Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sistemas de Identidades Polinomiais sem Base Finita

por
Marcos Mesquita Resende

Agosto 2009

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sistemas de Identidades Polinomiais sem Base Finita

por

Marcos Mesquita Resende

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

Mestre em Matemática

Brasília, 2009.

Comissão examinadora:

Prof. Dr. Alexei Krassilnikov - Orientador (MAT/UNB)

Prof. Dr. Plamen Koshlukov - Membro (IMECC/UNICAMP)

Prof. Dr. Dimas José Gonçalves - (MAT/UNB)

Agradecimentos

Ao meu orientador Alexei Krasilnikov pela preocupação em tirar as dúvidas, pela ajuda na escolha do tema e na construção do meu conhecimento.

Aos professores Rudolf Maier e Rui Seimetz, que durante a graduação me inspiraram de alguma forma a gostar de álgebra e teoria dos números.

Aos colegas de gradução, Humberto Carneiro e Leonardo Borges, por me fazerem gostar de matemática, sem eles eu dificilmente teria chegado aqui.

Aos amigos do mestrado, em especial Igor Lima, Felipe Silva, João Marcelo, João Vítor, Laura Cristina e Rafaela Prado pelo apoio nos momentos mais difíceis e por terem me ajudado nos problemas que teriam sido muito mais complicados resolver sozinho.

Finalmente agradeço aos meus pais, que sempre me incentivaram durante todo esse caminho.

"I like mathematics because it is not human and has nothing particular to do with this planet or with the whole accidental universe - because, like Spinoza's God, it won't love us in return..."
Bertrand Russel

Resumo

Seja $\mathbb{F}$ um corpo e seja A a $\mathbb{F}$-álgebra associativa livre (sem unidade) com geradores livres $x_1, x_2, ...$ Seja $f = f(x_1, ..., x_n) \in A$ e seja G uma álgebra associtativa sobre $\mathbb{F}$. Dizemos que $f = 0$ é uma *identidade polinomial* (ou apenas uma *identidade*) em G se $f(g_1, ..., g_n) = 0$ para todos $g_1, ..., g_n \in G$. Dois sistemas de identidades polinomiais $\{u_i = 0 \,|\, i \in I\}$ e $\{v_j = 0 \,|\, j \in J\}$ são *equivalentes* se toda $\mathbb{F}$-álgebra associativa satisfazendo todas as identidades $u_i = 0$ satisfaz todas as identidades $v_j = 0$ e vice-versa. Se o sistema de identidades polinomiais $\{u_i = 0 \,|\, i \in I\}$ é equivalente a algum sistema finito de identidades, dizemos que o sistema $\{u_i = 0 \,|\, i \in I\}$ tem *base finita*.

Nesta dissertação, faremos um estudo detalhado de dois sistemas de identidades polinomiais que não possuem base finita, ou seja, que não são equivalentes a um conjunto finito de identidades. O primeiro deles consiste num sistema de identidades polinomiais que não tem base finita em álgebras associativas (sobre um corpo de característica 2) sem unidade e com unidade, enquanto o segundo vale apenas para álgebras associativas (sobre um corpo de característica 2) sem unidade e contém a identidade $x^6 = 0$. Esta dissertação foi baseada nos artigos [7] e [8] de Gupta e Krasilnikov, e no capítulo 3 do livro *Free Algebras and PI-Algebras* do Drensky [4].

Palavras-chave: Identidades polinomais, variedades de álgebras, propriedade da base finita.

Abstract

Let $\mathbb{F}$ be a field and let A be the free associative $\mathbb{F}$-algebra (without 1) on free generators $x_1, x_2, ...$ Let $f = f(x_1, ..., x_n) \in A$ and let G be an associative algebra over $\mathbb{F}$. We say that $f = 0$ is a *polynomial identity* (or an *identity*) in G if $f(g_1, ..., g_n) = 0$ for all $g_1, ..., g_n \in G$. Two systems of polynomial identities $\{u_i = 0 \,|\, i \in I\}$ and $\{v_j = 0 \,|\, j \in J\}$ are *equivalent* if every associative $\mathbb{F}$-algebra satisfying all the identities $u_i = 0$ satisfies all the identities $v_j = 0$ and vice versa. If a system of polynomial identities $\{u_i = 0 \,|\, i \in I\}$ is equivalent to some finite system of identities, we say that the system $\{u_i = 0 \,|\, i \in I\}$ has a *finite basis* or is *finitely based*.

In this dissertation, we study in detail two systems of polynomial identites that are not finitely based, that is, they are not equivalent to a finite set of identities. The first one consists of a system of polynomial identities that has no finite basis in associative algebras (over a field of characteristic 2) with or without unity, whereas the second one works only in non-unitary associative algebras (over a field of characteristic 2) and contains the identity $x^6 = 0$. This dissertation was based on the articles [7] and [8] by Gupta and Krasilnikov, and the chapter 3 from the book *Free Algebras and PI-Algebras* by Drensky [4].

Keywords: Polynomial Identities, varieties of algebras, finite basis property.

Sumário

Introdução

Uma das razões de se introduzir a noção de variedades de grupos e álgebras é que as variedades dão uma classificação, ainda que simples, de todos os grupos e álgebras em termos da linguagem de identidades. Essa classificação é muito rudimentar no sentido que é possível, por exemplo, provar que a única variedade de álgebras comutativas unitárias sobre um corpo infinito é a variedade de todas as álgebras comutativas. Desse ponto de vista, álgebras comutativas são "triviais". Como nós queremos classificar todas as variedades, a primeira pergunta que surge é se podemos fazer isso em um número finito de termos.

Uma variedade tem base finita quando pode ser definida por um sistema finito de identidades. O *problema da base finita*, um dos problemas fundamentais no estudo de identidades polinomiais para um sistema de identidades em grupos ou álgebras, consiste em descobrir se o sistema é equivalente a algum sistema finito de identidades. Neste trabalho nós consideramos o problema para variedades de álgebras associativas, a questão é se todas elas podem ser definidas por um sistema finito de identidades polinomiais. Junto com um caso similar na teoria dos grupos, esse foi um dos principais problemas na teoria de variedades de grupos e álgebras por mais de 30 anos. Se $char\mathbb{F} = 0$ esse problema é conhecido como o *problema de Specht* que diz: todo sistema de identidades polinomiais em $\mathbb{F}$-álgebras associativas tem base finita? Se $\mathbb{F}$ é um corpo de característica 0, então a resposta é sim. Esse é um resultado celebrado obtido por Kemer em 1987 [9]. Por outro lado, se $\mathbb{F}$ é um corpo de característica $p > 0$, então a resposta é não. Isso foi provado por Belov [2], Grishin [5] (para $p = 2$) e Shchigolev [13] (vide também [3, 6, 14]). O problema foi inicialmente questionado para grupos por Neumann em sua tese em 1935 (vide [10] para referências) e por Specht [15] em 1950 para álgebras associativas sobre um corpo de característica 0.

Até hoje, está em aberto o problema para algumas classes de grupos e álgebras. Aqui nós daremos alguns exemplos de variedades de álgebras associativas sobre um corpo de característica 2 que não tem base finita de suas identidades polinomiais.

Seja $\mathbb{F}$ um corpo e seja A uma $\mathbb{F}$-álgebra associativa livre (sem unidade) com geradores livres $x_1, x_2, ...$ Seja $f = f(x_1, ..., x_n) \in A$ e seja G uma álgebra associtativa sobre $\mathbb{F}$. Dizemos que $f = 0$ é uma identidade polinomial (ou apenas uma identidade) em G se $f(g_1, ..., g_n) = 0$ para todos $g_1, ..., g_n \in G$. Dois sistemas de identidades polinomiais $\{u_i = 0 \,|\, i \in I\}$ e $\{v_j = 0 \,|\, j \in J\}$ são *equivalentes* se toda $\mathbb{F}$-álgebra associativa satisfazendo todas as identidades u_i satisfaz todas as identidades v_j e vice-versa. Se o sistema de identidades polinomiais $\{u_i = 0 \,|\, i \in I\}$ é equivalente a algum sistema finito de identidades, dizemos que o sistema $\{u_i = 0 \,|\, i \in I\}$ tem *base finita*.

O objetivo do presente trabalho é estudar sistemas de identidades polinomiais sem base finita de álgebras associativas sobre um corpo de característica 2. Seja $[x, y] = xy - yx$. O primeiro de nossos resultados principais é o seguinte teorema demonstrado por Gupta e Krasilnikov em [7].

Teorema 1 ([7]). *Para um corpo $\mathbb{F}$ qualquer de característica 2 o sistema de identidades polinomiais*

$$\{[x, y^2]x_1^2x_2^2 \cdots x_n^2[x, y^2]^3 \,|\, n = 0, 1, 2, ...\}$$

não é equivalente a nenhum sistema finito de identidades polinomiais em $\mathbb{F}$-álgebras associativas.

No final dos anos setenta e início dos anos oitenta, a seguinte conjectura foi muito conhecida entre os algebristas trabalhando no problema da base finita para anéis associativos.

Conjectura. *Existem sistemas de identidades polinomiais sem base finita em anéis associativos que contém uma identidade da forma $x^n = 0$. Em particular, existem tais sistemas que contém a identidade $x^8 = 0$.*

Em [5] Grishin provou que a primeira parte da conjectura era verdade: existe um sistema sem base finita que contém a identidade $x^{32} = 0$. Neste trabalho também vamos estudar uma demonstração para a segunda parte da conjectura (numa forma ainda mais forte) e ver que ela é verdade. Seja

$$u_n = [[y_1, z_1], t_1]x_1^2x_2^2 \cdots x_n^2[[y_2, z_2], t_2][[y_1, z_1], t_1][[y_2, z_2], t_2],$$

o segundo resultado principal do texto é o seguinte teorema demonstrado por Gupta e Krasilnikov em [8].

Teorema 2 ([8]). *Para um corpo $\mathbb{F}$ qualquer de característica 2 o sistema de identidades polinomiais*

$$\{x^6 = 0\} \cup \{u_n = 0 \,|\, n = 0, 1, ...\}$$

não é equivalente a nenhum sistema finito de identidades em $\mathbb{F}$-álgebras associativas.

Note que ambos os teoremas valem se $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, logo vale o corolário abaixo.

Corolário. *Os sistemas*

$$\{x^6 = 0\} \cup \{u_n = 0 \,|\, n = 0, 1, ...\}$$

e

$$\{[x, y^2]x_1^2x_2^2 \cdots x_n^2[x, y^2]^3 \,|\, n = 0, 1, 2, ...\}$$

de identidades polinomiais em anéis associativos não tem base finita.

