_{\alpha,\beta}$.

(i) Definimos o `conjugado` de a por $\overline{a} = a_0 - a_1 i - a_2 j - a_3 k$.

(*ii*) Definimos a `forma normal` (ou `norma`) de $A_{\alpha,\beta}$ como sendo a aplicação $N\colon A_{\alpha,\beta} \to \mathbb{F}$ tal que $N(a) = a\overline{a}$, para todo $a \in A_{\alpha,\beta}$.

Se $a = a_0 + a_1 i + a_2 j + a_3 k$, então $\overline{a} = a_0 - a_1 i - a_2 j - a_3 k$ e

$$\begin{aligned} a\overline{a} &= (a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k) \\ &= (a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2) + (-a_0 a_1 + a_1 a_0 + \beta a_2 a_3 - \beta a_3 a_2) i \\ &\quad +(-a_0 a_2 + a_2 a_0 - \alpha a_1 a_3 + \alpha a_3 a_1) j + (-a_0 a_3 + a_3 a_0 + a_1 a_2 - a_2 a_1) k \\ &= a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2, \end{aligned}$$

logo $a\overline{a} \in \mathbb{F}$ e N está bem definida.

Dada a forma normal N definimos a aplicação $B\colon A_{\alpha,\beta} \times A_{\alpha,\beta} \to \mathbb{F}$ como

$$B(a,b) = \frac{N(a+b) - N(a) - N(b)}{2}.$$

Como $N(a) = a\overline{a}$ para todo $a \in A_{\alpha,\beta}$, podemos assim expressar B na forma

$$B(a,b) = \frac{a\overline{b} + b\overline{a}}{2}.$$

Temos ainda que B é uma aplicação bilinear simétrica. De fato, temos que $B(a,b) = B(b,a)$ e

$$B(\delta a + b, c) = \frac{(\delta a + b)\overline{c} + c(\delta\overline{a} + \overline{b})}{2} = \frac{\delta(a\overline{c} + c\overline{a}) + (b\overline{c} + c\overline{b})}{2} = \delta B(a,c) + B(b,c)$$

para todos $a, b, c \in A_{\alpha,\beta}$ e $\delta \in \mathbb{F}$.

Notemos que se $a \in A_{\alpha,\beta}$ e $\delta \in \mathbb{F}$ então $N(\delta a) = \delta^2 N(a)$ segue direto da definição de N. Dessa forma, temos o seguinte lema:

Lema 3.2.2. *A forma normal N de $A_{\alpha,\beta}$ é uma forma quadrática.*

Denotaremos N por $\langle 1, -\alpha, -\beta, \alpha\beta\rangle$.

Seja $a \in A_{\alpha,\beta}$ não nulo. $N(a) \neq 0$ implica que a possui inverso, a saber $a^{-1} = \overline{a}/N(a)$. Por outro lado, se $N(a) = a\bar{a} = 0$, a é divisor de zero, então a não pode ser invertível. Portanto, a é invertível se, e somente se, $N(a) \neq 0$.

Pela Definição 2.2.10, temos que N pode ser anisotrópica ou isotrópica, isto é,

1) se $N(a) = 0$ implica que $a = 0$, então N é *anisotrópica*;

2) se existe $a \in A_{\alpha,\beta}$ com $a \neq 0$ tal que $N(a) = 0$, então N é *isotrópica*.

Lema 3.2.3.

(*i*) *A* $\mathbb{F}$*-álgebra* $A_{\alpha,\beta}$ *é uma álgebra de divisão se, e somente se, sua norma é anisotrópica.*

(*ii*) *A* $\mathbb{F}$*-álgebra* $A_{\alpha,\beta}$ *é isomorfa a uma álgebra de matrizes* 2×2 *sobre o corpo* $\mathbb{F}$ *se, e somente se, sua norma é isotrópica.*

Demonstração. Se N é anisotrópica, então todo elemento não nulo de $A_{\alpha,\beta}$ possui inverso e, dessa forma, $A_{\alpha,\beta}$ é uma álgebra de divisão. Por outro lado, se $A_{\alpha,\beta}$ é uma álgebra de divisão, então todo elemento de $A_{\alpha,\beta}$ não nulo possui inverso, logo $N(a)\neq 0$ para todo a não nulo e N é anisotrópica. No caso que N é isotrópica, existe $a\in A_{\alpha,\beta}$ não nulo tal que $N(a)=0$, logo esse a é um divisor de zero e $A_{\alpha,\beta}$ não pode ser uma álgebra de divisão. Assim, pelo Corolário 2.1.6, $A_{\alpha,\beta}$ é isomorfa a uma álgebra de matrizes 2×2 sobre $\mathbb{F}$. Por outro lado, se $A_{\alpha,\beta}$ é isomorfa a $M_2(\mathbb{F})$, como em $M_2(\mathbb{F})$ existem elementos não nulos não invertíveis, então existe $a\in A_{\alpha,\beta}$ tal que $a\neq 0$ não possui inverso, portanto $N(a)=0$ e N é isotrópica. □

Exemplo 3.2.4.

1) Seja $A_{\alpha,\beta}$ tal que $\mathbb{F}=\mathbb{Q}$ ou $\mathbb{R}$ e $\alpha,\beta<0$. Neste caso, $A_{\alpha,\beta}$ é uma álgebra de divisão, pois, se $a=a_0+a_1i+a_2j+a_3k\in A_{\alpha,\beta}$ tal que $N(a)=0$, então

$$0=N(a)=a_0^2-\alpha a_1^2-\beta a_2^2+\alpha\beta a_3^2,$$

onde $a_0^2,\ -\alpha a_1^2,\ -\beta a_2^2,\ \alpha\beta a_3^2>0$. Logo, $a_0^2-\alpha a_1^2-\beta a_2^2+\alpha\beta a_3^2=0$ se, e somente se, $a_0=a_1=a_2=a_3=0$ e, assim, $a=0$.

2) A $\mathbb{F}$-álgebra $A_{\alpha,1}$ é isomorfa a $M_2(\mathbb{F})$ para todo $\alpha\in\mathbb{F}^*$, pois $\langle 1,-\alpha,-1,\alpha\rangle$ é isotrópica. De fato, tomemos $1+j\in A_{\alpha,1}$, então

$$N(1+j)=(1+j)(1-j)=1-j^2=1-1=0.$$

3) Se $\alpha\in\mathbb{F}\setminus\{0,1\}$, então a $\mathbb{F}$-álgebra $A_{\alpha,1-\alpha}$ é isomorfa a $M_2(\mathbb{F})$. De fato, calculando a norma do elemento $1+i+j\in A_{\alpha,1-\alpha}$, obtemos

$$N(1+i+j)=(1+i+j)(1-i-j)=1-i^2-j^2=1-\alpha-(1-\alpha)=0,$$

logo $\langle 1,-\alpha,-(1-\alpha),\alpha(1-\alpha)\rangle$ é isotrópica.

4) A $\mathbb{F}$-álgebra $A_{\alpha,-\alpha}$ é isomorfa a $M_2(\mathbb{F})$ para todo $\alpha \in \mathbb{F}^*$. De fato,

$$N(\alpha + k) = \alpha^2 + (-\alpha^2) = 0,$$

logo $\langle 1, -\alpha, \alpha, -\alpha^2 \rangle$ é isotrópica.

5) Se $x \in \mathbb{F}^*$ e $y \in \mathbb{F}$, então a $\mathbb{F}$-álgebra $A_{-1,x^2+y^2} = \langle i, j : i^2 = -1, j^2 = x^2 + y^2, k = ij = -ji \rangle$ é isomorfa a $M_2(\mathbb{F})$. De fato, tomando $a = x + yi + j \in A_{-1,x^2+y^2}$, obtemos

$$N(a) = x^2 - y^2 i^2 - j^2 = x^2 + y^2 - (x^2 + y^2) = 0,$$

logo $\langle 1, 1, -(x^2 + y^2), -(x^2 + y^2) \rangle$ é isotrópica.

3.3 Isomorfismos e isometrias

Dadas duas $\mathbb{F}$-álgebras $A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$, com formas normais N e N', respectivamente, estudaremos nesta seção quais condições são necessárias para que as $\mathbb{F}$-álgebras sejam isomorfas.

Pela Definição 2.2.3, temos que se N e N' são as normas referentes às $\mathbb{F}$-álgebras $A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$, respectivamente, então N e N' são isométricas se existe um isomorfismo γ entre $A_{\alpha,\beta}$ em $A_{\alpha',\beta'}$ como espaços vetoriais tal que $N'(\gamma(a)) = N(a)$, para todo $a \in A_{\alpha,\beta}$.

Teorema 3.3.1. *Sejam $A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$ duas $\mathbb{F}$-álgebras e N e N' suas normas, respectivamente. $A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$ são $\mathbb{F}$-álgebras isomorfas se, e somente se, N e N' são isométricas.*

A fim de demonstrar o teorema acima, demonstraremos primeiro alguns lemas.

Começamos observando que o subespaço vetorial de $A_{\alpha,\beta}$ gerado (como espaço vetorial) por i, j, k e denotado por $A^0_{\alpha,\beta}$ é uma álgebra de Lie simples de dimensão 3 com a operação comutador induzida da operação produto da $\mathbb{F}$-álgebra $A_{\alpha,\beta}$.

Proposição 3.3.2. *O subespaço vetorial $A^0_{\alpha,\beta}$ de $A_{\alpha,\beta}$ é uma álgebra de Lie simples.*

Demonstração. Notemos que, como $[i, j] = 2k$, $[j, k] = -2\beta i$ e $[k, i] = -2\alpha j$, temos que $A^0_{\alpha,\beta}$ é fechado sob a operação comutador, logo $A^0_{\alpha,\beta}$ é uma álgebra de Lie. Agora, se $A^0_{\alpha,\beta}$ tivesse um ideal próprio $I \neq 0$, então teríamos que $A^0_{\alpha,\beta}/I$ e I teriam dimensão 1 ou 2, logo seriam solúveis e, pela Proposição 1.4.9, $A^0_{\alpha,\beta}$ seria solúvel. Entretanto, $[A^0_{\alpha,\beta}, A^0_{\alpha,\beta}] = A^0_{\alpha,\beta}$, logo $A^0_{\alpha,\beta}$ não é solúvel e, assim, não existe tal ideal I. Portanto, $A^0_{\alpha,\beta}$ é simples. □

A fim de facilitar nossa notação, sempre que tivermos um elemento $a = a_0 + a_1 i + a_2 j + a_3 k \in A_{\alpha,\beta}$ não nulo, o denotaremos por $a = a_0 + \dot{a}$, onde $a_0 \in \mathbb{F}$ e $\dot{a} = a_1 i + a_2 j + a_3 k \in A^0_{\alpha,\beta}$.

Lema 3.3.3. *Seja $a \in A_{\alpha,\beta}$ não nulo. Então, $a \in A^0_{\alpha,\beta}$ se, e somente se, $a^2 \in \mathbb{F}$ e $a \notin \mathbb{F}$.*

Demonstração. Notemos que

$$a^2 = (a_0 + \dot{a})^2 = (a_0^2 + \alpha a_1^2 + \beta a_2^2 - \alpha\beta a_3^2) + 2a_0(a_1 i + a_2 j + a_3 k).$$

Se $a \in A^0_{\alpha,\beta}$, então $a_0 = 0$ e, consequentemente, $a^2 \in \mathbb{F}$ e $a \notin \mathbb{F}$.

Por outro lado, se $a \notin \mathbb{F}$, temos que $a_i \neq 0$ para pelo menos um $i = 1, 2, 3$, então para que $a^2 \in \mathbb{F}$ precisamos de $a_0 = 0$, logo $a \in A^0_{\alpha,\beta}$. □

Lema 3.3.4. *Se $\Phi\colon A_{\alpha,\beta} \to A_{\alpha',\beta'}$ é um isomorfismo de álgebras associativas, então a restrição de Φ a $A^0_{\alpha,\beta}$ induz um isomorfismo de álgebras de Lie entre $A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$.*

Demonstração. Pelo Lema 3.3.3, se $a \in A^0_{\alpha,\beta}$, então $a^2 \in \mathbb{F}$ e $a \notin \mathbb{F}$. Como Φ é um isomorfismo de álgebras, temos que $(\Phi(a))^2 = \Phi(a^2) \in \mathbb{F}$ e $\Phi(a) \notin \mathbb{F}$ e, consequentemente, $\Phi(a) \in A^0_{\alpha',\beta'}$. Logo $\Phi(A^0_{\alpha,\beta}) = A^0_{\alpha',\beta'}$.

Notemos que, para todos $a, b \in A_{\alpha,\beta}$,

$$\Phi([a,b]) = \Phi(ab - ba) = \Phi(a)\Phi(b) - \Phi(b)\Phi(a) = [\Phi(a), \Phi(b)]$$

e, assim, Φ induz um isomorfismo de álgebras de Lie entre $A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$. □

Agora, demonstraremos o Teorema 3.3.1.