Segue de um resultado de Popov [16] que sobre qualquer corpo $\mathbb{F}$, qualquer sistema de identidades polinomiais em $\mathbb{F}$-álgebras associativas contendo, para algum n, a identidade

$$[...[[x_1, x_2], x_3], ..., x_n][[x_{n+1}, x_{n+2}], x_{n+3}], ..., x_{2n}] = 0$$

tem base finita. O mesmo é verdade para qualquer sistema de identidades contendo, para algum n, a identidade

$$[x_1, x_2][x_3, x_4] \cdots [x_{2n-1}, x_{2n}] = 0$$

desde que o corpo $\mathbb{F}$ seja infinito [17]. Por outro lado, ao contrário das duas identidades acima, a identidade

$$x_1[[x_2, x_3], x_4]x_5[[x_6, x_7], x_8]x_9$$

pode ser incluída num sistema de identidades polinomiais sem base finita. Isso segue do seguinte corolário.

Corolário. *Para um corpo $\mathbb{F}$ qualquer de característica 2 o sistema que consiste da identidade*

$$x_1[[x_2, x_3], x_4]x_5[[x_6, x_7], x_8]x_9 = 0,$$

e das identidades

$$w_n = [x, y^2]x_1^2 \cdots x_n^2[x, y^2]^3 \;\; (n = 0, 1, 2, ...)$$

não é equivalente a nenhum sistema finito de identidades polinomiais em $\mathbb{F}$-álgebras associativas.

Podemos considerar o problema da base finita para álgebras unitárias (isto é, para álgebras com unidade 1) bem como para álgebras que não são necessariamente unitárias. Veremos que o Teorema 1 também vale para álgebras unitárias, esse fato será um corolário da demonstração. No entanto para o Teorema 2 já não podemos dizer o mesmo. De fato, em geral uma álgebra com unidade não satisfaz uma identidade da forma $x^n = 0$.

No primeiro capítulo daremos as definições necessárias para o entendimento do resto do texto, tanto para as demonstrações dos teoremas principais quanto para os resultados auxiliares, junto com elas algumas proposições e teoremas que são resultados relativamente bem conhecidos da álgebra geral.

No segundo capítulo faremos uma exposição detalhada da construção de uma álgebra que nos possibilitará provar os dois teoremas aqui enunciados. Finalmente no terceiro capítulo faremos a demonstração dos teoremas principais e enunciaremos (com demonstração) alguns corolários provenientes da demonstração do primeiro teorema.

Capítulo 1

Preliminares

Neste capítulo vamos expor as definições das principais estruturas algébricas usadas no decorrer da dissertação, além de resultados conhecidos sobre as mesmas. Falaremos sobre álgebras livres e identidades polinomiais, o que nos permitirá entender a teoria por trás dos teoremas principais. Alguns resultados aqui apresentados serão expostos sem demonstração, faremos apenas referência a livros em que o leitor poderá consultá-las se desejar.

1.1 Propriedades Básicas de Álgebras

Nesta seção, K será um corpo de característica qualquer, salvo menção contrária. Todos os espaços vetoriais e álgebras são sobre o corpo K.

Definição 1. Um espaço vetorial R é chamado uma álgebra linear (ou uma K-álgebra) se R é equipado com uma operação binária $*$ (isto é, uma aplicação $* : (R, R) \to R$), chamada *multiplicação*, tal que para todo $a, b, c \in R$ e qualquer $\alpha \in K$

$$(a + b) * c = a * c + b * c,$$
$$a * (b + c) = a * b + a * c,$$
$$\alpha(a * b) = (\alpha a) * b = a * (\alpha b).$$

Definição 2. O subespaço S de uma álgebra R é chamado de *subálgebra* se é fechado com respeito a multiplicação, isto é, s_1,$s_2 \in S$ implica que $s_1 * s_2 \in S$. A subálgebra I de R é chamada um ideal à esquerda de R se $RI \subseteq I$ (isto é, $r * i \in I$ para todo $r \in R$, $i \in I$). Similarmente definimos ideal à direita e ideal bilateral (ou simplesmente ideal, que significa um ideal à esquerda e à direita ao mesmo tempo e é denotado por $I \lhd R$).

Abaixo seguem exemplos de álgebras sobre um corpo K.

Exemplo 1. (i) L - uma extensão qualquer do corpo K com as operações usuais;
(ii) $K[x]$, $K[x_1, ..., x_m]$ - os polinômios em uma ou várias variáveis (comutativas);
(iii) $M_n(K)$ - o espaço vetorial de todas as matrizes $n \times n$ com entradas em K, e com multiplicação usual de matrizes.

Os teoremas usuais sobre homomorfismos de espaços vetoriais, grupos e anéis continuam valendo para álgebras.

Definição 3. Seja R uma álgebra sobre K.

(i) R é associativa se $(a * b) * c = a * (b * c)$ para todo $a, b, c \in R$;
(ii) R é comutativa se $a * b = b * a$, $a, b \in R$;
(iii) R é uma álgebra de Lie se para todo $a, b, c \in R$,

$$a * a = 0, \text{ anticomutatividade,}$$
$$(a * b) * c + (b * c) * a + (c * a) * b = 0, \text{ a identidade de Jacobi;}$$

(iv) R é unitária se R tem uma *unidade* e com a propriedade $e * r = r * e = r$, para todo $r \in R$.

Definição 4. Sejam V e W espaços vetoriais. Para construirmos o produto tensorial $V \otimes_K W$ de V e W primeiro consideramos o conjunto dos elementos do produto cartesiano $V \times W$. O espaço $F(V \times W)$ denotará o espaço vetorial que tem como base os elementos do conjunto $V \times W$. Seja R o subespaço de $F(V \times W)$ gerado por

$$(v_1 + v_2) \times w - (v_1 \times w + v_2 \times w);$$
$$v \times (w_1 + w_2) - (v \times w_1 + v \times w_2);$$
$$c(v \times w) - (cv) \times w;$$
$$c(v \times w) - v \times (cw).$$

Dessa forma o produto tensorial entre dois espaços V e W é o espaço quociente $F(V \times W)/R$. É imediato verificar que as seguintes igualdades valem em $V \otimes_K W$

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w;$$
$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2;$$

$$cv \otimes w = v \otimes cw = c(v \otimes w).$$

onde v, v_i, w, e w_i são vetores de V e W (respectivamente). Assim podemos dizer que

$$(\sum_{i \in I} \alpha_i v_i) \otimes (\sum_{j \in J} \beta_j w_j) = \sum_{i \in I} \sum_{j \in J} \alpha_i \beta_j (v_i \otimes w_j), \alpha_i, \beta_j \in K.$$

Se V e W são álgebras, então $V \otimes W$ também é uma álgebra com multiplicação definida a partir de

$$(v' \otimes w')(v'' \otimes w'') = (v'v'') \otimes (w'w''), v', v'' \in V, w', w'' \in W.$$

O produto tensorial é caracterizado por uma propriedade universal. Considere o problema de construir uma aplicação bilinear ψ do produto cartesiano $V \times W$ no espaço vetorial X. A construção do produto tensorial $V \otimes W$, junto com a aplicação bilinear natural $\varphi : V \times W \to V \otimes W$ dada por

$$\varphi(u, w) = u \otimes w,$$

é a solução universal desse problema no seguinte sentido. Para qualquer outro par (X, ψ), onde X é um espaço vetorial, e ψ uma aplicação bilinear $V \times W \to X$, existe uma única aplicação linear

$$T : V \otimes W \to X$$

tal que

$$\psi = T \circ \varphi.$$

Como qualquer propriedade universal, isso caracteriza o produto tensorial unicamente a menos de isomorfismo.

Daremos agora a definição de álgebra livre, cuja compreensão é essencial para entender as álgebras com identidade polinomiais.

Definição 5. Seja C uma classe de álgebras e seja $F \in C$ uma álgebra gerada pelo conjunto X. A álgebra F é chamada de *álgebra livre na classe C, livremente gerada pelo conjunto X*, se para qualquer álgebra $R \in C$, toda aplicação $X \to R$ pode ser extendida a um homomorfismo $F \to R$. A cardinalidade $|X|$ do conjunto X é chamada de *posto* de F.

Exemplo 2. Para qualquer conjunto X a álgebra de polinômios $K[X]$ é livre na classe de todas as K-álgebras associativas, comutativas e unitárias.

Exemplo 3. Para qualquer conjunto X a álgebra $K\langle X\rangle$ com base o conjunto de todas as palavras

$$x_{i_1}\cdots x_{i_n},\ x_{i_j}\in X,\ n=0,1,2,...,$$

e multiplicação definida por

$$(x_{i_1}\cdots x_{i_m})(x_{j_1}\cdots x_{j_n})=x_{i_1}\cdots x_{i_m}x_{j_1}\cdots x_{j_n},\ x_{i_k},x_{j_l}\in X,$$

é livre na classe de todas as álgebras unitárias associativas.

1.2 Álgebras com Identidades Polinomiais

Nesta seção, fixaremos $X=\{x_1,x_2,...\}$ como um conjunto infinito enumerável e K será um corpo de característica qualquer. Algumas vezes serão utilizados outros símbolos, (por exemplo $y,z,y_i,z_j,etc.$) para os elementos de X.

Definição 6. (i) Seja $f=f(x_1,...,x_n)\in K\langle X\rangle$ e seja R uma álgebra associativa. Dizemos que $f=0$ é uma *identidade polinomial* para R se

$$f(r_1,...,r_n)=0 \text{ para todo } r_1,...,r_n\in R.$$

Muitas vezes é dito apenas que f é uma identidade polinomial para R.

(ii) Se a álgebra associativa R satisfaz uma identidade polinomial $f=0$ não trivial (isto é, f é um elemento não nulo de $K\langle X\rangle$), chamamos R de uma PI-álgebra ("PI"= "Polynomial Identity", que significa identidade polinomial em português).

Exemplo 4. (i) A álgebra R é comutativa se e somente se satisfaz a identidade polinomial

$$[x_1,x_2]=x_1x_2-x_2x_1=0$$

.

(ii) Seja R uma álgebra associativa de dimensão finita, e seja $dimR<n$. Então R satisfaz a *identidade padrão (ou "standard") de grau n*

$$s_n(x_1,...,x_n)=\sum_{\sigma\in S_n}sgn(\sigma)x_{\sigma(1)}\cdots x_{\sigma(n)}=0,$$

onde S_n é o grupo simétrico de ordem n.

Algumas propriedades importantes de álgebras associativas são expressas na linguagem de identidades polinomiais. Nós vimos isso para a comutatividade no exemplo acima. Existem outros exemplos para álgebras sem unidade. A álgebra R é *nil de índice limitado* se existe um $n \in \mathbb{N}$ tal que $x^n = 0$ é uma identidade em R; a álgebra R é *nilpotente de classe* $\leq n$ se $x_1 \cdots x_n = 0$ em R.

Vamos falar agora sobre Variedades e Álgebras Relativamente Livres

Definição 7. Seja $\{f_i(x_1, ..., x_{n_i}) \in K\langle X\rangle | \, i \in I\}$ um conjunto de polinômios na álgebra associativa livre $K\langle X\rangle$. A classe C de todas as álgebras associativas satisfazendo as identidades polinomiais $f_i = 0$, $i \in I$, é chamada de *variedade* (de álgebras associativas) definida (ou determinada) pelo *sistema de identidades polinomiais* $\{f_i | \, i \in I\}$. A variedade B é chamada de *subvariedade* de C se $B \subset C$. O conjunto $T(C)$ de todas as identidades polinomiais satisfeitas pela variedade C é chamado de T-ideal ou o *ideal verbal* de C. Nós dizemos que o T-ideal $T(C)$ é gerado como um T-ideal pelo conjunto de identidades $\{f_i | \, i \in I\}$ da variedade C. Nós usamos a notação $T(C) = \langle f_i | \, i \in I\rangle^T$ e dizemos que o conjunto $\{f_i | \, i \in I\}$ é uma *base de identidades polinomiais* de C. Os elementos de $T(C)$ são chamados de *consequências* das identidades polinomiais da base. Se R é uma álgebra qualquer, denotamos por $T(R)$ o T-ideal das identidades polinomiais de R.

Exemplo 5. A classe de todas as álgebras comutativas é uma variedade definida pela identidade $[x_1, x_2] = 0$. A classe de todas as álgebras associativas é também uma variedade definida pelo conjunto vazio de identidades polinomiais.

Definição 8. Fixamos um conjunto Y. A álgebra $F_Y(C)$ na variedade C é chamada de *álgebra relativamente livre* de C livremente gerada por Y, se $F_Y(C)$ é livre na classe C.

Agora vamos ver que álgebras relativamente livres existem e que duas álgebras de mesmo posto são isomorfas.

Proposição 1. *Seja C a variedade definida por $\{f_i | \, i \in I\}$, seja Y um conjunto qualquer e seja J o ideal de $K\langle Y\rangle$ gerado por*

$$\{f_i(g_1, ..., g_{n_i}) \, | \, g_j \in K\langle Y\rangle, \, i \in I\}.$$

Então a álgebra $F = K\langle Y\rangle / J$ é uma álgebra relativamente livre em C com conjunto de geradores livres $\overline{Y} = \{y + J \, | \, y \in Y\}$. Quaisquer duas álgebras relativamente livres de mesmo posto em C são isomorfas.

Demonstração. Ver [4, p.23].

□

Para finalizar a seção, enunciamos o Teorema de Birkhoff que nos dá uma forma de encontrar variedades de álgebras sem necessariamente termos as identidades correspondentes.

Teorema 3 (Birkhoff)**.** *A classe de álgebras C é uma variedade se, e somente se, C é fechada sobre somas cartesianas, subálgebras e álgebras quocientes de álgebras em C.*

Demonstração. Ver [4, p.24].

□

1.3 A Propriedade da Base Finita

Definição 9. Uma variedade de álgebras associativas C tem base finita, se C pode ser definida por um sistema finito de identidades polinomiais (da álgebra associativa livre $K\langle X\rangle$, $X = \{x_1, x_2, ...\}$). Se C não pode ser definida por um sistema finito de identidades, então C tem *base infinita*. Se todas as *subvariedades* de C, incluindo a própria C, têm base finita, então C satisfaz a *propriedade de Specht*.

O problema de Specht consiste em decidir se toda variedade de álgebras associativas ou de Lie tem base finita (pode ser feita a mesma pergunta para grupos). As investigações no problema de Specht seguem duas direções:

(i) Mostrar que algumas variedades satisfazem a propriedade de Specht.

(ii) Construir contra-exemplos para o problema de Specht, isto é, exemplos de variedades que não tem base finita para suas identidades.

Nesse sentido, o primeiro resultado significativo na direção (i) foi devido a Oates e Powell [11] que estabeleceram que uma variedade gerada por um grupo finito tem a propriedade de Specht. Depois, o método foi extendido para o caso quando a variedade é gerada por um anel finito com algumas condições (por exemplo, anéis de Lie, anéis associativos, etc.).

Teorema 4 ([9], [1])**.** *Seja R um grupo finito ou uma álgebra (associativa ou de Lie) finita sobre um corpo finito. Então $varR$ (a variedade de álgebras/grupos correspondente a T(R)) tem a propriedade de Specht.*

Enunciamos aqui formalmente o Teorema de Kemer, que foi mencionado na introdução.

Teorema 5 (Kemer)**.** *Toda variedade de álgebras associativas sobre um corpo de característica* 0 *tem uma base finita.*

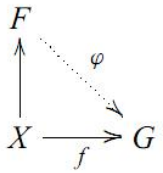
Uma identidade polinomial $g = 0$ é uma consequência das identidades $f_i = 0$, $i \in I$, se $g \in \langle f_i \,|\, i \in I\rangle^T$, o T-ideal gerado por f_i, $i \in I$.

Daremos agora a definição abaixo que é equivalente à outra definição para sistemas de identidades polinomiais equivalentes apresentada na introdução.

Definição 10. Dois conjuntos de identidades polinomiais são *equivalentes* se eles geram o mesmo T-ideal.

1.4 Apresentações de Grupos

Definição 11. Se X é um subconjunto de um grupo F, então F é um *grupo livre* com *base* X se, para cada grupo G e toda função $f : X \to G$, existe um único homomorfismo $\varphi : F \to G$ com $\varphi(x) = f(x)$ para todo $x \in X$.



Seja X um conjunto não vazio, e seja X^{-1} uma réplica disjunta de X; isto é, X e X^{-1} são disjuntos e existe uma bijeção $X \to X^{-1}$ a qual nós denotamos por $x \mapsto x^{-1}$. Defina o ***alfabeto*** em X como sendo

$$X \cup X^{-1}.$$

Se n é um inteiro positivo, definimos uma ***palavra*** em X de comprimento $n \geq 1$ como sendo uma função $w : \{1, 2, ..., n\} \to X \cup X^{-1}$. Na prática, escrevemos uma palavra w de comprimento n da seguinte forma: se $w(i) = x_i^{e_i}$, então

$$w = x_1^{e_1} \cdots x_n^{e_n},$$

onde $x_i \in X$ e $e_i = \pm 1$.

É possível provar que para cada conjunto X, existe um grupo livre que é livre na base X. Uma pergunta que surge naturalmente é se dois grupos livres com mesma base X são isomorfos.

Proposição 2. (*i*) *Seja* X_1 *a base de um grupo livre* F_1 *e* X_2 *a base de um grupo livre* F_2. *Se existe uma bijeção* $f : X_1 \to X_2$, *então existe um isomorfismo* $\phi : F_1 \to F_2$ *extendendo* f.
(*ii*) *Se* F *é um grupo livre com base* X, *então* F *é gerado por* X.

Demonstração. Ver [12, p.304].

□

Proposição 3. *Todo grupo* G *é quociente de um grupo livre.*

Demonstração. Seja X um conjunto tal que existe uma bijeção $f : X \to G$ (por exemplo, poderíamos tomar X como o conjunto subjacente ao grupo G e $f = 1_G$), e seja F o grupo livre com base X. Então existe um homomorfismo $\phi : F \to G$ extendendo f, e ϕ é sobrejetiva pois f o é. Então, $G \simeq F/ker\phi$.
□

Agora estamos em condição de dar a definição do que seria apresentação de um grupo.

Definição 12. Uma apresentação de um grupo G é um par ordenado

$$G = (X \,|\, R),$$

onde X é um conjunto, R é um conjunto de palavras em X, e $G = F/N$, onde F é o grupo livre com base X e N é o subgrupo normal gerado por R, ou seja, o subgrupo gerado por todos os conjugados dos elementos de R. Chamamos o conjunto X de ***geradores*** e o conjunto R de ***relações***.

Note que a proposição 2 diz que todo grupo tem uma apresentação.

Definição 13. Um grupo G é dito ***finitamente gerado*** se ele tem uma apresentação $(X \,|\, R)$ em que X é finito. Um grupo G é dito ***finitamente apresentável*** se tem uma apresentação $(X \,|\, R)$ em que tanto X como R são finitos.

Como observação, lembramos que existem grupos finitamente gerados que não tem apresentação finita. Daremos agora alguns exemplos de apresentações de grupos.

Exemplo 6. (*i*) Um grupo pode admitir várias apresentações. Por exemplo, $G = \mathbb{Z}_6$ tem apresentações

$$(x \,|\, x^6)$$

bem como

$$(a, b \mid a^3, b^2, aba^{-1}b^{-1}).$$

Um problema muito conhecido é o de determinar se duas apresentações determinam grupos isomorfos. Pode ser provado que não existe um algoritmo que resolve esse problema.

(*ii*) O grupo livre com base X tem apresentação

$$(X \mid \emptyset).$$

Um grupo livre é assim chamado precisamente porque tem uma apresentação com nenhuma relação.

Um estudo mais detalhado sobre grupos livres (construção e prova de existência) e apresentações poderá ser visto em [12, p. 297].

Capítulo 2

Resultados Auxiliares

Neste capítulo vamos construir uma álgebra R que satisfaz propriedades importantes que serão desejadas na demonstração dos teoremas principais. Aqui definiremos a álgebra e demonstraremos duas proposições referentes a ela. Observamos que durante todo o capítulo $\mathbb{F}$ será um corpo de característica 2.

2.1 A Álgebra R

Seja $(a,b) = a^{-1}b^{-1}ab$ e seja G um grupo dado pela apresentação

$$G = \langle a_i \, (i \in \mathbb{N}) \mid ((a_i, a_j), a_k), \, (a_i, a_j)^2, \, a_i^4 \, (i,j,k \in \mathbb{N}) \rangle$$

Lema 1. *Dados $g, h, l \in G$ temos :*

(i) $(g,h) \in Z(G)$, onde $Z(G)$ denota o centro do grupo G;

(ii) $(gh, l) = (g,l)(h,l)$;

(iii) $(g,h)^2 = 1$;

(iv) $g^4 = 1$.