Demonstração. Seja $\Phi\colon A_{\alpha,\beta} \to A_{\alpha',\beta'}$ um isomorfismo de álgebras e tomemos $a = a_0 + \dot{a} \in A_{\alpha,\beta}$, então $\overline{a} = a_0 - \dot{a}$. Notemos que $\Phi(a) = a_0 + \Phi(\dot{a})$ e $\Phi(\overline{a}) = a_0 - \Phi(\dot{a})$. Pelo Lema 3.3.4, como $\Phi(\dot{a}) \in A^0_{\alpha',\beta'}$, temos que $\Phi(\overline{a}) = \overline{\Phi(a)}$. Dessa forma,

$$N'(\Phi(a)) = \Phi(a)\overline{\Phi(a)} = \Phi(a)\Phi(\overline{a}) = \Phi(a\overline{a}) = \Phi(N(a)) = N(a).$$

Logo N e N' são isométricas.

Assumamos que N e N' são isométricas. Pelo Teorema de Cancelamento de Witt (Teorema 2.2.8), temos que $\langle -\alpha, -\beta, \alpha\beta\rangle$ e $\langle -\alpha', -\beta', \alpha'\beta'\rangle$ são isométricas, então existe uma isometria $\sigma\colon A^0_{\alpha,\beta} \to A^0_{\alpha',\beta'}$. Notemos que se B_0 e B_0' são as aplicações bilineares referentes a N_0 e N_0' (N_0 é a forma normal de $A_{\alpha,\beta}$ restrita a $A^0_{\alpha,\beta}$), respectivamente, temos que $B_0'(\sigma(a), \sigma(b)) = B_0(a,b)$. Por um lado, como $\overline{c} = -c$ para todo $c \in A^0_{\alpha,\beta}$, temos que

$$B_0(a,b) = \frac{-ab - ba}{2}$$

e, por outro lado

$$B_0'(\sigma(a),\sigma(b)) = \frac{-\sigma(a)\sigma(b) - \sigma(b)\sigma(a)}{2}.$$

Dessa forma, podemos observar que $\sigma(i)^2 = \alpha$, $\sigma(j)^2 = \beta$ e $\sigma(i)\sigma(j) = -\sigma(j)\sigma(i)$. Assim, a aplicação $\widetilde{\sigma}\colon A_{\alpha,\beta} \to A_{\alpha',\beta'}$ tal que $\widetilde{\sigma}(i) = \sigma(i)$ e $\widetilde{\sigma}(j) = \sigma(j)$ é um isomorfismo entre $A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$. □

Agora, consideremos a forma de Killing K da álgebra de Lie $A^0_{\alpha,\beta}$. Temos que $K\colon A^0_{\alpha,\beta} \times A^0_{\alpha,\beta} \to \mathbb{F}$ é tal que $K(a,b) = \mathrm{tr}(\mathrm{ad}_a\mathrm{ad}_b)$.

Notemos que, como $[i,j] = 2k$, $[j,k] = -2\beta i$ e $[k,i] = -2\alpha j$, então

$$\mathrm{ad}_i = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 2\alpha \\ 0 & 2 & 0 \end{pmatrix}, \qquad \mathrm{ad}_j = \begin{pmatrix} 0 & 0 & -2\beta \\ 0 & 0 & 0 \\ -2 & 0 & 0 \end{pmatrix} \qquad \text{e} \qquad \mathrm{ad}_k = \begin{pmatrix} 0 & 2\beta & 0 \\ -2\alpha & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

logo

$$\begin{array}{lll} K(i,i) = 8\alpha, & K(i,j) = 0 & \text{e} \quad K(i,k) = 0, \\ K(j,i) = 0, & K(j,j) = 8\beta & \text{e} \quad K(j,k) = 0, \\ K(k,i) = 0, & K(k,j) = 0 & \text{e} \quad K(k,k) = -8\alpha\beta. \end{array}$$

Se Q é a forma quadrática relacionada à forma de Killing, temos que, para todo $a = a_1 i + a_2 j + a_3 k \in A^0_{\alpha,\beta}$,

$$Q(a) = 8\alpha a_1^2 + 8\beta a_2^2 - 8\alpha\beta a_3^2.$$

Por outro lado, se N_0 é a forma normal de $A_{\alpha,\beta}$ restrita a $A^0_{\alpha,\beta}$, então

$$N_0(a) = -\alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2,$$

logo $Q(a) = -8N_0(a)$.

Sejam Q e Q' as formas quadráticas referentes às formas de Killing de $A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$, respectivamente. Pelo Teorema 2.2.13, se $A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$ são isomorfas, então Q e Q' são isométricas.

Teorema 3.3.5. *Sejam $A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$ duas álgebras dos quatérnios e N e N' suas formas normais, respectivamente. Consideremos $A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$ as correspondentes álgebras de Lie e Q e Q' as formas quadráticas referentes a suas formas de Killing, respectivamente. Então, são equivalentes:*

(*i*) *$A_{\alpha,\beta}$ e $A_{\alpha',\beta'}$ são $\mathbb{F}$-álgebras associativas isomorfas;*

(*ii*) *N e N' são isométricas;*

(*iii*) *Q e Q' são isométricas;*

(*iv*) *$A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$ são $\mathbb{F}$-álgebras de Lie isomorfas.*

Demonstração. Pelo Lema 3.3.4, (i) implica em (iv). Segue do Teorema 3.3.1 que (i) é válida se, e somente se, (ii) é válida.

Pelo Teorema 2.2.13, temos que (iv) implica em (iii) e, para concluirmos o teorema, basta mostrar que se (iii) é válida então (ii) é válida.

Assim, se Q e Q' são isométricas, então N_0 e N_0' também o são, pois $Q = -8N_0$ e $Q' = -8N_0'$. Se $a = a_0 + a_1 i + a_2 j + a_3 k \in A_{\alpha,\beta}$, então $N(a) = a_0^2 + N_0(\dot{a})$. Logo, se N_0 e N_0' são isométricas, N e N' também o são e, assim, (iii) implica em (ii). □

3.4 Álgebras dos quatérnios sobre $\mathbb{Q}$

Nesta seção, iremos considerar apenas álgebras sobre o corpo $\mathbb{Q}$. Já vimos que, dados $\alpha, \beta \in \mathbb{Q}^*$, a $\mathbb{Q}$-álgebra $A_{\alpha,\beta}$ ou é isomorfa a $M_2(\mathbb{Q})$ ou é uma álgebra de divisão. Também já temos que a $\mathbb{Q}$-álgebra $A_{1,\alpha}$ é sempre isomorfa a $M_2(\mathbb{Q})$ (veja item 2 do Exemplo 3.2.4). Nesta seção, consideraremos p um número primo ímpar e estudaremos as $\mathbb{Q}$-álgebras $A_{-1,\pm p}$, concluindo que existem infinitas $\mathbb{Q}$-álgebras de divisão não isomorfas.

Iremos separar nosso estudo em dois casos: quando $p \equiv 1 \pmod 4$ e quando $p \equiv 3 \pmod 4$.

Se $p \equiv 1 \pmod 4$, pela Proposição 2.3.11, existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + y^2$. Segue do item 5 do Exemplo 3.2.4 que $A_{-1,p}$ é isomorfa a $M_2(\mathbb{F})$. Pelo item 1 do Exemplo 3.2.4 e item 3 do Exemplo 3.1.2, $A_{-1,-p}$ é uma álgebra de divisão isomorfa a $A_{-1,-1}$. Dessa forma, segue o seguinte resultado.

Proposição 3.4.1. *Seja p um primo tal que $p \equiv 1 \pmod 4$. Então a $\mathbb{Q}$-álgebra dos quatérnios $A_{-1,p}$ é isomorfa a $M_2(\mathbb{Q})$ e $A_{-1,-p}$ é uma álgebra de divisão isomorfa a $A_{-1,-1}$.*

Agora estaremos interessados no caso quando $p \equiv 3 \pmod 4$.

Proposição 3.4.2. *Sejam p e q inteiros positivos. Então,*

(i) *$A_{-1,p}$ e $A_{-1,-q}$ não são isomorfas;*

(ii) *$A_{-1,-q}$ é uma $\mathbb{Q}$-álgebra de divisão;*

(iii) *se p é um número primo tal que $p \equiv 3 \pmod 4$, então $A_{-1,p}$ é uma $\mathbb{Q}$-álgebra de divisão.*

Demonstração. A fim de provarmos (i), sejam $A_{-1,p} = \langle i, j : i^2 = -1, j^2 = p, k = ij = -ji \rangle$, $A_{-1,-q} = \langle \overline{i}\,\overline{j} : \overline{i}^2 = -1, \overline{j} = -q, \overline{k} = \overline{i}\,\overline{j} = -\overline{j}\,\overline{i} \rangle$ e N e N' suas formas normais, respectivamente. Consideremos as correspondentes álgebras de Lie $A^0_{-1,p}$ e $A^0_{-1,-q}$ e as formas quadráticas Q e Q' referentes a suas formas de Killing, respectivamente.

Por um lado, se $a = a_1 i + a_2 j + a_3 k \in A^0_{-1,p}$,

$$Q(a) = -8a_1^2 + 8pa_2^2 + 8pa_3^2$$

podemos assumir tanto valores negativos quanto positivos. Por outro lado,

$$Q'(a') = -8{a'_1}^2 - 8q{a'_2}^2 - 8q{a'_3}^2 \leq 0$$

para todo $a' = a'_1\overline{i} + a'_2\overline{j} + a'_3\overline{k} \in A^0_{-1,-q}$. Logo, essas duas formas não podem ser isométricas. Portanto, pelo Teorema 3.3.5, $A_{-1,p}$ e $A_{-1,-q}$ não são isomorfas.

Agora, (ii) segue pelo item 1 do Exemplo 3.2.4, $A_{-1,-q}$ é uma álgebra de divisão.

Finalmente, a fim de provarmos (iii), consideremos $a = a_0 + a_1 i + a_2 j + a_3 k \in A_{-1,p}$, então

$$N(a) = {a_0}^2 + {a_1}^2 - p{a_2}^2 - p{a_3}^2.$$

Queremos mostrar que $N(a) = 0$ implica que $a_0 = a_1 = a_2 = a_3 = 0$. Temos que $a_0, a_1, a_2, a_3 \in \mathbb{Q}$, se m é o mínimo múltiplo comum dos denominadores de a_0, a_1, a_2 e a_3, temos que $ma_i \in \mathbb{Z}$ para todo $i = 0, 1, 2, 3$ e, dessa forma, podemos assumir que $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, com o máximo divisor comum de a_0, a_1, a_2 e a_3 igual a 1, pois caso contrário basta dividir pelo fator comum.

Assim, se $N(a) = 0$, então

$$ {a_0}^2 + {a_1}^2 = p{a_2}^2 + p{a_3}^2.$$

Notemos que ${a_0}^2 + {a_1}^2 \equiv 0 \,(\text{mod } p)$. Se a_1 não é congruente a 0 módulo p, então a_1 é invertível e, assim, $(a_0 {a_1}^{-1})^2 \equiv -1 \,(\text{mod } p)$ e -1 é um resíduo quadrático módulo p. Logo, pelo Corolário 2.3.8, temos que $p \equiv 1 \,(\text{mod } 4)$, contrariando o fato de $p \equiv 3 \,(\text{mod } 4)$ e, portanto, $a_1 \equiv 0 \,(\text{mod } p)$. Assim, $a_0 \equiv 0 \,(\text{mod } p)$ e existem $x, y \in \mathbb{Z}$ tais que $a_0 = xp$ e $a_1 = yp$. Então, $p{a_2}^2 + p{a_3}^2 = {a_0}^2 + {a_1}^2 = x^2p^2 + y^2p^2$, logo $a_2^2 + a_3^2 = x^2p + y^2p$.

De maneira análoga, existem $z, w \in \mathbb{Z}$ tais que $a_2 = zp$ e $a_3 = wp$, o que contraria o fato do máximo divisor comum entre a_0, a_1, a_2 e a_3 ser 1. Portanto, a única solução é $a_0 = a_1 = a_2 = a_3 = 0$. Dessa forma, N é anisotrópica e, pelo item (ii) do Lema 3.2.3, $A_{-1,p}$ é uma álgebra de divisão. □

Teorema 3.4.3. *Sejam p e q primos distintos tais que $p \equiv 3 \,(\text{mod } 4)$ e $q \equiv 3 \,(\text{mod } 4)$. Então, $A_{-1,\pm p}$ e $A_{-1,\pm q}$ são $\mathbb{Q}$-álgebras de divisão não isomorfas.*

Demonstração. Pela Proposição 3.4.2, temos que $A_{-1,p}$ e $A_{-1,-q}$ são $\mathbb{Q}$-álgebras de divisão não isomorfas. O mesmo vale para as $\mathbb{Q}$-álgebras $A_{-1,-p}$ e $A_{-1,q}$.