Demonstração. Começamos lembrando as seguintes propriedades gerais para comutadores: $(ab, c) = (a,c)^b(b,c)$ e $(a, bc) = (a,c)(a,b)^c$, onde z^w é o elemento $w^{-1}zw$, para $z, w \in G$. Perceba que $(a_i, a_j) \in Z(G)$ e portanto $(a_i, a_j)^x \in Z(G)$ para $x \in G$. Podemos, em geral, escrever

$$(g,h) = (a_{i_1} \cdots a_{i_m}, a_{j_1} \cdots a_{j_n})$$

e usando as propriedades mencionadas, concluímos diretamente que todo elemento da forma (g,h) com $g,h \in G$ pode ser escrito como produto de comutadores de geradores da forma (a_i,a_j), e portanto pertence ao centro de G. Isso demonstra a afirmação (i) e a afirmação (ii) é imediata. Para a afirmação (iii) basta notar que como todo comutador (g,h) pode ser escrito como produto de comutadores de geradores, por exemplo $(g,h) = (a_{i_1},a_{i_2})\cdots(a_{i_{n-1}},a_{i_n})$, então

$$(g,h)^2 = (a_{i_1},a_{i_2})^2\cdots(a_{i_{n-1}},a_{i_n})^2 = 1.$$

Lembramos que por (ii) $(a_i^2,a_j) = (a_i,a_j)^2 = 1$ e portanto a_i^2 está no centro de G. Note que um elemento $g \in G$ pode ser escrito na forma $a_{i_1}\cdots a_{i_j}$, e que vale o seguinte $(a_{i_1}\cdots a_{i_j})^2 = a_{i_1}^2\cdots a_{i_j}^2 h$ onde h é um produto de comutadores. Como quadrados e comutadores de variáveis são centrais, segue pela própria definição do grupo G que$(a_{i_1}\cdots a_{i_j})^4 = 1$, assim temos o resultado (iv).

□

Seja G^2 o subgrupo de G gerado por todos os elementos g^2 $(g \in G)$. Como $(g^2,h) = (g,h)^2 = 1$ para todo $g,h \in G$, temos que G^2 é central em G.

Seja $\mathbb{F}G$ a álgebra do grupo G sobre o corpo $\mathbb{F}$. Seja $f_{ij} = (a_i,a_j) + a_i^2a_j^2 + a_i^2 + a_j^2 \in \mathbb{F}G$ e V o ideal em $\mathbb{F}G$ gerado pelos elementos f_{ij} $(i,j \in \mathbb{N})$. Defina $R = \mathbb{F}G/V$.

Seja M_n o conjunto das combinações $\mathbb{F}$-lineares de elementos do conjunto $\{r_1^2\cdots r_l^2 \mid l \leq n, r_i \in R\, para\, todo\, i\}$. Lembre-se que $[r,s] = rs - sr$. Para provar os teoremas precisaremos do seguinte

Proposição 4. *Para cada inteiro positivo n existem $s_1,...,s_{n+1} \in R$ tais que $s_1^2\cdots s_{n+1}^2 \notin M_n$.*

Proposição 5. *Para cada $r,s,t \in R$ temos $[r^2,t] = 0$ e $[[r,s],t] = 0$.*

2.2 Demonstração da Proposição 4

Lema 2. *Seja $f(g_1,g_2) = (g_1,g_2) + g_1^2g_2^2 + g_1^2 + g_2^2$ $(g_1,g_2 \in G)$. Para cada $g_1,g_2 \in G$ temos $f(g_1,g_2) \in V$.*

Demonstração. Todo elemento $g \in G$ pode ser escrito como $g = a_{i_1}\cdots a_{i_k}h$ onde $i_1 < \cdots < i_k$, $h \in G^2$. De fato, um elemento g qualquer pode ser escrito na forma $g = a_{j_1}\cdots a_{j_k}$ e com a simples observação de que $a_ia_j = a_ja_i(a_i,a_j)$ podemos trocar as ordens dos índices se necessário colocando um comutador na frente. Daí segue que g pode ser escrito como produto de geradores satisfazendo $i_1 < \cdots < i_l$ com possivelmente um produto de quadrados (caso alguma variável se repita) e comutadores de geradores à direita. Um

produto de comutadores pode ser escrito como um elemento de G^2, basta notar que para um grupo G qualquer o grupo quociente G/G^2 é um grupo de expoente 2 e portanto abeliano, logo $G' \leq G^2$. Para um elemento $g \in G$ como descrito acima, defina o seu *peso* por $wt(g) = k$. Perceba que se $wt(g_1) = 0$ ou $wt(g_2) = 0$, então $f(g_1, g_2) = 0$. Por exemplo, se $wt(g_1) = 0$, então $g_1 = h \in G^2$ e portanto

$$f(g_1, g_2) = (h, g_2) + h^2 g_2^2 + h^2 + g_2^2 = 1 + g_2^2 + 1 + g_2^2 = 0,$$

basta notar que h é de forma geral um produto de elementos de G^2 onde todos elementos comutam e assim sendo h^2 é um produto de elementos do tipo g^4 que como observamos anteriormente são iguais a 1.

Vamos provar o Lema 2 por indução em $wt(g_1) + wt(g_2)$. Se $wt(g_1) + wt(g_2) = 2$, então $wt(g_i) = 0$ (para $i = 1$ ou 2) e isso já implica que $f(g_1, g_2) = 0$, ou $wt(g_1) = wt(g_2) = 1$ e nesse caso $g_1 = a_{i_1} h'$ e $g_2 = a_{j_1} h''$ e lembrando que $h', h'' \in G^2$ e portanto comutam, é imediato verificar que $f(g_1, g_2) = f_{ij}$ para algum $i, j \in \mathbb{N}$, assim $f(g_1, g_2) \in V$.

Suponha que $f(h_1, h_2) \in V$ para todos $h_1, h_2 \in G$ tais que $wt(h_1) + wt(h_2) < n$. Sejam $g_1, g_2 \in G$, $wt(g_1) + wt(g_2) = n > 2$. Suponha que $wt(g_1) > 1$, perceba que g_1 pode ser escrito de tal forma que $g_1 = g_1' g_1''$, onde $wt(g_1) = wt(g_1') + wt(g_1'')$ e $wt(g_1')$, $wt(g_1'') > 0$. Como $wt(g_1) > 1$ temos que $wt(g_2) < n$, e já que

$$(g_1', g_2) + (g_1')^2 g_2^2 + (g_1')^2 + g_2^2 + V = V$$

pela hipótese de indução, o que implica

$$(g_1', g_2) + V = (g_1')^2 g_2^2 + (g_1')^2 + g_2^2 + V,$$

e equações similares valem para (g_1'', g_2) e (g_1', g_1'') temos

$$(g_1, g_2) + g_1^2 g_2^2 + g_1^2 + g_2^2 + V = (g_1' g_1'', g_2) + (g_1' g_1'')^2 g_2^2 + (g_1' g_1'')^2 + g_2^2 + V$$

$$= (g_1', g_2)(g_1'', g_2) + (g_1')^2 (g_1'')^2 g_2^2 (g_1', g_1'') + (g_1')^2 (g_1'')^2 (g_1', g_1'') + g_2^2 + V$$

$$= ((g_1')^2 (g_2)^2 + (g_1')^2 + g_2^2)((g_1'')^2 g_2^2 + (g_1'')^2 + g_2^2) + (g_1')^2 (g_1'')^2 (g_2^2 + 1)$$

$$\times((g_1')^2 (g_1'')^2 + (g_1')^2 + (g_1'')^2) + g_2^2 + V = f + V$$

Usando a distributividade, com cálculos diretos mostramos que $f = 0$. Portanto, se $wt(g_1) + wt(g_2) = n$ e $wt(g_1) > 1$, então $f(g_1, g_2) \in V$. Caso $wt(g_1) + wt(g_2) = n > 2$ e $wt(g_1) = 1$ então $wt(g_2) > 1$ e pelo argumento acima, $f(g_2, g_1) \in V$. Note agora que dados g, h quaisquer em G, temos que $(\ g, h)(g, h) = 1$ e $(g, h)(h, g) = 1$, logo $(g, h) = (h, g)$ e portanto $f(g_2, g_1) = f(g_1, g_2)$, o que conclui a demonstração.

□

Lema 3. *Para cada $g_1, g_2 \in G$ temos*

$$(g_1g_2)^2 + 1 + V = (g_1^2 + 1) + (g_2^2 + 1) + V.$$

Demonstração. Temos que

$$\begin{aligned}(g_1g_2)^2 + 1 + V &= g_1^2g_2^2(g_1, g_2) + 1 + V \\ &= g_1^2g_2^2(g_1, g_2) + g_1^2g_2^2(g_1^2g_2^2 + g_1^2 + g_2^2) + g_1^2g_2^2(g_1^2g_2^2 + g_1^2 + g_2^2) + 1 + V \\ &= g_1^2g_2^2((g_1, g_2) + g_1^2g_2^2 + g_1^2 + g_2^2) + g_1^2g_2^2(g_1^2g_2^2 + g_1^2 + g_2^2) + 1 + V = a.\end{aligned}$$

Pelo Lema 1

$$f = (g_1, g_2) + g_1^2g_2^2 + g_1^2 + g_2^2 \in V$$

e portanto

$$g_1^2g_2^2((g_1, g_2) + g_1^2g_2^2 + g_1^2 + g_2^2) \in V.$$

Logo,

$$\begin{aligned}a &= g_1^2g_2^2(g_1^2g_2^2 + g_1^2 + g_2^2) + 1 + V \\ &= 1 + g_2^2 + g_1^2 + 1 + V = (g_1^2 + 1) + (g_2^2 + 1) + V\end{aligned}$$

como queríamos. □

Lema 4. *Seja $h_i \in G\,(i = 1, ..., 2s)$ e seja $c = h_1 \cdots h_{2s}$. Se $c \in G^2$ então*

$$[h_1, h_2] \cdots [h_{2s-1}, h_{2s}] \in V.$$

Demonstração. Seja $u = [h_1, h_2] \cdots [h_{2s-1}, h_{2s}] + V$. Note que pelo Lema 2, $(1 + (h_i, h_j)) + V = (1 + h_i^2)(1 + h_j^2) + V$ e portanto

$$[h_i, h_j] + V = h_ih_j(1 + (h_i, h_j)) + V = h_ih_j(1 + h_i^2)(1 + h_j^2) + V.$$

A primeira igualdade se dá pelo fato do corpo $\mathbb{F}$ ser de característica 2. Note que $(1 + h_i^2)b = b + h_i^2b = b + bh_i^2 = b(1 + h_i^2)$, logo temos que $u = h_1 \cdots h_{2s}(1 + h_1^2) \cdots (1 + h_{2s}^2) + V$. Perceba que $h_{2s} = h_{2s-1}^{-1} \cdots h_1^{-1}c$ e que como $h^4 = 1$ nós temos que $h^2 = h^{-2}$. Pelo Lema 3, concluímos que

$$(1 + h_{2s}^2) + V = (1 + (h_{2s-1}^{-1} \cdots h_1^{-1}c)^2) + V = (1 + h_1^2) + \cdots + (1 + h_{2s-1}^2) + V.$$

Já que $(1+h_i^2)^2 = 1+h_i^4 = 0$ para todo i, temos que

$$u = h_1 \cdots h_{2s}(1+h_1^2)\cdots(1+h_{2s-1}^2)((1+h_1^2)+\cdots+(1+h_{2s-1}^2)) + V = V$$

como queríamos.

□

Lema 5. *A álgebra $R = \mathbb{F}G/V$ é soma direta de espaços vetoriais*

$$(a_{i_1}\cdots a_{i_q}\mathbb{F}G^2 + V)/V \quad (q \geq 0\,,\ i_1 < \cdots < i_q)$$

Demonstração. Começamos com a observação preliminar de que se U é um espaco vetorial dado por $U = U_1 \oplus \cdots \oplus U_k$ e V é um subespaço de U tal que $V = V_1 \oplus \cdots \oplus V_k$, onde V_i é subespaço de U_i, então $U/V \simeq U_1/V_1 \oplus \cdots \oplus U_k/V_k$. Note que $\mathbb{F}G$ é soma direta dos subespaços vetoriais $a_{i_1}\cdots a_{i_q}\mathbb{F}G^2$ $(q \geq 0,\ i_1 < \cdots < i_q)$. De fato, é imediato que a interseção entre quaisquer dois desses subespaços é nula, e para um elemento $f \in \mathbb{F}G$ temos que $f = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_k g_k$. Como foi visto no Lema 2, cada g_i pode ser escrito na forma $a_{i_1}\cdots a_{i_m}h$ onde $i_1 < \cdots < i_m$ e $h \in G^2$, logo $f \in \bigoplus_{q\geq 0, i_1<\cdots<i_q} a_{i_1}\cdots a_{i_q}\mathbb{F}G^2$. Assim sendo, para provar o Lema 5 basta provar que

$$V = \bigoplus_{q\geq 0, i_1<\cdots<i_q} V \cap a_{i_1}\cdots a_{i_q}\mathbb{F}G^2.$$

Seja V' o ideal de $\mathbb{F}G^2$ gerado por todos elementos $f_{ij} = (a_i, a_j) + a_i^2 a_j^2 + a_i^2 + a_j^2$ $(\ i, j = 1, 2, ...)$. Então

$$V = \mathbb{F}G \cdot V' = \bigoplus_{q\geq 0, i_1<\cdots<i_q} a_{i_1}\cdots a_{i_q}\mathbb{F}G^2 \cdot V' = \bigoplus_{q\geq 0, i_1<\cdots<i_q} a_{i_1}\cdots a_{i_q}V'. \quad (3)$$

Como $a_{i_1}\cdots a_{i_q}V' \subseteq V \cap a_{i_1}\cdots a_{i_q}\mathbb{F}G^2$, o resultado segue.

□

Note que na verdade, $a_{i_1}\cdots a_{i_q}V' = V \cap a_{i_1}\cdots a_{i_q}\mathbb{F}G^2$. De fato, se $v \in V \cap a_{i_1}\cdots a_{i_q}\mathbb{F}G^2$ então, por (3), $v = \sum v_{j_1\cdots j_l}$ com $v_{j_1\cdots j_l} \in a_{j_1}\cdots a_{j_l}V' \subseteq a_{j_1}\cdots a_{j_l}\mathbb{F}G^2$. Por outro lado, v é escrito como elemento da forma $a_{i_1}\cdots a_{i_q}h$ com $h \in \mathbb{F}G^2$, logo $v = v_{i_1\cdots i_q} \in a_{i_1}\cdots a_{i_q}V'$.

Lema 6. *Seja*

$$A = \{(a_{j_1}^2 + 1)\cdots(a_{j_m}^2 + 1)\,|\,m \geq 0,\ j_1 < \cdots < j_m\}.$$

Então o subconjunto $A + V$ da álgebra $\mathbb{F}G/V$ é linearmente independente sobre $\mathbb{F}$.

Demonstração. Como $A \subset \mathbb{F}G^2$, é suficiente provar que $A+V$ é linearmente independente em $(\mathbb{F}G^2+V)/V$. Lembramos que se A é uma álgebra, B uma subálgebra de A e $V \lhd A$ então $(B+V)/V \simeq B/(B \cap V)$, esse é o primeiro teorema do isomorfismo (para álgebras). Assim, é equivalente provar que $A+(\mathbb{F}G^2 \cap V)$ é linearmente independente em $\mathbb{F}G^2/(\mathbb{F}G^2 \cap V)$. Como $V' = V \cap \mathbb{F}G^2$, é suficiente provar que $A+V'$ é linearmente independente em $\mathbb{F}G^2/V'$. Seja $R = \mathbb{F}[t_i \,|\, i = 1,2,...]$ e sejam I e J os ideais de R gerados por $\{t_i \,|\, i = 1,2,...\}$ e $\{t_i^2 \,|\, i = 1,2,...\}$ respectivamente. É fácil verificar que o conjunto $\{(1+f)+J \,|\, f \in I\}$ é um subgrupo abeliano de expoente 2 do grupo $U(R/J)$ de todas as unidades da álgebra R/J. De fato basta notar que $(1+f)^2+J = 1+2f+f^2+J = 1+J$. Lembramos aqui que se temos uma função f que aplica elementos da base de um espaço vetorial E num espaço vetorial F, então f pode ser extendida a uma aplicação linear $T : E \to F$. Note agora que o grupo G^2 é um 2-grupo abeliano elementar (e portanto um espaço vetorial sobre $\mathbb{Z}_2$), logo qualquer aplicação de elementos da base de G^2 para um grupo pode ser extendida para uma aplicação linear de G^2 nesse grupo. Afirmamos que uma base para G^2 é

$$\{a_i^2 \,|\, i = 1,2,...\} \cup \{(a_i,a_j) \,|\, i,j = 1,2,...; i > j\}.$$

Basta notar que todos os elementos desse conjunto são linearmente independentes, centrais e um elemento qualquer de G^2 pode ser escrito como produto de quadrados de geradores e comutadores deles pelo mesmo motivo explicado no Lema 1. Assim sendo, a aplicação

$$\chi : (a_i,a_j) \mapsto t_it_j+1+J \,;\, a_i^2 \mapsto t_i+1+J$$

pode ser extendida a um homomorfismo de G^2 em $U(R/J)$ e pelo mesmo motivo podemos estender essa aplicação χ para um homomorfismo da álgebra do grupo G^2 sobre o corpo $\mathbb{F}$ para a álgebra do grupo $U(R/J)$ sobre o corpo $\mathbb{F}$. Denotaremos também por χ essa aplicação. Já que

$$\chi((a_i,a_j)+a_i^2a_j^2+a_i^2+a_j^2) = \chi((a_i,a_j))+\chi(a_i^2a_j^2)+\chi(a_i^2)+\chi(a_j^2)$$

$$= t_it_j+1+t_it_j+t_i+t_j+1+t_i+1+t_j+1 = 0$$

para todo i,j, nós temos que $\chi(V') = 0$. Portanto, o homomorfismo $\overline{\chi} : \mathbb{F}G^2/V' \to R/J$ que faz corresponder $\overline{\chi}(f+V') = \chi(f)$ para todo $f \in \mathbb{F}G^2$ é bem definido. É imediato verificar que $\chi((a_{j_1}^2+1)\cdots(a_{j_m}^2+1)) = t_{j_1}\cdots t_{j_m}+J$. Note que o conjunto

$$\overline{\chi}(A+V') = \{t_{j_1}\cdots t_{j_m}+J \,|\, m \geq 0, j_1 < \cdots < j_m\}$$

é claramente uma base para R/J, logo seus elementos são linearmente independentes em R/J e portanto $A+V'$ é linearmente independente em $\mathbb{F}G^2/V'$. Isso completa a demonstração do Lema 6.

□

Agora estamos em condição de completar a demonstração da Proposição 4. Seja L_n o conjunto das combinações $\mathbb{F}$-lineares de elementos do conjunto $\{r_1^2 \cdots r_l^2 \,|\, l \leq n, r_i \in \mathbb{F}G \,\forall\, i\}$ e assim $(L_n + V)/V = M_n$. Tome $s_i = a_i + V$ $(i = 1, ..., n+1)$. É suficiente provar que $a_1^2 \cdots a_{n+1}^2 \notin L_n + V$. Seja $r \in \mathbb{F}G$, $r = \sum_i \alpha_i g_i$ onde $\alpha_i \in \mathbb{F}$, $g_i \in G$ para todo i. Observamos que

$$(\sum_{i=1}^{n} x_i)^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j = \sum_{i=1}^{n} x_i^2 + \sum_{i>j}^{n}(x_i x_j + x_j x_i) = \sum_{i=1}^{n} x_i^2 + \sum_{i>j}^{n}[x_i, x_j].$$

Então nós temos que

$$r^2 = (\sum_i \alpha_i g_i)^2 = (\alpha + \sum_i \alpha_i (g_i + 1))^2 = \alpha^2 + \sum_i \alpha_i^2 (g_i^2 + 1) + \sum_{i<j} \alpha_i \alpha_j [g_i, g_j],$$

onde $\alpha = \sum_i \alpha_i$. Portanto, para cada $r_1, ..., r_l \in \mathbb{F}G$, o produto $r_1^2 \cdots r_l^2$ é uma combinação $\mathbb{F}$-linear de 1 e elementos da forma $(g_1^2 + 1) \cdots (g_k^2 + 1)$ $(k \leq l)$ e $(g_1^2 + 1) \cdots (g_p^2 + 1)[h_1, h_2] \cdots [h_{2q-1}, h_{2q}]$ $(q > 0, p + q \leq l)$, onde $g_i, h_i \in G$ para todo i, j. Segue que todo elemento de L_n é uma combinação de 1 e elementos das formas

$$(g_1^2 + 1) \cdots (g_l^2 + 1) \quad (0 < l \leq n) \quad (5)$$

e

$$(g_1^2 + 1) \cdots (g_p^2 + 1)[h_1, h_2] \cdots [h_{2q-1}, h_{2q}] \quad (q > 0, p + q \leq n). \quad (6)$$