A fim de estudarmos as $\mathbb{Q}$-álgebras $A_{-1,p}$ e $A_{-1,q}$, notemos que, pelo Lema 2.3.9 (Lei de Reciprocidade Quadrática), podemos supor, sem perda de generalidade, que p é um resíduo quadrático módulo q. Além disso, pelos itens 1 e 2 do Exemplo 3.1.2, podemos nos ater ao estudo das $\mathbb{Q}$-álgebras $A_{p,p} = \langle i, j \colon i^2 = j^2 = p, k = ij = -ji \rangle$ e $A_{q,q} = \langle \overline{i}, \overline{j} \colon \overline{i}^2 = \overline{j}^2 = q, \overline{k} = \overline{i}\,\overline{j} = -\overline{j}\,\overline{i} \rangle$, pois $A_{-1,p}$ e $A_{-1,q}$ são isomorfas a $A_{p,p}$ e $A_{q,q}$, respectivamente.

Suponhamos que $A_{p,p}$ e $A_{q,q}$ são isomorfas. Pelo Teorema 3.3.5, se Q e Q' são as formas quadráticas referentes às formas de Killing de $A^0_{p,p}$ e $A^0_{q,q}$, respectivamente, então Q e Q' são isométricas. Dessa forma, existe uma isometria $\sigma \colon A^0_{p,p} \to A^0_{q,q}$ tal que $Q'(\sigma(a)) = Q(a)$, para todo $a \in A^0_{p,p}$. Tomemos $a = i \in A^0_{p,p}$ e suponhamos que $\sigma(a) = a_1\overline{i} + a_2\overline{j} + a_3\overline{k}$, com $a_1, a_2, a_2 \in \mathbb{Q}$. Por um lado,

$$Q(a) = 8p$$

e, por outro lado,

$$Q'(\sigma(a)) = Q'(a_1\overline{i} + a_2\overline{j} + a_3\overline{k}) = 8qa_1^2 + 8qa_2^2 - 8q^2a_3^2.$$

Como σ é uma isometria, temos que $p = q(a_1^2 + a_2^2 - qa_3^2)$.

Se $a_1, a_2, a_3 \in \mathbb{Z}$, então essa igualdade é impossível e, assim, vamos assumir que a_i é uma fração com denominador diferente de 1 para pelo menos um $i = 1, 2, 3$. Multiplicando a equação pelo mínimo múltiplo comum dos denominadores de a_1^2, a_2^2 e a_3^2, podemos reescrevê-la na forma

$$x^2p = q(y^2 + z^2 - qw^2),$$

tal que $x, y, z, w \in \mathbb{Z}$ e $\mathrm{mdc}(x, y, z, w) = 1$.

Como q e p são primos distintos, temos que q divide x e, assim, existe $l \in \mathbb{Z}$ tal que $x = lq$. Substituindo na equação, temos que

$$qpl^2 \;=\; y^2 + z^2 - qw^2 \tag{3.1}$$

e, assim, $y^2 \equiv -z^2 \pmod{q}$.

Logo, temos duas possibilidades: $\mathrm{mdc}(y, q) = \mathrm{mdc}(z, q) = 1$ ou $\mathrm{mdc}(y, q) = \mathrm{mdc}(z, q) = q$.

Mostraremos que em ambos os casos obtemos uma contradição.

Caso 1 - $\mathrm{mdc}(y, q) = \mathrm{mdc}(z, q) = 1$**:**

Neste caso, pelo Teorema de Euler-Fermat (Teorema 2.3.3), $y^{q-1} \equiv 1 \pmod{q}$ e $z^{q-1} \equiv 1 \pmod{q}$. Como $y^2 \equiv -z^2 \pmod{q}$, temos que $(y^2)^{(q-1)/2} \equiv (-z^2)^{(q-1)/2} \pmod{q}$, o que implica em $y^{q-1} \equiv (-1)^{(q-1)/2} z^{q-1} \pmod{q}$ e, assim,

$$1 \equiv (-1)^{(q-1)/2} \pmod{q}.$$

Agora, como $q \equiv 3 \pmod 4$, temos que $q - 1 \equiv 2 \pmod 4$, o que implica que $(q-1)/(2)$ é um número ímpar e, assim, $(-1)^{(q-1)/2} = -1$. Logo, $1 \equiv -1 \pmod q$ e, portanto, q divide 2, contrariando o fato de q ser um número ímpar.

Caso 2 - $\mathrm{mdc}(y, q) = \mathrm{mdc}(z, q) = q$**:**

Neste caso, existem $y', z' \in \mathbb{Z}$ tais que $y = qy'$ e $z = qz'$. Logo, substituindo na Equação (3.1), temos que

$$pl^2 = qy'^2 + qz'^2 - w^2 \tag{3.2}$$

e, assim, $pl^2 \equiv -w^2 \pmod q$.

Novamente, temos, a princípio, duas possibilidades: $\mathrm{mdc}(l, q) = \mathrm{mdc}(w, q) = 1$ ou $\mathrm{mdc}(l, q) = \mathrm{mdc}(w, q) = q$. No entanto, como $\mathrm{mdc}(x, y, z, w) = 1$, então $\mathrm{mdc}(l, q) = \mathrm{mdc}(w, q) = 1$ é o único caso possível.

Trabalhando com a congruência $pl^2 \equiv -w^2 \pmod q$ e usando novamente o Teorema de Euler-Fermat (Teorema 2.3.3) e o fato de que $(q-1)/2$ ser um número ímpar, temos que

$$p^{(q-1)/2} \equiv -1 \pmod q.$$

Logo, pelo Critério de Euler (Proposição 2.3.7), p não é um resíduo quadrático módulo q, contrariando assim o fato de p ser um resíduo quadrático módulo q.

Portanto, σ não pode ser uma isometria e, assim, $A_{-1,p}$ e $A_{-1,q}$ não são isomorfas.
O raciocínio para $A_{-1,-p}$ e $A_{-1,-q}$ é análogo. □

Dessa forma, concluímos da Proposição 3.4.2 e do Teorema 3.4.3 que, se p é um número primo tal que $p \equiv 3 \pmod 4$, as $\mathbb{Q}$-álgebras $A_{-1,\pm p}$ são álgebras de divisão não isomorfas. Portanto, como o conjunto $\{p \in \mathbb{N}\colon p \text{ é primo}, p \equiv 3 \pmod 4\}$ é infinito (Teorema 2.3.12), temos infinitas $\mathbb{Q}$-álgebras de divisão.

Capítulo 4

Álgebras de Lie simples de dimensão 3

Já vimos na Seção 1.6 que se duas álgebras de Lie são isomorfas então suas álgebras envolventes universais também são isomorfas. Neste capítulo, veremos que no caso de álgebras de Lie simples de dimensão 3 sobre um corpo $\mathbb{F}$ de característica diferente de 2, duas álgebras envolventes universais serem isomorfas implica no isomorfismo entre as álgebras de Lie correspondentes. Isto é, duas álgebras de Lie L e H simples de dimensão 3 são isomorfas se, e somente se, suas envolventes universais U_L e U_H são isomorfas. Conforme veremos, o ponto chave está no fato de que toda $\mathbb{F}$-álgebra de Lie simples de dimensão 3 é isomorfa a uma $\mathbb{F}$-álgebra $A^0_{\alpha,\beta}$, para alguns $\alpha, \beta \in \mathbb{F}^*$. Os principais resultados aqui estudados podem ser encontrados no artigo [Mal92] de P. Malcolmson. Vamos assumir, em todo o capítulo, que $\mathbb{F}$ é um corpo de característica diferente de 2.

4.1 Redução ao estudo das álgebras $A^0_{\alpha,\beta}$

Nesta primeira seção, mostraremos que, dada uma álgebra de Lie L simples de dimensão 3 sobre o corpo $\mathbb{F}$, existem $\alpha, \beta \in \mathbb{F}^*$ tais que L é isomorfa à álgebra $A^0_{\alpha,\beta}$. Para tanto, mostraremos que existe uma base $\{x, y, z\}$ para L tal que $[y, z] = \lambda x,\ [z, x] = \mu y,\ [x, y] = z$, para alguns $\lambda, \mu \in \mathbb{F}^*$.

Seja L uma álgebra de Lie simples de dimensão 3 sobre $\mathbb{F}$. Denotemos por $S(x, y, z)$ a matriz dos coeficientes dos elementos $[y, z], [z, x]$ e $[x, y]$ na base $\{x, y, z\}$ de L. Isto é, se

$$[y,z] = a_{yz}^x x + a_{yz}^y y + a_{yz}^z z,$$

$$[z,x] = a_{zx}^x x + a_{zx}^y y + a_{zx}^z z,$$

$$[x,y] = a_{xy}^x x + a_{xy}^y y + a_{xy}^z z,$$

então

$$S(x,y,z) = \begin{pmatrix} a_{yz}^x & a_{yz}^y & a_{yz}^z \\ a_{zx}^x & a_{zx}^y & a_{zx}^z \\ a_{xy}^x & a_{xy}^y & a_{xy}^z \end{pmatrix}.$$

Lema 4.1.1. *Se L é uma álgebra de Lie simples de dimensão 3, então $S(x,y,z)$ é uma matriz simétrica.*

Demonstração. Se L é uma álgebra de Lie, então $[u,u] = 0$ para todo $u \in L$ e, assim,

$$[x,[y,z]] = a_{yz}^y [x,y] + a_{yz}^z [x,z],$$

$$[y,[z,x]] = a_{zx}^x [y,x] + a_{zx}^z [y,z],$$

$$[z,[x,y]] = a_{xy}^x [z,x] + a_{xy}^y [z,y].$$

Logo, pela identidade de Jacobi,

$$\begin{aligned} 0 &= [x,[y,z]] + [y,[z,x]] + [z,[x,y]] \\ &= a_{yz}^y [x,y] + a_{yz}^z [x,z] + a_{zx}^x [y,x] + a_{zx}^z [y,z] + a_{xy}^x [z,x] + a_{xy}^y [z,y] \\ &= (a_{zx}^z - a_{xy}^y)[y,z] + (a_{xy}^x - a_{yz}^z)[z,x] + (a_{yz}^y - a_{zx}^x)[x,y]. \end{aligned}$$

Como $3 = \dim L = \dim[L,L] = \dim\langle [y,z],[z,x],[x,y]\rangle$, segue que $[y,z]$, $[z,x]$ e $[x,y]$ são linearmente independentes e obtemos que $a_{zx}^z = a_{xy}^y$, $a_{xy}^x = a_{yz}^z$ e $a_{yz}^y = a_{zx}^x$. Portanto, $S(x,y,z)$ é simétrica. □

Seja $\{x',y',z'\}$ outra base de L tal que $x' = ax + by + cz$, $y' = dx + ey + fz$ e $z' = gx + hy + iz$, e

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}.$$

O lema seguinte nos permite relacionar as matrizes $S(x,y,z)$ e $S(x',y',z')$.

Lema 4.1.2. *Sejam $\{x,y,z\}$ uma base de L e $\{x',y',z'\}$ outra base de L nas condições acima, então*

$$S(x',y',z') = \det(A)(A^{-1})^t S(x,y,z) A^{-1}.$$

Demonstração. Notemos que $\det(A) \neq 0$, pois $\{x', y', z'\}$ é uma base de L, logo A possui inversa.

Temos que

$$[y', z'] = (ei - fh)[y, z] + (fg - di)[z, x] + (dh - eg)[x, y],$$

$$[z', x'] = (ch - bi)[y, z] + (ai - cg)[z, x] + (bg - ah)[x, y],$$

$$[x', y'] = (bf - ce)[y, z] + (cd - af)[z, x] + (ae - db)[x, y].$$

Seja $B = \mathrm{adj}(A^t)$, isto é,

$$B = \begin{pmatrix} ei - fh & fg - di & dh - eg \\ ch - bi & ai - cg & bg - ah \\ bf - ce & cd - af & ae - db \end{pmatrix}.$$

É conhecido que $A^t B = \det(A) I$, o que implica em

$$B = \det(A)(A^{-1})^t.$$

Seja C a matriz dos coeficientes dos elementos $[y, z], [z, x]$ e $[x, y]$ na base $\{x', y', z'\}$. Então, pela mudança de base, temos que $S(x, y, z) = CA$, o que implica em

$$C = S(x, y, z)A^{-1}.$$

Também pela mudança de base, temos que $S(x', y', z') = BC$, logo

$$S(x', y', z') = \det(A)(A^{-1})^t S(x, y, z)A^{-1}.$$

□

Teorema 4.1.3. *Seja L uma álgebra de Lie simples de dimensão 3 sobre um corpo $\mathbb{F}$ de característica diferente de 2. Então, existe uma base $\{x, y, z\}$ de L tal que, para alguma escolha de $\lambda, \mu \in \mathbb{F}^*$, $L = \langle x, y, z : [y, z] = \lambda x, [z, x] = \mu y, [x, y] = z \rangle$.*

Demonstração. Para demonstrar o teorema, é suficiente provar que existe uma base de L tal que $S(x, y, z)$ é diagonal.