Suponha por absurdo que $a_1^2 \cdots a_{n+1}^2 \in L_n + V$, então $(a_1^2 + 1) \cdots (a_{n+1}^2 + 1) \in L_n + V$, basta fazer as multiplicações e observar que aparecem somas de monômios que são produtos (com número de termos menor ou igual a n) de quadrados mais um monômio da forma $a_1^2 \cdots a_{n+1}^2$, e portanto

$$(a_1^2 + 1) \cdots (a_{n+1}^2 + 1) + V = \beta + \sum_i \beta_i^{(1)} f_i^{(1)} + \sum_j \beta_j^{(2)} f_j^{(2)} + V$$

onde $\beta, \beta_i^{(1)}, \beta_j^{(2)} \in \mathbb{F}$, em que $f_i^{(1)}$ e $f_j^{(2)}$ são da forma (5) e (6) respectivamente. Note que $(a_1^2+1)\cdots(a_{n+1}^2+1)$ e $\beta + \sum_i \beta_i^{(1)} f_i^{(1)}$ estão contidos em $\mathbb{F}G^2$ enquanto cada elemento

$$f_j^{(2)} = (g_{j1}^2+1)\cdots(g_{jp_j}^2+1)[h_1^{(j)}, h_2^{(j)}]\cdots[h_{2q_j-1}^{(j)}, h_{2q_j}^{(j)}]$$

da forma (6) está contido em $h_1^{(j)}\cdots h_{2q_j}^{(j)}\mathbb{F}G^2$. Portanto, pelo Lema 5, temos que, para todo j, $h_1^{(j)}\cdots h_{2q_j}^{(j)} \in G^2$. Então, pelo Lema 4, $[h_1^{(j)}, h_2^j]\cdots[h_{2q_j-1}^j, h_{2q_j}^{(j)}] \in V$ e portanto $f_j^{(2)} \in V$ para todo j. Daí segue que, $(a_1^2+1)\cdots(a_{n+1}^2+1)+V = \beta + \sum \beta_i f_i^{(1)} + V$, onde $\beta, \beta_i \in \mathbb{F}$ e $f_i^{(1)}$ é da forma (5) para todo i. Note que, pelo Lema 3, para cada $f_i^{(1)}$ da forma (5) o elemento $f_i^{(1)} + V$ é uma combinação linear de produtos $(a_{i_1}^2+1)\cdots(a_{i_l}^2+1)+V$ com o mesmo número l de fatores $(a_{i_k}^2+1)$ que em (5). Assim, o elemento $(a_1^2+1)\cdots(a_{n+1}^2+1)+V$ é uma combinação $\mathbb{F}$-linear de $1+V$ e elementos $(a_{i_1}^2+1)\cdots(a_{i_l}^2+1)+V$ com $l \leq n$. Isso contradiz o Lema 6 que diz que $(a_1^2+1)\cdots(a_{n+1}^2+1)+V$, $1+V$ e $(a_{i_1}^2+1)\cdots(a_{i_l}^2+1)+V$ $(0 < l \leq n;\ i_1 < \cdots < i_l)$ são linearmente independentes em $\mathbb{F}G/V$. A prova da Proposição 4 está completa.

2.3 Demonstração da Proposição 5

Perceba que $[r^2, t] = [[r, t], r]$ para todo $r, t \in \mathbb{F}G$. Portanto, é suficiente provar que $[[r_1, r_2], r_3] \in V$ para todo $r_i \in \mathbb{F}G$. Seja $r_l = \sum_{j_l} \alpha_{l_{j_l}} g_{l_{j_l}}$ para $l = 1, 2$ e 3 e $\alpha_{l_{j_l}} \in \mathbb{F}$, $g_{l_{j_l}} \in G$. Como

$$[[r_1, r_2], r_3] = \sum_{j_1}\sum_{j_2}\sum_{j_3} \alpha_{1_{j_1}}\alpha_{2_{j_2}}\alpha_{3_{j_3}}[[g_{1_{j_1}}, g_{2_{j_2}}], g_{3_{j_3}}],$$

para provarmos a Proposição 5 basta provar que $[[g_1, g_2], g_3] \in V$ para todo $g_1, g_2, g_3 \in G$.

Note que

$$\begin{aligned}[[g_1, g_2], g_3] &= g_1g_2g_3 + g_2g_1g_3 + g_3g_1g_2 + g_3g_2g_1 \\ &= g_1g_2g_3(1 + (g_2, g_1) + (g_3, g_1)(g_3, g_2) + (g_3, g_2)(g_3, g_1)(g_2, g_1)) \\ &= g_1g_2g_3(1 + (g_2, g_1))(1 + (g_3, g_1)(g_3, g_2)).\end{aligned}$$

Pelo Lema 2 temos que

$$1 + (g_2, g_1) + V = (1 + g_2^2)(1 + g_1^2) + V,$$

para todo $g_1, g_2 \in G$. Assim sendo, com cálculos diretos se verifica que

$$1 + (g_3, g_1)(g_3, g_2) + V = (1 + g_3^2)(1 + g_1^2) + (1 + g_3^2)(1 + g_2^2) + V.$$

Daí segue que

$$[[g_1, g_2], g_3] + V = g_1 g_2 g_3 (1 + g_2^2)(1 + g_1^2)((1 + g_3^2)(1 + g_1^2) + (1 + g_3^2)(1 + g_2^2)) + V.$$

Note que $(1 + g^2)^2 = 1 + g^4 = 0$, portanto temos que $[[g_1, g_2], g_3] + V = V$. Isso conclui a demonstração da Proposição 5.

Capítulo 3

Alguns Sistemas de Identidades Polinomiais sem Base Finita

Neste capítulo temos como objetivo demonstrar os teoremas principais desse trabalho, que dão exemplos de sistemas de identidades polinomiais de álgebras associativas sem base finita. As demonstrações aqui apresentadas tem como base os artigos [7] e [8] de Gupta e Krasilnikov.

3.1 Demonstração do Teorema 1 e Corolários

Nesta seção vamos provar o Teorema 1 e seus corolários usando as Proposições 4 e 5. Essas proposições foram demonstradas no capítulo 'Resultados Auxiliares'.

Demonstração do Teorema 1

Seja $\mathbb{F}$ um corpo arbitrário de característica 2 e seja

$$w_n = [x, y^2]x_1^2 \cdots x_n^2[x, y^2]^3 \ \ (n = 0, 1, 2, ...).(4)$$

De acordo com a Definição 10 (dada no capítulo de preliminares) o teorema vale se o sistema $\{w_n = 0 \mid n = 0, 1, ...\}$ não é equivalente a nenhum de seus subsistemas finitos. Vamos provar que isso acontece construindo, para cada inteiro positivo n, uma álgebra associativa B_n sobre o corpo $\mathbb{F}$ tal que B_n satisfaz as identidades $w_k = 0$ para todo $k < n$ mas não satisfaz a identidade $w_{n+1} = 0$.

Vamos construir tal álgebra utilizando a $\mathbb{F}$-álgebra R definida no capítulo de resultados auxiliares. Expomos novamente duas propriedades importantes da álgebra R. Lembramos que M_n é o conjunto das combinações $\mathbb{F}$-lineares

de elementos do conjunto $\{r_1^2 \cdots r_l^2 \mid l \leq n, r_i \in R \text{ para todo } i\}$. Pelas Proposições 4 e 5, temos:

(*i*)*Para cada inteiro positivo n existem* $s_1, ..., s_{n+1} \in R$ *tais que* $s_1^2 \cdots s_{n+1}^2 \notin M_n$.

(*ii*) *Para cada* $r, s, t \in R$ *temos* $[r^2, t] = 0$ *e* $[[r, s], t] = 0$.

Defina R_n como sendo o quociente da álgebra de matrizes

$$A = \begin{bmatrix} 0 & R & R & R & R \\ 0 & R & R & R & R \\ 0 & 0 & 0 & R & R \\ 0 & 0 & 0 & R & R \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 & a_{12} & a_{13} & a_{14} & a_{15} \\ 0 & a_{22} & a_{23} & a_{24} & a_{25} \\ 0 & 0 & 0 & a_{34} & a_{35} \\ 0 & 0 & 0 & a_{44} & a_{45} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \;\middle|\; a_{ij} \in R \right\}$$

sobre o ideal

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & M_n \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \;\middle|\; a \in M_n \right\}.$$

Ressaltamos aqui que B é de fato um ideal pois pela própria definição de M_n, este é um subespaço vetorial de R e se multiplicarmos qualquer elemento de B com algum de A é imediata a verificação de que este elemento é nulo, logo pertence a B. Assim sendo escrevemos:

$$R_n = \begin{bmatrix} 0 & R & R & R & R/M_n \\ 0 & R & R & R & R \\ 0 & 0 & 0 & R & R \\ 0 & 0 & 0 & R & R \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Seja

$$D = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e para cada $r \in R$, seja

$$\mathbf{r} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & r & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.1}$$

Defina B_n como sendo a subálgebra de R_n gerada por D e por todas as matrizes $\mathbf{r}$ ($r \in R$). Vamos verificar que a álgebra B_n satisfaz as identidades $w_k = 0$ para todo $k < n$ e, por outro lado, não satisfaz a identidade w_{n+1}.

Seja I o ideal de B_n gerado (como um ideal bilateral) por D. Todo elemento de I é da forma $\alpha\ D + \mathbf{v}'\ D + D\ \mathbf{u}' + \mathbf{v}''D\mathbf{u}'' + d$, onde $\alpha \in \mathbb{F}$, $\mathbf{u}', \mathbf{v}', \mathbf{u}'', \mathbf{v}''$ são da forma (3.1) para $u', v', u'', v'' \in R$ e $d \in I^2$. Com cálculos diretos podemos verificar que $\mathbf{v}''D\mathbf{u}'' = 0$. Como um fato geral de matrizes 5×5 podemos notar que qualquer elemento desse ideal I é da forma:

$$\begin{bmatrix} 0 & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

onde os * indicam uma entrada qualquer.

Disso concluímos com cálculos diretos que qualquer elemento $d \in I^2$ deve ser da forma

$$\begin{bmatrix} 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Fazendo os cálculos para $\mathbf{v}'\ D$ e $D\ \mathbf{u}'$ temos matrizes da forma

$$\mathbf{v}'\mathrm{D}=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & v' & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & v' \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{e} \quad \mathrm{D}\mathbf{u}' = \begin{bmatrix} 0 & u' & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & u' & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Isto implica pelas observações anteriores que todo elemento de I é da forma:

$$\begin{bmatrix} 0 & u & * & * & * \\ 0 & 0 & v & * & * \\ 0 & 0 & 0 & u & * \\ 0 & 0 & 0 & 0 & v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.2}$$

para $u, v \in R$ (as entradas denotadas por * não são importantes para a demonstração).

Considere agora a subálgebra $\mathbf{R}=\{\mathbf{r} \mid r \in R\}$. Pelas observações acima é imediata a verificação que $I \cap \mathbf{R} = 0$ e ainda mais, temos que $\mathbf{R}$ é uma álgebra isomorfa a R, basta considerar a aplicação de $\mathbf{R}$ em R que faz $\mathbf{r} \mapsto r$. Assim sendo, fica claro que B_n é uma extensão do ideal I pela subálgebra $\mathbf{R}$ que, por ser isomorfa a R, satisfaz a identidade $[x, y^2] = 0$. Portanto, para cada $b_1, b_2 \in B_n$, temos que $[b_1, b_2^2] \in I$, portanto $[b_1, b_2^2]$ é da forma (3.2).

Seja k um inteiro positivo. Seja $c_i \in B_n$ $(i = 1, 2, ..., k)$ dado por $c_i = \mathbf{r}_i + d_i$ (note que pela observação acima um elemento qualquer de B_n pode ser escrito dessa forma), onde $\mathbf{r}_i \in \mathbf{R}$ e $d_i \in I$ para todo i. Verificaremos que o elemento

$$[b_1, b_2^2]c_1^2c_2^2 \cdots c_k^2[b_1, b_2^2]^3$$

é da forma

$$\begin{bmatrix} 0 & 0 & 0 & 0 & f + M_n \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{3.3}$$

onde $f = r_1^2 \cdots r_k^2(uv)^2$. De fato, temos que $c_i^2 = (\mathbf{r}_i + d_i)^2 = \mathbf{r}_i^2 + \mathbf{r}_i d_i + d_i \mathbf{r}_i + d_i^2$ que é um elemento da forma

$$\begin{bmatrix} 0 & * & * & * & * \\ 0 & r_i^2 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & r_i^2 & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e portanto $c_1^2 \cdots c_k^2$ é igual a

$$\begin{bmatrix} 0 & * & * & * & * \\ 0 & r_1^2 \cdots r_k^2 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & r_1^2 \cdots r_k^2 & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Suponha então que $[b_1, b_2^2]$ seja escrito como

$$\begin{bmatrix} 0 & u & * & * & * \\ 0 & 0 & v & * & * \\ 0 & 0 & 0 & u & * \\ 0 & 0 & 0 & 0 & v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

fica então imediata a verificação de que $[b_1, b_2^2]^3$ é igual a

$$\begin{bmatrix} 0 & 0 & 0 & uvu & * \\ 0 & 0 & 0 & 0 & vuv \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Logo $[b_1, b_2^2]c_1^2c_2^2 \cdots c_k^2[b_1, b_2^2]^3$ é igual a

$$\begin{bmatrix} 0 & u & * & * & * \\ 0 & 0 & v & * & * \\ 0 & 0 & 0 & u & * \\ 0 & 0 & 0 & 0 & v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & * & * & * & * \\ 0 & r_1^2 \cdots r_k^2 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & r_1^2 \cdots r_k^2 & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & uvu & * \\ 0 & 0 & 0 & 0 & vuv \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & f+M_n \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

onde $f = ur_1^2 \cdots r_k^2 vuv$. Pela Proposição 5 os elementos da forma r^2 estão no centro de R e portanto $f = r_1^2 \cdots r_k^2 (uv)^2$. Se $k < n$, então $f \in M_n$ e portanto

$$[b_1, b_2^2] c_1^2 c_2^2 \cdots c_k^2 [b_1, b_2^2]^3 = 0$$

para todo $b_i, c_j \in B_n$. Logo, B_n satisfaz a identidade $w_k = 0$ para todo $k < n$.

Para provar que B_n não satisfaz a identidade $w_{n+1} = 0$ considere o elemento

$$d = [D, \mathbf{1}^2]\mathbf{s}_1^2 \cdots \mathbf{s}_{n+1}^2 [D, \mathbf{1}^2]^3,$$

onde $s_1, ..., s_{n+1} \in R$ são tais que $s_1^2 \cdots s_{n+1}^2 \notin M_n$ (tais termos existem pela Proposição 4) e $\mathbf{1}$, $\mathbf{s}_i$ são matrizes da forma 3.1 correspondentes a $1 \in R$ e $s_i \in R$ respectivamente. É fácil verificar que $[D, \mathbf{1}^2] = D$. De fato, $\mathbf{1}^2 = \mathbf{1}$ e

$$[D, \mathbf{1}] = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$- \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = D.$$

Então calculando da mesma forma que foi feito acima veremos que d é da forma 3.3 com $f = s_1^2 \cdots s_{n+1}^2$. Pela escolha dos elementos $s_1, ..., s_{n+1}$, nós temos $f \notin M_n$ e portanto $d \neq 0$. Assim, $w_{n+1} = 0$ não é satisfeita por B_n como requerido. Isso completa a prova do Teorema 1.

Seja, para cada $n = 0, 1, 2, ...,$

$$w_n^{(0)} = [x, y^2]^3 x_1^2 x_2^2 \cdots x_n^2 [x, y^2],$$

$$w_n^{(1)} = [[x,y],z]x_1^2x_2^2\cdots x_n^2[[x,y],z]^3,$$

$$w_n^{(2)} = [[y_1,z_1],t_1]x_1^2x_2^2\cdots x_n^2[[y_2,z_2],t_2][[y_1,z_1],t_1][y_2,z_2],t_2],$$

$$w_n^{(3)} = [x,y^2]x_1^2x_2^2\cdots x_n^2[z,t^2][x,y^2][z,t^2],$$

$$w_n^{(4)} = [x,y^2]x_1^2x_2^2\cdots x_n^2[x,y^2]^2x_{n+1}^2\cdots x_{2n}^2[x,y^2],$$

$$w_n^{(5)} = [[x,y],z]x_1^2x_2^2\cdots x_n^2[[x,y],z]^2x_{n+1}^2\cdots x_{2n}^2[[x,y],z],$$

$$w_n^{(6)} = [[y_1,z_1],t_1]x_1^2x_2^2\cdots x_n^2[[y_2,z_2],t_2][[y_1,z_1],t_1]x_{n+1}^2\cdots x_{2n}^2[[y_2,z_2],t_2].$$

Corolário 1. *Seja $\mathbb{F}$ um corpo de característica 2, então para cada $i = 0,1,...,6$ o sistema $\{w_n^{(i)} = 0 \,|\, n = 0,1,2,...\}$ de identidades polinomiais não tem base finita em $\mathbb{F}$-álgebras associativas.*

Demonstração. Observamos que pelo mesmo motivo que um comutador da forma $[x,y^2]$ é da forma (3.2), um comutador da forma $[[x,y],z]$ também o é (basta notar que pela Proposição 4 a álgebra R satisfaz a identidade $[[x_1,x_2],x_3] = 0$). Basta então calcular diretamente usando os cálculos acima para perceber que, para cada inteiro positivo n, a álgebra B_n satisfaz as identidades $w_k^{(i)} = 0$ ($i = 0,1,2,3; k < n$) e não satisfaz as identidades $w_{n+1}^{(i)} = 0$ $(i = 0,1,2,3)$. E da mesma forma é possível checar que B_{2n+1} satisfaz as identidades $w_k^{(i)} = 0$ ($i = 4,5,6; k \leq n$) e não satisfaz as identidades $w_{n+1}^{(i)} = 0$ $(i = 4,5,6)$.

□

Corolário 2. *Seja $\mathbb{F}$ um corpo de característica 2, então o sistema de identidades*

$$w_n = [x,y^2]x_1^2\cdots x_n^2[x,y^2]^3 \ \ (n = 0,1,2,...)$$

não é equivalente a nenhum sistema de identidades finito em $\mathbb{F}$-álgebras associativas com unidade.

Demonstração. Seja $B_n^{(1)}$ o fecho unitário (a menor álgebra contendo 1 e B_n) da álgebra B_n. É imediato que $B_n^{(1)}$ pode ser vista como $\mathbb{F}\oplus B_n$, ou seja, como soma direta de espaços vetoriais $\mathbb{F}$ e B_n sobre o corpo $\mathbb{F}$, onde os elementos de $\mathbb{F}$ agem em B_n por multiplicação escalar e o elemento 1 de $\mathbb{F}$ é a unidade

de $B_n^{(1)}$. Para provar o corolário basta provar que $B_n^{(1)}$ satisfaz as identidades $w_k = 0\,(k < n)$ e, por outro lado, não satisfaz a identidade $w_{n+1} = 0$.

Seja $\overline{b}$, $\overline{b'}$, $\overline{b_1}$, ..., $\overline{b_k}$ elementos arbitrários de $B_n^{(1)}$ e seja

$$d = [\overline{b}, (\overline{b'})^2]\overline{b_1}^2 \cdots \overline{b_k}^2[\overline{b}, (\overline{b'})^2]^3.$$

Então $\overline{b} = \alpha + b$, $\overline{b'} = \alpha' + b'$, $\overline{b_i} = \alpha_i + b_i$ onde α, α', $\alpha_i \in \mathbb{F}$, b, b', $b_i \in B_n$. Temos

$$d = [\alpha + b, (\alpha' + b')^2](\alpha_1 + b_1)^2 \cdots (\alpha_k + b_k)^2[\alpha + b, (\alpha' + b')^2]^3$$

$$= [b, (b')^2](\alpha_1^2 + b_1^2) \cdots (\alpha_k^2 + b_k^2)[b, (b')^2]^3.$$

Portanto, d é uma combinação linear (sobre o corpo $\mathbb{F}$) de elementos

$$[b, (b')^2]b_{i_1}^2 \cdots b_{i_l}^2[b, (b')^2]^3 \quad (l \leq k;\, i_1 < \cdots < i_l \leq k).$$

Como B_n satisfaz as identidades $w_l = 0$ $(l < n)$, nós temos que

$$[b, (b')^2]b_{i_1}^2 \cdots b_{i_l}^2[b, (b')^2]^3 = 0$$

para todo $l \leq k$ e portanto $d = 0$.

Assim sendo, $B_n^{(1)}$ satisfaz as identidades $w_k = 0$ $(k < n)$. Por outro lado, a álgebra $B_n^{(1)}$ não satisfaz a identidade $w_{n+1} = 0$ pois a álgebra B_n não a satisfaz. Isso completa a demonstração do corolário.

□

Corolário 3. *Para um corpo $\mathbb{F}$ qualquer de característica 2 o sistema que consiste da identidade*

$$x_1[[x_2, x_3], x_4]x_5[[x_6, x_7], x_8]x_9 = 0,$$

e das identidades

$$w_n = [x, y^2]x_1^2 \cdots x_n^2[x, y^2]^3 \ \ (n = 0, 1, 2, ...)$$

não é equivalente a nenhum sistema finito de identidades polinomiais em $\mathbb{F}$-álgebras associativas.

Demonstração. Sejam $d_1, ..., d_9$ elementos arbitrários de B_n. Lembre-se que a álgebra R satisfaz a identidade $[[x_1, x_2], x_3] = 0$, e portanto, para cada i, j, k nós temos $[[d_i, d_j], d_k] \in I$ o que implica que $[[d_i, d_j], d_k]$ é da forma (3.2). Já que

$$\begin{bmatrix} 0 & * & * & * & * \\ 0 & * & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & * & * & * & * \\ 0 & * & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\times \begin{bmatrix} 0 & * & * & * & * \\ 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & * & * & * & * \\ 0 & * & * & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = 0,$$

nós temos que $d_1[[d_2, d_3], d_4]d_5[[d_6, d_7], d_8]d_9 = 0$. O resultado segue.

□

3.2 Demonstração do Teorema 2

Nesta seção vamos provar o Teorema 2 usando as Proposições 4 e 5. Essas proposições foram demonstradas no capítulo 'Resultados Auxiliares'.