Pelo Lema 4.1.1, $S(x, y, z)$ é simétrica, então podemos ver $S(x, y, z)$ como uma matriz associada a uma forma quadrática, e pelo Corolário 2.2.7, existe uma matriz P tal que $P^t S(x, y, z)P$ é diagonal.

Assim, existe uma base $\{x', y', z'\}$ de L tal que os coeficientes de x', y' e z' na base $\{x, y, z\}$ correspondam, respectivamente, às entradas das colunas de P^{-1}. Pelo Lema 4.1.2,

$$S(x', y', z') = \det(P^{-1})P^t S(x, y, z)P,$$

logo $S(x', y', z')$ é diagonal. Então, podemos escrever

$$S(x', y', z') = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

para alguns $\alpha, \beta, \gamma \in \mathbb{F}^*$. Dessa forma, $[y', z'] = \alpha x', [z', x'] = \beta y'$ e $[x', y'] = \gamma z'$.

Agora, definimos $y'' = (1/\gamma)y'$, então

$$[y'', z'] = \frac{1}{\gamma}[y', z'] = \frac{1}{\gamma}\alpha x',$$

$$[z', x'] = \beta y' = \gamma\beta y'',$$

$$[x', y''] = \frac{1}{\gamma}[x', y'] = \frac{1}{\gamma}\gamma z' = z'$$

e, portanto, $S(x', y'', z') = \begin{pmatrix} \gamma^{-1}\alpha & 0 & 0 \\ 0 & \gamma\beta & 0 \\ 0 & 0 & 1 \end{pmatrix}$. □

Exemplo 4.1.4.

(1) A álgebra de Lie $sl_2(\mathbb{F})$, com a base formada pelos elementos

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ e } h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

cumpre que $[e, f] = h, [h, e] = 2e$ e $[h, f] = -2f$, logo essa base não satisfaz as condições acima. Porém, se tomarmos a base formada pelos elementos

$$x = \begin{pmatrix} 0 & 1/2 \\ -1/2 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \text{ e } z = \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix},$$

temos que $[y, z] = -x, [z, x] = y$ e $[x, y] = z$.

(2) Seja $su_3(\mathbb{F}) = \left\{ \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix} : a, b, c \in \mathbb{F} \right\}$. Como já vimos,

$$\left\{ x = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, z = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \right\}$$

é uma base para $su_3(\mathbb{F})$ e $[y, z] = -x, [z, x] = -y, [x, y] = -z$.

Dessa forma, tomando $x' = -x$, temos que $\{x', y, z\}$ é uma base para $su_3(\mathbb{F})$ e $[y, z] = -x = x', [z, x'] = -[z, x] = y$ e $[x', y] = -[x, y] = z$.

Teorema 4.1.5. *Seja L uma álgebra de Lie simples de dimensão 3. Então, L é isomorfa a $A^0_{\alpha,\beta} = \langle i, j, k \colon [j, k] = -2\beta i, [k, i] = -2\alpha j, [i, j] = 2k \rangle$ para alguma escolha de $\alpha, \beta \in \mathbb{F}^*$.*

Demonstração. Pelo Teorema 4.1.3, $L = \langle x, y, z \colon [y, z] = \lambda x, [z, x] = \mu y, [x, y] = z \rangle$ para alguma escolha de $\lambda, \mu \in \mathbb{F}^*$. Definimos $\psi \colon L_{\lambda,\mu} \to A^0_{-\mu,-\lambda}$ tal que $\psi(x) = i/2$, $\psi(y) = j/2$ e $\psi(z) = k/2$.

Como

$$\psi([y, z]) = \psi(\lambda x) = \frac{\lambda}{2} i,$$

$$[\psi(y), \psi(z)] = \left[\frac{j}{2}, \frac{k}{2}\right] = \frac{\lambda}{2} i,$$

$$\psi([z, x]) = \psi(\mu y) = \frac{\mu}{2} j,$$

$$[\psi(z), \psi(x)] = \left[\frac{k}{2}, \frac{i}{2}\right] = \frac{\mu}{2} j,$$

$$\psi([x, y]) = \psi(z) = \frac{1}{2} k,$$

$$[\psi(x), \psi(y)] = \left[\frac{i}{2}, \frac{j}{2}\right] = \frac{1}{2} k,$$

segue que ψ é um isomorfismo de álgebras de Lie.

Tomando $\alpha = -\mu$ e $\beta = -\lambda$, temos que L é isomorfa a $A^0_{\alpha,\beta}$. □

Como exemplo temos que $sl_2(\mathbb{F})$ é isomorfa a $A^0_{-1,1}$ (veja item 1 do Exemplo 4.1.4), enquanto $su_3(\mathbb{F})$ é isomorfa a $A^0_{-1,-1}$ (veja item 2 do Exemplo 4.1.4).

Segue do teorema acima, das Proposições 3.1.3, 3.1.4 e 3.1.5 e do Teorema 3.4.3 o seguinte resultado.

Teorema 4.1.6. *Seja L uma álgebra de Lie simples de dimensão 3 sobre um corpo $\mathbb{F}$ de característica diferente de 2. Então,*

(*i*) *se $\mathbb{F} = \mathbb{C}$ ou $\mathbb{F} = \mathbb{F}_q$, existe, a menos de isomorfismo, apenas uma $\mathbb{F}$-álgebra de Lie simples de dimensão 3;*

(*ii*) *se $\mathbb{F} = \mathbb{R}$, existem, a menos de isomorfismo, duas $\mathbb{R}$-álgebras de Lie simples de dimensão 3 não isomorfas, a saber $A^0_{1,1}$ e $A^0_{-1,-1}$;*

(*iii*) *se $\mathbb{F} = \mathbb{Q}$, existem infinitas $\mathbb{Q}$-álgebras de Lie simples de dimensão 3 não isomorfas.*

4.2 Álgebra envolvente universal de L

Nesta seção, traremos o resultado mais importante deste capítulo, o qual diz que duas álgebras de Lie L e H simples de dimensão 3 são isomorfas se, e somente se, suas respectivas envolventes universais U_L e U_H são isomorfas. Com este objetivo, utilizaremos o seguinte lema técnico.

Lema 4.2.1. *Se $\mathrm{tr}(a) = 0$, então a^2 é central em $M_2(\mathbb{F})$. Em particular, os elementos da forma $(ab - ba)^2$ são centrais em $M_2(\mathbb{F})$ para todos $a, b \in M_2(\mathbb{F})$.*

Demonstração. Se $a \in M_2(\mathbb{F})$, então $p(x) = x^2 - \mathrm{tr}(a)x + \det(a)$ é o polinômio característico de a. Se $\mathrm{tr}(a) = 0$, temos que $p(x) = x^2 + \det(a)$ é seu polinômio característico e $p(a) = 0$. Logo, $a^2 = -\det(a)I$, onde I é a matriz identidade 2×2, e, portanto, a^2 é central em $M_2(\mathbb{F})$.□

Teorema 4.2.2. *Seja L uma $\mathbb{F}$-álgebra de Lie simples de dimensão 3 e U sua álgebra envolvente universal. Então, U contém um único ideal maximal I de codimensão 4. Para esse ideal I, o anel quociente U/I é isomorfo a uma álgebra dos quatérnios. Mais precisamente, se $\alpha, \beta \in \mathbb{F}^*$ são tais que L é isomorfa a $A^0_{\alpha,\beta}$ e se I é o único ideal maximal de U de codimensão 4, então U/I é isomorfa a $A_{\alpha,\beta}$.*

Demonstração. Pelo Teorema 4.1.5, existem $\alpha, \beta \in \mathbb{F}^*$ tais que L é isomorfa a $A^0_{\alpha,\beta}$. Assim, podemos trabalhar com a $\mathbb{F}$-álgebra $A^0_{\alpha,\beta}$. Para simplificar a notação, denotaremos por $U_{\alpha,\beta}$ a álgebra envolvente universal de $A^0_{\alpha,\beta}$.

Notemos que $A_{\alpha,\beta} = \mathbb{F} \oplus A^0_{\alpha,\beta}$ (soma direta como espaço vetorial). Temos também que o automorfismo identidade de $A^0_{\alpha,\beta}$ é um homomorfismo de álgebras de Lie de $A^0_{\alpha,\beta}$ sobre $A_{\alpha,\beta}$, logo, pela propriedade universal das álgebras envolventes universais, existe um homomorfismo sobrejetivo natural de $U_{\alpha,\beta}$ sobre $A_{\alpha,\beta}$. Assim, pelo Primeiro Teorema do Isomorfismo (Teorema 1.2.8), se K é o núcleo desse homomorfismo, K é um ideal de codimensão 4 de $U_{\alpha,\beta}$ tal que $U_{\alpha,\beta}/K$ é isomorfo a $A_{\alpha,\beta}$. Como $A_{\alpha,\beta}$ é simples, então K é um ideal maximal de $U_{\alpha,\beta}$. E temos

assim garantida a existência de um ideal maximal I de codimensão 4 de $U_{\alpha,\beta}$ e também que, para esse ideal I, $U_{\alpha,\beta}/I$ é isomorfo a $A_{\alpha,\beta}$.

A fim de demonstrar a unicidade, suponhamos que J é um ideal maximal de codimensão 4 de $U_{\alpha,\beta}$. Então, $U_{\alpha,\beta}/J$ é uma $\mathbb{F}$-álgebra simples de dimensão 4.

Seja $\overline{\mathbb{F}}$ o fecho algébrico do corpo $\mathbb{F}$ e consideremos a $\overline{\mathbb{F}}$-álgebra $(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$. Pelo Teorema 2.1.7, $\dim_{\overline{\mathbb{F}}}((U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}) = \dim_{\mathbb{F}}(U_{\alpha,\beta}/J) = 4$ e $(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$ é uma $\overline{\mathbb{F}}$-álgebra simples. Logo, pelo Teorema 2.1.8, $(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$ é isomorfa a $M_2(\overline{\mathbb{F}})$ e $Z((U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}) = \overline{\mathbb{F}}$.

Como $(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$ é isomorfa a $M_2(\overline{\mathbb{F}})$, segue do Lema 4.2.1, que $(ab-ba)^2$ é central para todo $a,b\in(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$. Assim, como $U_{\alpha,\beta}/J$ está contida em $(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$, temos que $(ab-ba)^2$ também é um elemento central para todo $a,b\in U_{\alpha,\beta}/J$. Além disso, como $(U_{\alpha,\beta}/J)\otimes\overline{\mathbb{F}}$ é uma $\overline{\mathbb{F}}$-álgebra central, $U_{\alpha,\beta}/J$ é uma $\mathbb{F}$-álgebra central.

Denotemos a imagem de $i,j,k\in U_{\alpha,\beta}$ em $U_{\alpha,\beta}/J$ por $\overline{i},\overline{j},\overline{k}$. Então,

$$\overline{j}\,\overline{k}-\overline{k}\,\overline{j}=[\overline{j},\overline{k}]=-2\beta\overline{i},\qquad \overline{k}\,\overline{i}-\overline{i}\,\overline{k}=[\overline{k},\overline{i}]=-2\alpha\overline{j},\qquad \overline{i}\,\overline{j}-\overline{j}\,\overline{i}=[\overline{i},\overline{j}]=2\overline{k}\tag{4.1}$$

e, portanto, como a característica de $\mathbb{F}$ é diferente de 2, temos que $\overline{i}^2,\overline{j}^2$ e $\overline{k}^2$ são centrais em $U_{\alpha,\beta}/J$.

Dessa forma,

$$0=[\overline{i},\overline{j}^2]=\overline{j}[\overline{i},\overline{j}]+[\overline{i},\overline{j}]\overline{j}=2\overline{j}\,\overline{k}+2\overline{k}\,\overline{j},$$

$$0=[\overline{j},\overline{k}^2]=\overline{k}[\overline{j},\overline{k}]+[\overline{j},\overline{k}]\overline{k}=-2\beta\overline{k}\,\overline{i}-2\beta\overline{i}\,\overline{k},$$

$$0=[\overline{k},\overline{i}^2]=\overline{i}[\overline{k},\overline{i}]+[\overline{k},\overline{i}]\overline{i}=-2\alpha\overline{i}\,\overline{j}-2\alpha\overline{j}\,\overline{i},$$

logo

$$\overline{j}\,\overline{k}=-\overline{k}\,\overline{j},\qquad \overline{k}\,\overline{i}=-\overline{i}\,\overline{k},\qquad \overline{i}\,\overline{j}=-\overline{j}\,\overline{i}\tag{4.2}$$

e, substituindo nas equações de (4.1),

$$\overline{j}\,\overline{k}=-\beta\overline{i},\qquad \overline{k}\,\overline{i}=-\alpha\overline{j},\qquad \overline{i}\,\overline{j}=\overline{k}.\tag{4.3}$$

Por outro lado,

$$0=[\overline{i},\overline{j}\,\overline{k}+\overline{k}\,\overline{j}]=\overline{j}[\overline{i},\overline{k}]+[\overline{i},\overline{j}]\overline{k}+\overline{k}[\overline{i},\overline{j}]+[\overline{i},\overline{k}]\overline{j}=4(\alpha\overline{j}^2+\overline{k}^2),$$

e

$$0=[\overline{j},\overline{k}\,\overline{i}+\overline{i}\,\overline{k}]=\overline{k}[\overline{j},\overline{i}]+[\overline{j},\overline{k}]\overline{i}+\overline{i}[\overline{j},\overline{k}]+[\overline{j},\overline{i}]\overline{k}=-4(\overline{k}^2+\beta\overline{i}^2),$$

o que implica em

$$\overline{k}^2 \;=\; -\beta\overline{i}^2 \;=\; -\alpha\overline{j}^2. \tag{4.4}$$

Notemos que, por (4.3) e (4.2), $\overline{k}^2 = \overline{i}\,\overline{j}\,\overline{i}\,\overline{j} = -\overline{i}\,\overline{j}^2\,\overline{i}$. Segue de (4.4) e (4.2) que

$$\overline{k}^2 = \frac{1}{\alpha}\,\overline{i}\,\overline{k}^2\,\overline{i} = \frac{1}{\alpha}\,\overline{k}\,\overline{i}^2\,\overline{k} = -\frac{1}{\alpha\beta}\,\overline{k}^4.$$

De forma análoga,

$$\overline{i}^2 = \frac{1}{\alpha}\,\overline{i}^4 \qquad \text{e} \qquad \overline{j}^2 = \frac{1}{\beta}\,\overline{j}^4.$$

Se $\overline{k}^2 = 0$, segue de (4.2) e (4.3) que $0 = \overline{k}^2\,\overline{i} = -\overline{k}\,\overline{i}\,\overline{k} = \alpha\overline{j}\,\overline{k} = -\alpha\beta\overline{i}$ e, assim, $\overline{i} = 0$. Agora, de (4.1), temos que $\overline{j} = \overline{k} = 0$, contrariando a dimensão de $U_{\alpha,\beta}/J$ e, portanto, $\overline{k}^2 \neq 0$. Similarmente, concluímos que $\overline{i}^2, \overline{j}^2 \neq 0$.

Como $\overline{i}^2, \overline{j}^2$ e $\overline{k}^2$ são elementos centrais não nulos de $U_{\alpha,\beta}/J$, temos que $\overline{i}^2$, $\overline{j}^2$, $\overline{k}^2 \in \mathbb{F}^*$(pois $Z(U_{\alpha,\beta}/J) = \mathbb{F}$) e, portanto,

$$\overline{k}^2 = -\alpha\beta, \qquad \overline{i}^2 = \alpha \qquad \text{e} \qquad \overline{j}^2 = \beta.$$

Notemos que, de (4.2), (4.3) e das relações acima, $ij + ji$, $k - ij$, $i^2 - \alpha$, $j^2 - \beta \in J$. Por outro lado, K é o núcleo do homomorfismo sobrejetivo natural de $U_{\alpha,\beta}$ sobre $A_{\alpha,\beta}$, logo K é o ideal gerado por $i^2 - \alpha$, $j^2 - \beta$, $ij + ji$ e $k - ij$ e, assim, $K \subseteq J$. Como K é maximal e $J \neq U_{\alpha,\beta}$, segue que $K = J$. □

Corolário 4.2.3. *Sejam L e H duas álgebras de Lie simples de dimensão 3 e U_L e U_H suas álgebras envolventes universais, respectivamente. Então, L é isomorfa a H se, e somente se, U_L é isomorfa a U_H.*

Demonstração. Pelo Teorema 4.1.5, existem $\alpha, \beta, \alpha', \beta' \in \mathbb{F}^*$ tais que L é isomorfa a $A^0_{\alpha,\beta}$ e H é isomorfa a $A^0_{\alpha',\beta'}$. Assim, podemos trabalhar com as $\mathbb{F}$-álgebras $A^0_{\alpha,\beta}$ e $A^0_{\alpha',\beta'}$ e, para simplificar notação, denotaremos por $U_{\alpha,\beta}$ e $U_{\alpha',\beta'}$ suas álgebras envolventes universais, respectivamente. Notemos que, se $A^0_{\alpha,\beta}$ é isomorfa a $A^0_{\alpha',\beta'}$, então $U_{\alpha,\beta}$ é isomorfa a $U_{\alpha',\beta'}$.

Por outro lado, assumamos que $U_{\alpha,\beta}$ é isomorfa a $U_{\alpha',\beta'}$. Pelo Teorema 4.2.2, existem únicos ideais maximais I e J de codimensão 4 de $U_{\alpha,\beta}$ e $U_{\alpha',\beta'}$, respectivamente, tais que $U_{\alpha,\beta}/I$ é isomorfa a $A_{\alpha,\beta}$ e $U_{\alpha',\beta'}/J$ é isomorfa a $A_{\alpha',\beta'}$. Assim, como $U_{\alpha,\beta}$ é isomorfa a $U_{\alpha',\beta'}$, pela unicidade de I e J, temos que $U_{\alpha,\beta}/I$ é isomorfa a $U_{\alpha',\beta'}/J$, implicando que $A_{\alpha,\beta}$ é isomorfa a $A_{\alpha',\beta'}$. Pelo Teorema 3.3.5, segue que $A^0_{\alpha,\beta}$ é isomorfa a $A^0_{\alpha',\beta'}$. □

Capítulo 5

Álgebras de Lie nilpotentes

Neste capítulo, estamos interessados em estudar determinadas características de uma álgebra de Lie L de dimensão finita sobre um corpo $\mathbb{F}$ que são herdadas de sua álgebra envolvente universal U. Mais precisamente, mostraremos que o fato de L ser ou não nilpotente é determinado por sua envolvente universal U. Mostraremos também que se L é nilpotente, então o seu grau de nilpotência e o número mínimo de geradores de L também são determinados por U. Iremos ainda definir a álgebra graduada do ideal de aumento de U e mostraremos que a álgebra graduada de L é determinada pela álgebra envolvente universal U de L. Os principais resultados aqui estudados podem ser encontrados no artigo de [RU07] de David Riley e Hamid Usefi. Nesse artigo os autores mostram que os resultados supracitados são válidos também quando L é uma $\mathbb{F}$-álgebra de dimensão infinita.

5.1 Ideal de aumento

Sejam L uma álgebra de Lie de dimensão finita sobre um corpo $\mathbb{F}$ e U sua álgebra envolvente universal. Consideramos $\{x_1, x_2, \ldots, x_\ell\}$ uma base ordenada de L e definimos a `transformação de aumento` como sendo o homomorfismo $\varepsilon_L \colon U \to \mathbb{F}$ induzido por $\varepsilon_L(x_i) = 0$, para todo $i = 1, 2, \ldots, \ell$. O núcleo de ε_L é denominado `ideal de aumento` de U e será denotado por $\omega(L)$. Mostraremos que $\omega(L)$ é um ideal residualmente nilpotente de U se, e somente se, L é uma álgebra de Lie nilpotente .

Seja $m \in U$, então pelo Teorema de Poincaré-Birkhoff-Witt (Teorema 1.6.3), m é uma combinação linear de PBW-monômios, isto é,

$$m = \sum_{i_1,\ldots,i_\ell \in \mathbb{N}} \alpha_{i_1,\ldots,i_\ell} x_1^{i_1} \ldots x_\ell^{i_\ell}.$$

Pela definição de ε_L, temos que $\varepsilon_L(m) = \alpha_{0,\ldots,0}$, logo $\omega(L) = LU = UL$.

Na Observação 1.6.5 comentamos que dadas duas álgebras de Lie L e H, então suas envolventes universais U_L e U_H são isomorfas se, e somente se, $\omega(L)$ e $\omega(H)$ são isomorfos. Mostraremos que este resultado é de fato verdadeiro.

Definição 5.1.1. Sejam L uma álgebra de Lie e $B = \{x_1, x_2, \ldots, x_\ell\}$ uma base ordenada de L. Se $m = x_{j_1} \ldots x_{j_l} \in U$ é um monômio de Poincaré-Birkhoff-Witt (PBW-monômio), com $x_{j_i} \in B$ para todo $i = 1, \ldots l$, então denotaremos por $|m|$ o `comprimento` l de m.

Lema 5.1.2. *Sejam L e H duas álgebras de Lie cujas envolventes universais U_L e U_H, respectivamente são isomorfas. Então, existe um isomorfismo $\eta\colon U_L \to U_H$ tal que $\eta(\omega(L)) = \omega(H)$. Por outro lado, se $\omega(L)$ e $\omega(H)$ são isomorfas, então U_L e U_H também são isomorfas.*

Demonstração. Seja $\phi\colon U_L \to U_H$ isomorfismo e consideremos a aplicação $\widetilde{\eta}\colon L \to U_H$ definida $\widetilde{\eta}(x) = \phi(x) - \varepsilon_H(\phi(x))$ para todo $x \in L$. A aplicação $\widetilde{\eta}$ é uma transformação linear. Como observamos $\phi([x,y]) = \phi(x)\phi(y) - \phi(y)\phi(x)$ e $\varepsilon_H(U_H) \subseteq \mathbb{F}$, logo $\varepsilon_H(\phi([x,y]) = 0$ e $[\phi(x), \varepsilon_H(\phi(y))] = 0$. Portanto $\widetilde{\eta}([x,y]) = [\widetilde{\eta}(x), \widetilde{\eta}(y)]$ para todos $x, y \in L$ e, assim, $\widetilde{\eta}$ é um homomorfismo de álgebras de Lie.

Pela propriedade universal da álgebra envolvente U_L, existe um único η tal que o diagrama

$$\begin{array}{ccc} L & \xrightarrow{\ i\ } & U_L \\ & \searrow^{\widetilde{\eta}} & \downarrow \eta \\ & & U_H \end{array}$$

comuta. Além disso, η preserva unidade. Como $\widetilde{\eta}(L) \subseteq \omega(H)$, então $\eta(\omega(L)) \subseteq \omega(H)$. Queremos mostrar que η é um isomorfismo e, para isso, é equivalente mostrar que $\phi^{-1} \circ \eta$ é um isomorfismo.

A fim de mostrar que $\phi^{-1} \circ \eta$ é injetiva, seja $B = \{x_1, x_2, \ldots, x_\ell\}$ uma base ordenada de L e tomemos $m = \sum_{i_1,\ldots,i_\ell \in \mathbb{N}} \alpha_{i_1,\ldots,i_\ell} x_1^{i_1} \ldots x_\ell^{i_\ell} \in U_L$. Então,

$$\begin{aligned} \phi^{-1} \circ \eta(m) &= \phi^{-1}\left(\sum \alpha_{i_1,\ldots,i_\ell} \widetilde{\eta}(x_1)^{i_1} \ldots \widetilde{\eta}(x_\ell)^{i_\ell}\right) \\ &= \sum \alpha_{i_1,\ldots,i_\ell} (x_1 - \varepsilon_H(\phi(x_1)))^{i_1} \ldots (x_\ell - \varepsilon_H(\phi(x_\ell)))^{i_\ell} \\ &= m + \sum \alpha_{m'} m' \end{aligned}$$

onde $|m'|$ é menor que o comprimento dos monômios que aparecem na decomposição de m. Assim, $\phi^{-1} \circ \eta(m) = 0$ se, e somente se, $m = 0$. Logo, $\phi^{-1} \circ \eta$ é injetiva.

Para verificar que $\phi^{-1} \circ \eta$ é sobrejetiva, basta notar que $\mathbb{F} \subseteq \mathrm{Im}(\phi^{-1} \circ \eta)$ pois ϕ e η preservam unidade. Notemos também que, para todo $x \in L$, segue que $\phi^{-1} \circ \eta(x) = \phi^{-1} \circ \widetilde{\eta}(x) = x - \varepsilon_H(\phi(x))$ e, assim, $L \subseteq \mathrm{Im}(\phi^{-1} \circ \eta)$. Como $\mathbb{F}$ e L geram U_L como álgebra, segue que $\phi^{-1} \circ \eta$ é sobrejetiva.

Assim, $\phi^{-1} \circ \eta$ é isomorfismo e, portanto, η é um isomorfismo entre U_L e U_H tal que $\eta(\omega(L)) = \omega(H)$.

Seja $\psi\colon \omega(L) \to \omega(H)$ um isomorfismo. Como $U_L = \mathbb{F} \oplus \omega(L)$, definimos $\Psi\colon U_L \to U_H$ tal que $\Psi(\alpha) = \alpha$ para todo $\alpha \in \mathbb{F}$ e $\Psi(m') = \psi(m')$ para todo $m' \in \omega(L)$. A aplicação Ψ é linear pois ψ é linear. Queremos mostrar que Ψ é um isomorfismo. Tomemos $m_1, m_2 \in U_L$, então $m_1 = \alpha_1 + m_1'$ e $m_2 = \alpha_2 + m_2'$ onde $\alpha_1, \alpha_2 \in \mathbb{F}$ e $m_1', m_2' \in \omega(L)$. Como ψ é isomorfismo,

$$\begin{aligned}
\Psi(m_1 m_2) &= \Psi(\alpha_1\alpha_2 + \alpha_1 m_2' + \alpha_2 m_1' + m_1' m_2') \\
&= \alpha_1\alpha_2 + \alpha_1\psi(m_2') + \alpha_2\psi(m_1') + \psi(m_1')\psi(m_2') \\
&= (\alpha_1 + \psi(m_1'))(\alpha_2 + \psi(m_2')) \\
&= \Psi(m_1)\Psi(m_2),
\end{aligned}$$

logo Ψ é um homomorfismo. Para vermos que Ψ é injetivo, se $\Psi(m_1) = 0$, então $\alpha_1 + \psi(m_1') = 0$, o que implica que $\alpha_1 = \psi(m_1') = 0$. Como ψ é isomorfismo, temos que $m_1' = 0$ e, assim, $m_1 = 0$ e Ψ é injetiva. Desde que $\mathbb{F} \subseteq \Psi(U_L)$ e $\omega(H) \subseteq \psi(\omega(L)) \subseteq \Psi(U_L)$, concluímos que Ψ é sobrejetivo. Portanto, Ψ é um isomorfismo entre U_L e U_H. □

Definição 5.1.3. Sejam L uma álgebra de Lie e $B = \{x_1, x_2, \ldots, x_\ell\}$ uma base ordenada de L.

(*i*) Definimos o `peso` de $x \in L$ como sendo o maior n tal que $x \in L^n$ e $x \notin L^{n+1}$ ou como sendo infinito quando não existir esse n. Denotaremos o peso de $x \in L$ por $\nu(x)$.

(*ii*) Se $m = x_{j_1} \ldots x_{j_l} \in U$ é um PBW-monômio, com $x_{j_i} \in B$ para todo $i = 1, \ldots l$, então $\nu(m) := \nu(x_{j_1}) + \cdots + \nu(x_{j_l})$. Se $m \in \mathbb{F}$, então $\nu(m) := 0$.

(*iii*) Uma base ordenada B de L é dita `homogênea` se $L^n = \text{span}\{x_j \in B\colon \nu(x_j) \geq n\}$, para todo $n \geq 1$.

Lema 5.1.4. *Toda álgebra de Lie de dimensão finita possui uma base homogênea.*

Demonstração. Seja L uma álgebra de Lie de dimensão finita. Como L tem dimensão finita, sua série central descendente estabiliza, isto é, existe um $n \in \mathbb{N}$ tal que $L^n = L^{n+i}$ para todo $i \in \mathbb{N}$.

Sejam n tal que $L^{n-1} \supsetneq L^n = L^{n+1}$, $B_n = \{y_i\colon i \in \mathcal{I}\}$ uma base de L^n e $\overline{B}_{n-1} = \{x_j + L^n\colon j \in \mathcal{J}\}$ uma base de L^{n-1}/L^n. Para cada $j \in \mathcal{J}$, consideremos uma pré-imagem x_j de $x_j + L^n$ pelo homomorfismo canônico e definimos o conjunto $B_{n-1} = \{x_j\colon j \in \mathcal{J}\}$.

Lembremos que dados um espaço vetorial V, um subespaço vetorial U de V, B uma base de U e $\overline{B}$ uma base de V/U, então, se $\widetilde{B}$ é o conjunto das pré-imagens de $\overline{B}$ pelo homomorfismo canônico, temos que $B \cup \widetilde{B}$ é uma base de V. Portanto, como toda álgebra de Lie é um espaço vetorial, segue que $B_n \cup B_{n-1}$ é uma base de L^{n-1}.

Para encontrarmos uma base de L^{n-2} fazemos o mesmo processo, tomando a base $B_n \cup B_{n-1}$ de L_{n-1} e completando com o conjunto de pré-imagens pelo homomorfismo canônico da base $\overline{B}_{n-2} = \{z_k + L^{n-1} \colon k \in \mathcal{K}\}$ de L^{n-2}/L^{n-1}.

Como n é finito, podemos repetir esse processo até encontrarmos uma base de L e, pela definição de base homogênea, essa será uma base homogênea de L. □

Apesar do nosso foco ser o de trabalhar com álgebras de dimensão finita, temos que o lema acima vale também para álgebras nilpotentes quaisquer.

Nosso interesse nessa seção é mostrar que a álgebra de Lie L é nilpotente se, e somente se, $\omega(L)$ é um ideal residualmente nilpotente de U. Com essa finalidade, enunciaremos e demonstraremos uma série de lemas que nos permitirão provar o resultado desejado.

Dado um monômio $m = x_{i_1} \dots x_{i_k}$, não necessariamente ordenado, denotaremos por $\overline{m}$ o PBW-monômio que obtemos de m por ordenar as variáveis $x_{i_1}, \dots, x_{i_k}$. Por exemplo, se $B = \{x_1, x_2, x_3\}$ com $x_1 < x_2 < x_3$ então $\overline{x_3 x_2 x_1 x_2} = x_1 x_2^2 x_3$.

Lema 5.1.5. *Sejam $B = \{x_1, \dots, x_\ell\}$ uma base homogênea da álgebra de Lie L, $m = x_{i_1} \dots x_{i_k} \in U$ um PBW-monômio e $x_l \in L$. Então*

$$mx_l = \overline{mx_l} + \sum \alpha_{m'} m',$$

onde cada m' é um PBW-monômio com $|m'| \leq k$ e $\nu(m') \geq \nu(m) + \nu(x_l)$. Em particular mx_l é combinação linear de PBW-monômios de comprimento não maior que $k+1$ e peso não menor que $\nu(m) + \nu(x_l)$.

Demonstração. Faremos essa demonstração usando o processo de indução sobre o comprimento de m. Se $|m| = 0$, não temos nada para provar. Assumimos que a afirmação é válida para PBW-monômios de comprimento menor que k. Seja $m = x_{i_1} \dots x_{i_k}$. Se $i_k \leq l$, então mx_l é um PBW-monômio, e a afirmação está trivialmente válida. Assumimos que $i_k > l$. Temos que

$$mx_l = x_{i_1} \dots x_{i_{k-1}} x_l x_{i_k} - x_{i_1} \dots x_{i_{k-1}} [x_l, x_{i_k}].$$

O produto $[x_l, x_{i_k}]$ pode ser escrito como $\sum_j \beta_j x_j$ com $x_j \in B$ e $\nu(x_j) \geq \nu(x_l) + \nu(x_{i_k})$. Logo

$$x_{i_1} \dots x_{i_{k-1}} [x_l, x_{i_k}] = \sum_j \beta_i x_{i_1} \dots x_{i_{k-1}} x_j.$$

Pela hipótese de indução, cada $x_{i_1}\cdots x_{i_{k-1}}x_j$ é uma combinação linear de PBW-monômios com comprimento menor ou igual que k e peso maior ou igual a $\nu(x_{i_1}\cdots x_{i_{k-1}})+\nu(x_j)\geq \nu(x_{i_1}\cdots x_{i_{k-1}})+\nu(x_{i_k})+\nu(x_l)=\nu(m)+\nu(x_l)$.

Usando de novo a hipótese de indução, obtemos que

$$x_{i_1}\ldots x_{i_{k-1}}x_l=\overline{x_{i_1}\ldots x_{i_{k-1}}x_l}+\sum\alpha_{m'}m'$$

onde cada m' é um PBW-monômio de comprimento menor que k e peso maior ou igual a $\nu(x_{i_1}\cdots x_{i_{k-1}})+\nu(x_l)$. Logo

$$x_{i_1}\ldots x_{i_{k-1}}x_lx_{i_k}=\overline{x_{i_1}\ldots x_{i_{k-1}}x_l}x_{i_k}+\sum\alpha_{m'}m'x_{i_k}.$$

Por hipótese, $\overline{x_{i_1}\ldots x_{i_{k-1}}x_l}x_{i_k}$ é um PBW-monômio e

$$\overline{x_{i_1}\ldots x_{i_{k-1}}x_l}x_{i_k}=\overline{x_{i_1}\ldots x_{i_{k-1}}x_lx_{i_k}}=\overline{x_{i_1}\ldots x_{i_{k-1}}x_{i_k}x_l}=\overline{mx_l}.$$

Logo cada $m'x_{i_k}$ é combinação linear de PBW-monômios de comprimento menor ou igual a k e peso maior ou igual a $\nu(m')+\nu(x_{i_k})\geq\nu(x_{i_1}\ldots x_{i_{k-1}})+\nu(x_l)+\nu(x_{i_k})=\nu(m)+\nu(x_l)$. □

Lema 5.1.6. *Seja $B=\{x_1,\ldots,x_\ell\}$ uma base homogênea da álgebra de Lie L e consideremos $m_1,m_2\in U$ dois PBW-monômios. Então $m_1m_2=\sum\alpha_m m$ onde cada m é um PBW-monômio e $\nu(m)\geq\nu(m_1)+\nu(m_2)$.*

Demonstração. Faremos essa demonstração usando o processo de indução sobre o comprimento de m_2.

Se $m_2=x_i\in L$, então o resultado segue do Lema 5.1.5. Assumamos que o lema é verdadeiro para todo PBW-monômio m_2 de comprimento menor ou igual a $k-1\geq 0$, isto é, o lema é válido para $x_{j_1}\ldots x_{j_{k-1}}$.

Seja $m_2=x_{j_1}\ldots x_{j_k}$. Então, $m_1m_2=m_1x_{j_1}\ldots x_{j_{k-1}}x_{j_k}$. Por hipótese de indução, $m_1x_{j_1}\ldots x_{j_{k-1}}=\sum\alpha_{\overline{m}}\overline{m}$ com $\nu(\overline{m})\geq\nu(m_1)+\nu(x_{j_1}\ldots x_{j_{k-1}})$. Definamos $\nu_0=\min\{\nu(\overline{m})\}$. Assim, pelo Lema 5.1.5, $m_1m_2=\sum\alpha_{\overline{m}}\overline{m}x_{j_k}=\sum\alpha_m m$ com

$$\nu(m)\geq\nu_0++\nu(x_{j_k})\geq\nu(m_1)+\nu(x_{j_1}\ldots x_{j_{k-1}})+\nu(x_{j_k})=\nu(m_1)+\nu(m_2).$$

□

Assim como definido na Seção 2.1 do Capítulo 2, temos a definição de $\omega(L)^n$ e, neste capítulo, denotaremos $\omega(L)^n$ por $\omega^n(L)$ para todo $n\geq 1$.

Lema 5.1.7. *Seja L uma álgebra de Lie e U sua envolvente universal. Considerando L^n como uma subálgebra de Lie de U, então $L^n \subseteq \omega^n(L)$ para todo $n \geq 1$.*

Demonstração. Quando $n = 1$ o resultado segue facilmente. Assumimos que $n > 1$ e $L^{n-1} \subseteq \omega^{n-1}(L)$. Tomemos $x \in L^n$, então $x = \sum \alpha_{ij}[x_i, x_j]$ com $x_i \in L$ e $x_j \in L^{n-1}$. Como U é uma álgebra de Lie com a operação colchete igual à operação comutador e $L^n \subseteq U$, temos que

$$x = \sum \alpha_{ij}[x_i, x_j] = \sum \alpha_{ij}(x_i x_j - x_j x_i).$$

Por hipótese de indução, $x_j \in \omega^{n-1}(L)$, então $x_i x_j, x_j x_i \in \omega^n(L)$ e, assim, $x \in \omega^n(L)$. Portanto, $L^n \subseteq \omega^n(L)$ para todo $n \geq 1$. □

Lema 5.1.8. *Seja $B = \{x_1, \ldots, x_\ell\}$ uma base homogênea da álgebra de Lie L. O ideal $\omega^n(L)$ de U é gerado pelos PBW-monômios $m \in U$ tais que $\nu(m) \geq n$ para todo $n \geq 1$.*

Demonstração. Seja $W_n := \text{span}\{m \in U : m \text{ é um PBW-monômio e } \nu(m) \geq n\}$. Queremos mostrar que $\omega^n(L) = W_n$.

Tomemos $m = x_{j_1} \ldots x_{j_k} \in W_n$, então m um PBW-monômio em U tal que $\nu(m) \geq n$. Temos que $x_{j_i} \in L^{\nu(x_{j_i})}$ para todo $i = 1, \ldots, k$, consequentemente, $x_{j_i} \in \omega^{\nu(x_{j_i})}(L)$ pelo Lema 5.1.7. Do fato que $\omega^i(L)\omega^j(L) = \omega^{i+j}(L)$ e $\nu(m) = \nu(x_{j_1}) + \cdots + \nu(x_{j_k})$, temos que

$$m \in \omega^{\nu(x_{j_1})}(L) \ldots \omega^{\nu(x_{j_k})}(L) = \omega^{\nu(x_{j_1})+\cdots+\nu(x_{j_k})}(L) = \omega^{\nu(m)}(L) \subseteq \omega^n(L)$$

e, assim, $W_n \subseteq \omega^n(L)$.

Mostraremos que $\omega^n(L) \subseteq W_n$ usando o processo de indução sobre n. Notemos que $\omega(L) \subseteq W_1$ e suponhamos que $\omega^{n-1}(L) \subseteq W_{n-1}$. Então, $\omega^n(L) = \omega^{n-1}(L)\omega(L) \subseteq W_{n-1}\omega(L)$ por hipótese de indução. Temos também que

$$W_{n-1}\omega(L) = \text{span}\{m_1 m_2 \in U : m_1, m_2 \text{ são PBW-monômios e } \nu(m_1) \geq n-1, \nu(m_2) \geq 1\}$$

e, pelo Lema 5.1.6,

$$\text{span}\{m_1 m_2 \in U : m_1, m_2 \text{ são PBW-monômios e } \nu(m_1) \geq n-1, \nu(m_2) \geq 1\} \subseteq W_n.$$

Assim, $\omega^n(L) \subseteq W_n$ e, portanto, $\omega^n(L) = W_n$. □

Lema 5.1.9. *Seja L uma $\mathbb{F}$-álgebra de Lie. Então $L \cap \omega^n(L) = L^n$, para todo $n \geq 1$.*

Demonstração. Já sabemos que $L^n \subseteq L$ e $L^n \subseteq \omega^n(L)$, logo $L^n \subseteq L \cap \omega^n(L)$.

Seja $B = \{x_1, \ldots, x_\ell\}$ uma base homogênea de L e tomemos $m \in L \cap \omega^n(L)$. Como $m \in L$, temos que $m = \sum \alpha_i x_i$ com $x_i \in B$. Por outro lado, $m \in \omega^n(L)$, então, pelo Lema 5.1.8, segue que $\nu(x_i) \geq n$, para todo $i = 1, \ldots, \ell$, o que implica que $x_i \in L^n$ para todo $i \in I$. Logo, $m \in L^n$ e, assim, $L \cap \omega^n(L) \subseteq L^n$. Portanto, $L \cap \omega^n(L) = L^n$. □

Lembremos que, $\omega(L)$ é residualmente nilpotente se $\bigcap_{n\geq 1} \omega^n(L) = \{0\}$ (Definição 2.1.1).

Teorema 5.1.10. *O ideal de aumento $\omega(L)$ é um ideal residualmente nilpotente de U se, e somente se, a $\mathbb{F}$-álgebra de Lie L de dimensão finita é nilpotente.*

Demonstração. Sabemos que $L^n \subseteq \omega^n(L)$, para todo $n \geq 1$. Assumindo que $\omega(L)$ é residualmente nilpotente, segue que

$$\bigcap_{n\geq 1} L^n \subseteq \bigcap_{n\geq 1} \omega^n(L) = \{0\},$$

logo L é residualmente nilpotente. Como L possui dimensão finita, segue que L é nilpotente.

Assumamos que L é nilpotente. Logo $\nu(x) < \infty$ para todo $x \in L$. Se m é um PBW-mônomio em U, então existe um índice finito t tal que $m = x_{j_1} \ldots x_{j_t}$ e, assim, $\nu(m) = \nu(x_{j_1}) + \cdots + \nu(x_{j_t}) < \infty$. Se existisse um $\overline{m} \in \bigcap_{n\geq 1} \omega^n(L)$ não nulo, então, pelo Lema 5.1.8, $\overline{m} = \sum \alpha_{m'} m'$ com $\nu(m') \geq n$ para todo $n \in \mathbb{N}$. Então, $\nu(m') = \infty$, o que não pode acontecer. Logo, $\bigcap_{n\geq 1} \omega^n(L) = \{0\}$ e, assim, $\omega(L)$ é um ideal residualmente nilpotente de U. □

Pelo Artigo [RU07], podemos observar que temos um resultado semelhante ao teorema acima para álgebras de Lie quaisquer, o qual diz que uma álgebra de Lie é residualmente nilpotente se, e somente se, o ideal de aumento de sua envolvente universal é residualmente nilpotente.

Exemplo 5.1.11.

1) Seja $L = \langle x, y \colon [x, y] = y \rangle$ a álgebra de Lie bidimensional não abeliana sobre o corpo $\mathbb{F}$. Já vimos que L não é nilpotente, portanto, pelo teorema acima, $\omega(L)$ não é residualmente nilpotente. De fato, como $L^n = \text{span}\{y\}$ para todo $n \geq 2$, temos que $\nu(y) = \infty$ e, assim, $y \in \bigcap_{n\geq 1} \omega^n(L)$.

2) Seja $L = \langle x, y, z \colon [x, y] = z \rangle$ a álgebra de Heisenberg. Pelo item 2 do Exemplo 1.4.3, temos que L é nilpotente. Então, pelo teorema acima, $\omega(L)$ é residualmente nilpotente.

5.2 Álgebras graduadas

Nesta seção, definiremos a álgebra graduada do ideal de aumento $\omega(L)$ da álgebra envolvente universal U da álgebra de Lie L, e mostraremos que existe um isomorfismo entre a álgebra

envolvente universal da álgebra graduada de L e a álgebra graduada de $\omega(L)$. Mostraremos também que se L e H são duas álgebras de Lie tais que suas envolventes universais são isomorfas, então $\mathrm{gr}(L)$ e $\mathrm{gr}(H)$ também são isomorfas.

Dada uma álgebra de Lie L e $\mathrm{gr}(L)$ sua álgebra graduada, já vimos na Seção 1.5 do Capítulo 1 que $\mathrm{gr}(L)$ é uma álgebra de Lie. Então, denotaremos a álgebra envolvente universal de $\mathrm{gr}(L)$ por U_{gr}.

Exemplo 5.2.1.

1) Se $L = \langle x, y \colon [x, y] = y \rangle$ a álgebra de Lie bidimensional não abeliana sobre o corpo $\mathbb{F}$, já vimos que a álgebra $\mathrm{gr}(L)$ é igual a L/L^2. Neste caso, se $\overline{x} = x + L^2$, então o conjunto $\{\overline{x}^e \colon e \in \mathbb{N}\}$ é uma base de U_{gr}.

2) Se $L = \langle x, y, z \colon [x, y] = z \rangle$ a álgebra de Heisenberg, já vimos que

$$\mathrm{gr}(L) = \mathrm{span}\{x + L^2, y + L^2\} \oplus \mathrm{span}\{z + L^3\}.$$

Neste caso, se $\overline{x} = x + L^2$, $\overline{y} = y + L^2$ e $\overline{z} = z + L^3$, então o conjunto $\{\overline{x}^{e_1}\overline{y}^{e_2}\overline{z}^{e_3} \colon e_1, e_2, e_3 \in \mathbb{N}\}$ é uma base de U_{gr}.

Seja U a álgebra envolvente universal da $\mathbb{F}$-álgebra de Lie L e $\mathrm{gr}(\omega(L))$ a álgebra graduada do ideal de aumento $\omega(L)$ definida na Seção 2.1 do Capítulo 2. Então, $\mathrm{gr}(\omega(L))$ é uma álgebra associativa, dada por

$$\mathrm{gr}(\omega(L)) = \mathbb{F} \oplus \left(\bigoplus_{i \geq 1} \frac{\omega^i(L)}{\omega^{i+1}(L)} \right),$$

e com o produto induzido por

$$(m_i + \omega^{i+1}(L))(m_j + \omega^{j+1}(L)) = m_i m_j + \omega^{i+j+1}(L)$$

com m_i, m_j PBW-monômios tais que $m_i \in \omega^i(L)$ e $m_j \in \omega^j(L)$.

Exemplo 5.2.2.

1) Seja $L = \langle x, y \colon [x, y] = y \rangle$ a álgebra de Lie bidimensional não abeliana sobre o corpo $\mathbb{F}$. Pelo item 3 do Exemplo 1.6.4, temos que $\{x^{e_1}y^{e_2} \colon e_1, e_2 \in \mathbb{N}\}$ é uma base da envolvente universal U de L. Pelo Lema 5.1.8, $\omega^n(L)/\omega^{n+1}(L)$ é gerado como espaço vetorial pelos PBW-monômios m em U tais que $\nu(m) = n$. Então, como $\nu(x) = 1$ e $\nu(y) = \infty$, temos que

$$\mathrm{gr}(\omega(L)) = \mathbb{F} \oplus \mathrm{span}\{x + \omega^2(L)\} \oplus \mathrm{span}\{x^2 + \omega^3(L)\} \oplus \cdots = \bigoplus_{n \geq 0} \mathrm{span}\{x^n + \omega^{n+1}(L)\}.$$

Neste caso, o conjunto $\{x^n + \omega^{n+1}(L) \colon n \in \mathbb{N}\}$ é uma base de $\mathrm{gr}(\omega(L))$.

2) Seja $L = \langle x, y, z \colon [x, y] = z \rangle$ a álgebra de Heisenberg. Pelo item 4 do Exemplo 1.6.4, temos que $\{x^{e_1} y^{e_2} z^{e_3} \colon e_1, e_2, e_3 \in \mathbb{N}\}$ é uma base da envolvente universal U de L. Como $\nu(x) = \nu(y) = 1$ e $\nu(z) = 2$, então, pelo Lema 5.1.8,1 temos que

$$\mathrm{gr}(\omega(L)) = \mathbb{F} \oplus \mathrm{span}\{x + \omega^2(L), y + \omega^2(L)\} \oplus \mathrm{span}\{x^2 + \omega^3(L), y^2 + \omega^3(L), z + \omega^3(L)\} \oplus \dots$$

Neste caso, o conjunto

$$\{x^{n_1} y^{n_2} z^{n_3} + \omega^{n_1+n_2+n_3+1}(L) \colon n_1, n_2, n_3 \in \mathbb{N}\}$$

é uma base de $\mathrm{gr}(\omega(L))$.

Podemos observar pelos Exemplos 5.2.1 e 5.2.2 que, quando L é a álgebra de Lie bidimensional não abeliana ou é a álgebra de Heisenberg, então U_{gr} e $\mathrm{gr}(\omega(L))$ são isomorfas. Mostraremos que este resultado é geral para toda álgebra de Lie de dimensão finita.

Proposição 5.2.3. *Sejam L uma $\mathbb{F}$-álgebra de Lie de dimensão finita e U sua envolvente universal. Se U_{gr} é a envolvente universal de $gr(L)$, então U_{gr} é isomorfa a $gr(\omega(L))$.*

Demonstração. A fim demonstrarmos essa proposição, iremos construir um isomorfismo ψ entre U_{gr} e $\mathrm{gr}(\omega(L))$.

Primeiro, como L tem dimensão finita, existe $n \in \mathbb{N}$ tal que $L^n = L^{n+1}$. Então, suponhamos que k seja tal que $L^k \supsetneq L^{k+1} = L^{k+2}$. Assim,

$$\mathrm{gr}(L) = \frac{L}{L^2} \oplus \cdots \oplus \frac{L^k}{L^{k+1}}.$$

Notemos também que, se $B = \{x_1, \dots, x_\ell\}$ é uma base homogênea de L, então $B_{gr} := \{x_{i_j} + L^{\nu(x_{i_j})+1} \colon x_{i_j} \in B \text{ e } \nu(x_{i_j}) < \infty\}$ é uma base de $\mathrm{gr}(L)$. Denotando $\overline{x}_{i_j} = x_{i_j} + L^{\nu(x_{i_j})+1}$ temos que se $m \in U_{gr}$ é um PBW-monômio, então $m = \overline{x}_{i_1} \dots \overline{x}_{i_t}$ com $1 \leq i_1 \leq \cdots \leq i_t \leq \ell$ e $\overline{x}_{i_j} \in B_{gr}$.

Pelo Lema 5.1.9 e como $\omega^{n+1}(L) \subseteq \omega^n(L)$, segue que

$$\frac{L^n}{L^{n+1}} = \frac{L \cap \omega^n(L)}{L \cap \omega^{n+1}(L)} = \frac{L \cap \omega^n(L)}{L \cap \omega^n(L) \cap \omega^{n+1}(L)}$$

e

$$\frac{L^n + \omega^{n+1}(L)}{\omega^{n+1}(L)} = \frac{(L \cap \omega^n(L)) + \omega^{n+1}(L)}{\omega^{n+1}(L)},$$

e pelo Segundo Teorema do Isomorfismo de Álgebras de Lie (Teorema 1.2.9), temos que L^n/L^{n+1} é isomorfa a $(L^n + \omega^{n+1}(L))/\omega^{n+1}(L)$ para todo $n = 1, \ldots, k$. Definamos, para cada n, o isomorfismo

$$\begin{array}{rccc} \phi_n\colon & \dfrac{L^n}{L^{n+1}} & \to & \dfrac{L^n + \omega^{n+1}(L)}{\omega^{n+1}(L)} \\ & x + L^{n+1} & \mapsto & x + \omega^{n+1}(L) \end{array}$$

e notemos que ϕ_n está bem definida, pois se $x+L^{n+1} = y+L^{n+1}$, então $x-y \in L^{n+1} \subseteq \omega^{n+1}(L)$. A fim de facilitar a notação, para cada $\overline{x}_{i_j} \in B_{gr}$, denotaremos $\phi_{\nu(x_{i_j})}(\overline{x}_{i_j}) = x_{i_j} + \omega^{\nu(x_{i_j})+1}(L)$ por $\widetilde{x}_{i_j}$.

Como $L^n + \omega^{n+1}(L) \subseteq \omega^n(L)$ para todo $n = 1, \ldots, n$, temos que $\phi_1, \ldots, \phi_k$ induzem o homomorfismo

$$\begin{array}{rccc} \phi\colon & \mathrm{gr}(L) & \to & \mathrm{gr}(\omega(L)) \\ & x = \sum \alpha_j \overline{x}_{i_j} & \mapsto & \sum \alpha_j \widetilde{x}_{i_j}. \end{array}$$

Tomemos $x + L^{\nu(x)+1}, y + L^{\nu(y)+1} \in \mathrm{gr}(L)$. Por um lado, temos que

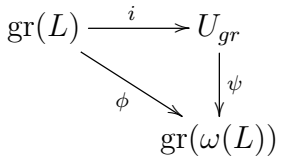
$$\phi([x + L^{\nu(x)+1}, y + L^{\nu(y)+1}]) = \phi([x, y] + L^{\nu(x)+\nu(y)+1}) = [x, y] + \omega^{\nu(x)+\nu(y)+1}(L)$$

e, por outro lado,

$$[\phi(x + L^{\nu(x)+1}), \phi(y + L^{\nu(y)+1})] = [x + \omega^{\nu(x)+1}(L), y + \omega^{\nu(y)+1}(L)] = [x, y] + \omega^{\nu(x)+\nu(y)+1}(L).$$

Logo, ϕ é um homomorfismo de álgebras de Lie.

Como $\mathrm{gr}(L)$ é uma álgebra de Lie, $\mathrm{gr}(\omega(L))$ é uma álgebra associativa e ϕ é um homomorfismo de álgebras de Lie, pela propriedade universal da álgebra envolvente temos que existe um único homomorfismo de álgebras associativas ψ tal que o diagarama



comuta, isto é, $\psi \circ i = \phi$. Mostraremos que ψ é um isomorfismo de álgebras associativas.

A fim de mostrarmos que ψ é sobrejetiva, por um lado, $L \subseteq \omega(L)$ e $\omega^2(L) \subseteq \omega(L)$, logo $L + \omega^2(L) \subseteq \omega(L)$. Por outro lado, pelo Lema 5.1.8, $\omega(L)$ é gerado por todos os PBW-monômios de peso maior e igual a 1. Assim, como todos PBW-monômios de peso 1 pertencem a L e todos PBW-monômios de peso maior ou igual a 2 pertencem a

$\omega^2(L)$, temos que $\omega(L) \subseteq L + \omega^2(L)$. Portanto, $L + \omega^2(L) = \omega(L)$. Assim, temos que

$$\psi(L/L^2) = \phi(L/L^2) = (L + \omega^2(L))/\omega^2(L) = \omega(L)/\omega^2(L)$$

e, como $\omega(L)/\omega^2(L)$ gera $\mathrm{gr}(\omega(L))$ como álgebra associativa, segue que ψ é sobrejetiva.

A fim de mostrarmos que ψ é injetiva, notemos que, por um lado, o conjunto dos PBW-monômios em U_{gr} é uma base de U_{gr}. Por outro lado, o conjunto dos monômios $x_{i_1} \dots x_{i_r} + \omega^{\nu(x_{i_1})+\dots+\nu(x_{i_r})+1}(L)$ tais que $x_{i_1} \dots x_{i_r} \in U$ são PBW-monômios, é uma base de $\mathrm{gr}(\omega(L))$. Assim, se $m = \overline{x}_{i_j} \dots \overline{x}_{i_t}$ um PBW-monômio em U_{gr}, então

$$\psi(m) = \phi(\overline{x}_{i_1}) \dots \phi(\overline{x}_{i_t}) = \widetilde{x}_{i_1} \dots \widetilde{x}_{i_t} = x_{i_1} \dots x_{i_t} + \omega^{\nu(x_{i_1})+\dots+\nu(x_{i_t})+1}(L)$$

e $\phi(m)$ é um elemento da base de $\mathrm{gr}(\omega(L))$. Tomemos $\overline{m} = \sum \alpha_{\overline{m}'}\overline{m}' \in \ker(\psi)$, então

$$0 = \psi(\overline{m}) = \sum \alpha_{\overline{m}'}\psi(\overline{m}') = \sum \alpha_{\overline{m}'}(m' + \omega^{\nu(m')+1}).$$

Assim, $\sum \alpha_{\overline{m}'}(m'+\omega^{\nu(m')+1}) = 0$ se, e somente se, $\alpha_{\overline{m}'} = 0$ para todo $\overline{m}'$. Portanto, $\ker(\psi) = \{0\}$ e ψ é injetiva. □

Pela proposição acima, $\mathrm{gr}(L)$ pode ser imerso na álgebra $\mathrm{gr}(\omega(L))$ e, assim, temos a identificação $L/L^2 = \omega(L)/\omega^2(L)$. Consequentemente, como a álgebra $\mathrm{gr}(L)$ é gerada como álgebra de Lie por L/L^2, segue que $\mathrm{gr}(L)$ é gerada como álgebra de Lie por $\omega(L)/\omega^2(L)$ e, dessa forma, segue que $\mathrm{gr}(L)$ é determinada pela álgebra envolvente universal U de L.

Teorema 5.2.4. *Sejam L e H duas $\mathbb{F}$-álgebras de Lie e U_L e U_H suas respectivas álgebras universais tais que U_L e U_H são isomorfas. Então, as álgebras $gr(L)$ e $gr(H)$ são isomorfas.*

5.3 Problema do isomorfismo

Nesta seção, iremos mostrar que se L e H são duas $\mathbb{F}$-álgebras de Lie tais que suas álgebras envolventes universais são isomorfas, então, se H é nilpotente, segue que L também é nilpotente. Além disso, mostraremos que quando H é nilpotente, o grau de nilpotência e o número mínimo de geradores de L e H são iguais.

Teorema 5.3.1. *Sejam L e H duas $\mathbb{F}$-álgebras de Lie e U_L e U_H suas respectivas álgebras envolventes universais tais que U_L e U_H são isomorfas. Seguem os seguintes resultados:*

(*i*) *Se H é nilpotente, então L também é nilpotente;*

(*ii*) *se H é nilpotente, então o grau de nilpotência de L e H são iguais;*

(*iii*) *se H é nilpotente, então o número mínimo de geradores de L e H são iguais.*

Demonstração. Temos que (*i*) segue do Teorema 5.1.10.

A fim de mostrarmos o item (*ii*), sejam L e H duas álgebras de Lie e U_L e U_H suas respectivas envolventes universais tais que U_L e U_H são isomorfas. Suponhamos que H é uma álgebra de Lie nilpotente com grau de nilpotência k, isto é, $H^k = \{0\}$ e $H^{k-1} \neq \{0\}$. Pelo item (*i*), temos que L também é nilpotente e queremos mostrar que seu grau de nilpotência também é k. Como $H^k = \{0\}$ e $H^{k-1} \neq \{0\}$, segue do Lema 1.5.5 que $\mathrm{gr}(H)^{k-1} = H^{k-1}$ e $\mathrm{gr}(H)^k = \{0\}$. Pelo Teorema 5.2.4, temos que U_H determina $\mathrm{gr}(H)$. Então, como U_L e U_H são isomorfas, temos que $\mathrm{gr}(L)$ e $\mathrm{gr}(H)$ também são isomorfas, portanto $\mathrm{gr}(L)^{k-1} \neq \{0\}$ e $\mathrm{gr}(L)^k = \{0\}$, isto é, $L^{k-1} \supsetneq L^k = L^{k+1}$. Como L é nilpotente, temos que $L^{k-1} \neq \{0\}$ e $L^k = \{0\}$. Portanto, o grau de nilpotência de L é k.

A fim de mostrarmos (*iii*), lembremos que o número mínimo de geradores de uma álgebra de Lie L nilpotente é a dimensão de L/L^2 (Teorema 1.4.8). Assim, como podemos fazer a identificação $L/L^2 = \omega(L)/\omega^2(L)$, temos que U determina a dimensão de L/L^2. Portanto, o número mínimo de geradores de L é determinado por U. □

Apesar de trabalharmos nessa dissertação apenas com álgebras de Lie de dimensão finita, temos que, pelo artigo [RU07], o teorema acima também é válido para álgebras de Lie quaisquer.

Referências Bibliográficas

[Ber78] George M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.

[Bir37] G. D. Birkhoff. Representability of Lie algebras and Lie groups by matrices. *Ann. of Math.*, 2(38):526–532, 1937.

[CKL04] Jang-Ho Chun, Takeshi Kajiwara, and Jong-Sook Lee. Isomorphism theorem on low dimensional Lie algebras. *Pacific J. Math.*, 214(1):17–21, 2004.

[Hum72] James E. Humphreys. *Introduction to Lie algebras and representation theory.* Springer-Verlag, New York-Berlin, 1972. Graduate Texts in Mathematics, Vol. 9.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Jac79] Nathan Jacobson. *Lie algebras*. Dover Publications, Inc., New York, 1979. Republication of the 1962 original.

[Jac89] Nathan Jacobson. *Basic algebra. II.* W. H. Freeman and Company, New York, second edition, 1989.

[Lam01] T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[Lew06] David W. Lewis. Quaternion algebras and the algebraic legacy of Hamilton's quaternions. *Irish Math. Soc. Bull.*, (57):41–64, 2006.

[Lor08] Falko Lorenz. *Algebra. Vol. II.* Universitext. Springer, New York, 2008. Fields with structure, Algebras and Advanced Topics, Translated from the German by Silvio Levy, with the collaboration of Levy.

[Mal92] P. Malcolmson. Enveloping algebras of simple three-dimensional Lie algebras. *J. Algebra*, 146(1):210–218, 1992.

[MMST11] F. E. B. Martínez, C. G. T. de A. Moreira, N. C. Saldanha, and E. Tengan. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.* IMPA, Rio de Janeiro, Brasil, 2011.

[Poi00] H. Poincaré. Sur les groupes continus. *Trans. Cambr. Philos. Soc.*, (18):220–255, 1900.

[RU07] David Riley and Hamid Usefi. The isomorphism problem for universal enveloping algebras of Lie algebras. *Algebr. Represent. Theory*, 10(6):517–532, 2007.

[Sha08] Zi Yang Sham. Quaternion Algebras and Quadratic Forms. Master's thesis, University of Waterloo, 2008.

[SU11] Csaba Schneider and Hamid Usefi. The isomorphism problem for universal enveloping algebras of nilpotent Lie algebras. *J. Algebra*, 337:126–140, 2011.

[TTT99] Tuong Ton-That and Thai-Duong Tran. Poincaré's proof of the so-called Birkhoff-Witt theorem. *Rev. Histoire Math.*, 5(2):249–284 (2000), 1999.

[Use10] Hamid Usefi. Isomorphism invariants of restricted enveloping algebras. *Pacific J. Math.*, 246(2):487–494, 2010.

[Wit37] E. Witt. Treue Darstellung Liescher Ringe. *J. Reine Angew. Math.*, (177):152–160, 1937.