Demonstração do Teorema 2

Seja $\mathbb{F}$ um corpo arbitrário de característica 2 e seja

$$u_n = [[y_1, z_1], t_1]x_1^2x_2^2 \cdots x_n^2[[y_2, z_2], t_2][[y_1, z_1], t_1][[y_2, z_2], t_2]. \quad (5)$$

De acordo com a Definição 10 (dada na seção de preliminares) o teorema vale se o sistema $\{u_n = 0 \,|\, n = 0, 1, ...\} \cup \{x^6 = 0\}$ não é equivalente a nenhum de seus subsistemas finitos. Vamos provar que isso acontece construindo, para cada inteiro positivo n, uma álgebra associativa B_n sobre o corpo $\mathbb{F}$ tal que B_n satisfaz as identidades $u_k = 0$ e $x^6 = 0$ para todo $k < n$ mas não satisfaz a identidade $u_{n+1} = 0$.

Seja $\mathbb{F}[t_1, t_2, t_3, t_4]$ uma álgebra de polinômios sobre $\mathbb{F}$, $1 \in \mathbb{F}[t_1, t_2, t_3, t_4]$, e seja L o ideal de $\mathbb{F}[t_1, t_2, t_3, t_4]$ gerado por $\{t_i^3 \,|\, i = 1, 2, 3, 4\}$. Defina $\mathbb{K} = \mathbb{F}[t_1, t_2, t_3, t_4]/L$ e seja $\xi_i = t_i + L$ $(i = 1, 2, 3, 4)$. É imediato que $\mathbb{K}$ é uma $\mathbb{F}$-álgebra com $\mathbb{F}$-base $\{\xi_1^{m_1}\xi_2^{m_2}\xi_3^{m_3}\xi_4^{m_4} \,|\, 0 \leq m_i < 3\}$.

Seja δ o ideal de $\mathbb{K}$ gerado por ξ_i $(i = 1, 2, 3, 4)$. Perceba que se $\alpha \in \delta$ então α é combinação de elementos da forma $\xi_1^{m_1}\xi_2^{m_2}\xi_3^{m_3}\xi_4^{m_4}$ com m_i não

todos nulos, e lembrando que se $f, g \in \mathbb{K}$ então $(f+g)^4 = f^4 + g^4$, temos que $\alpha^4 = 0$.

Seja $\overline{R} = \mathbb{K} \otimes_{\mathbb{F}} R$. Como a identidade $[[x,y],z]$ é multilinear e, pela Proposição 4, a álgebra R satisfaz essa identidade, $\overline{R}$ satisfaz a identidade $[[x,y],z] = 0$ também. Como em uma álgebra sobre um corpo de característica 2 temos $[x,y^2] = [[x,y],y]$, a identidade $[x,y^2] = 0$ também é satisfeita em $\overline{R}$.

Defina J como o ideal de $\overline{R}$ gerado por todos os elementos da forma $\xi_i \otimes 1 \, (i = 1,2,3,4)$ e $1 \otimes (g+1+V)$ $(g \in G)$. Seja Δ o ideal de $\mathbb{F}G$ gerado por $(g+1), g \in G$. É imediato verificar que $V \subset \Delta$. Afirmamos que $J = \delta \otimes R + \mathbb{K} \otimes \Delta/V$. De fato, basta notar que o ideal gerado por um elemento $a \otimes b \in V \otimes W$ é da forma $< a > \otimes < b >$ onde $< a >$ representa o ideal gerado por a em V e $< b >$ o ideal gerado por b em W. Note agora que $R = \mathbb{F}(1+V) + \Delta/V$. Isso ocorre pois $\mathbb{F}G$ tem base

$$\{g \,|\, g \in G\}$$

$$= \{1\} \cup \{g \,|\, g \in G, g \neq 1\},$$

logo também é base

$$\{1\} \cup \{g+1 \,|\, g \in G, g \neq 1\}.$$

Portanto o conjunto gerador de $R = \mathbb{F}G/V$ é $\{1+V\} \cup \{g+1+V \,|\, g \in G\}$ e o resultado segue. Assim sendo, segue que

$$J = \delta \otimes (\mathbb{F}(1+V) + \Delta/V) + \mathbb{K} \otimes \Delta/V$$

$$= \delta \otimes \mathbb{F}(1+V) + \mathbb{K} \otimes \Delta/V$$

e daí verificamos que todo elemento de J pode ser escrito na forma $\alpha_0 \otimes 1 + \sum_{i \geq 1} \alpha_i \otimes h_i$, onde $\alpha_0 \in \delta$ e, para todo $i > 0$, $\alpha_i \in \mathbb{K}$ e $h_i = g_i + 1 + V$ para algum $g_i \in G$.

Seja $\overline{M_n} = \mathbb{K} \otimes_{\mathbb{F}} M_n$. É imediato verificar que $\overline{R}$ é um $\mathbb{K}$-módulo. Vamos provar que $\overline{M_n}$ é um $\mathbb{K}$-submódulo de $\overline{R}$ gerado pelo conjunto $\{r_1^2 \cdots r_k^2 \,|\, 0 \leq k \leq n, r_i \in \overline{R}\}$. De fato, é suficiente provar que para cada k, $0 \leq k \leq n$, e qualquer $r_i \in \overline{R}$ temos que $r_1^2 \cdots r_k^2 \in \overline{M_n}$. Seja $r \in \overline{R}$, $r = \sum_i \alpha_i \otimes h_i$, onde $\alpha_i \in \mathbb{K}, h_i \in R$. Então pela mesma observação feita na demonstração da Proposição 4 temos que

$$r^2 = \sum_i \alpha_i^2 \otimes h_i^2 + \sum_{i<j} \alpha_i \alpha_j \otimes [h_i, h_j],$$

e portanto $r_1^2 \cdots r_k^2$ é uma combinação $\mathbb{K}$-linear de elementos da forma $1 \otimes h_{i_1}^2 \cdots h_{i_k}^2$ e $1 \otimes h_{i_1}^2 \cdots h_{i_p}^2 [h_{j_1}, h_{j_2}] \cdots [h_{j_{2q-1}}, h_{j_{2q}}] (p+q=k)$. Note que $[h_i, h_j] \in$

$\mathbb{F}G^2$ pois $[h_i, h_j] = [h_i, h_j] + h_i^2 + h_j^2 + h_i^2 + h_j^2 = (h_i + h_j)^2 + h_i^2 + h_j^2$. Então $h_{i_1}^2 \cdots h_{i_k}^2 \in M_n$ e $h_{i_1}^2 \cdots h_{i_p}^2 [h_{j_1}, h_{j_2}] \cdots [h_{j_{2q-1}}, h_{j_{2q}}] \in M_n$ se $p + q = k$, nós temos $r_1^2 \cdots r_k^2 \in \overline{M_n}$ como queríamos.

Defina R_n como o quociente da álgebra de matrizes

$$\begin{bmatrix} 0 & \overline{R} & \overline{R} & \overline{R} & \overline{R} \\ 0 & \overline{R} & \overline{R} & \overline{R} & \overline{R} \\ 0 & 0 & 0 & \overline{R} & \overline{R} \\ 0 & 0 & 0 & \overline{R} & \overline{R} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

sobre o ideal

$$\begin{bmatrix} 0 & 0 & 0 & 0 & \overline{M_n} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

assim sendo

$$R_n = \begin{bmatrix} 0 & \overline{R} & \overline{R} & \overline{R} & \overline{R}/\overline{M_n} \\ 0 & \overline{R} & \overline{R} & \overline{R} & \overline{R} \\ 0 & 0 & 0 & \overline{R} & \overline{R} \\ 0 & 0 & 0 & \overline{R} & \overline{R} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Seja

$$D = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e para cada $r \in \overline{R}$, seja

$$\mathbf{r} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & r & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{3.4}$$

Defina B_n como a subálgebra de R_n gerada por D e por todas matrizes do tipo $\mathbf{r}$ ($r \in J$). Nós vamos verificar que a álgebra B_n satisfaz as identidades

$w_k = 0$ para todo $k < n$ e, por outro lado, não satisfaz a identidade $w_{n+1} = 0$. Depois iremos provar que, para cada n, a identidade $x^6 = 0$ é satisfeita em B_n. Seja I o ideal de B_n gerado (como um ideal bilateral) por D. Todo elemento de I é da forma

$$\alpha D + D\mathbf{u}_1 + \mathbf{v}_1 D + \mathbf{v}_2 D\mathbf{u}_2 + \beta D^2 + \mathbf{v}_3 D^2 + D^2\mathbf{u}_3 + D\mathbf{w}_3 D$$

$$+\mathbf{v}_4 D\mathbf{w}_4 D + D\mathbf{w}_5 D\mathbf{u}_5 + \mathbf{v}_6 D^2\mathbf{u}_6 + \mathbf{v}_7 D\mathbf{w}_7 D\mathbf{u}_7 + d,$$

onde $d \in I^3, \alpha, \beta \in \mathbb{K}, \mathbf{u}_i, \mathbf{v}_j, \mathbf{w}_k$ são da forma 3.4 com $u_i, v_j, w_k \in J$. Como feito na demonstração do Teorema 1, é imediato checar que para todo $\mathbf{r}_1, \mathbf{r}_2$ da forma 3.4 nós temos que $\mathbf{r}_1 D \mathbf{r}_2 = 0$. Portanto

$$\mathbf{v}_2 D\mathbf{u}_2 = \mathbf{v}_4 D\mathbf{w}_4 D = D\mathbf{w}_5 D\mathbf{u}_5 = \mathbf{v}_7 D\mathbf{w}_7 D\mathbf{u}_7 = 0.$$

Observe que

$$D^2\mathbf{r} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & r & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & r & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e portanto com cálculos inteiramente análogos concluímos que os elementos $\mathbf{v}_3 D^2, D^2\mathbf{u}_3, \mathbf{v}_6 D^2\mathbf{u}_6$ e d são da forma

$$\begin{bmatrix} 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note agora que

$$D\mathbf{w}D = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & w & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & w & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & w & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & w \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e portanto segue que todo elemento de I é da forma

$$\begin{bmatrix} 0 & u & w & * & * \\ 0 & 0 & v & * & * \\ 0 & 0 & 0 & u & w \\ 0 & 0 & 0 & 0 & v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{3.5}$$

para alguns $u, v, w \in \overline{R}$ (as entradas denotadas por $*$ não são importantes para a demonstração).

É imediato que B_n é uma soma do ideal I e da subálgebra $\mathbf{J} = \{\mathbf{r} \,|\, r \in J\}$ e $I \cap \mathbf{J} = 0$. A álgebra $\mathbf{J}$ é isomorfa à álgebra J, basta considerar o isomorfismo natural $\mathbf{r} \mapsto r$ e a verificação é imediata. Assim $\mathbf{J}$ satisfaz a identidade $[[x, y], z] = 0$.

Seja k um inteiro positivo e seja $b_i^{(l)}, c_j \in B_n (i = 1, 2, 3; l = 1, 2; j = 1, 2, ..., k)$. Pela observação acima $[[b_1^{(l)}, b_2^{(l)}], b_3^{(l)}] \in I$, então $[[b_1^{(l)}, b_2^{(l)}], b_3^{(l)}]$ é da forma (3.5) para $l = 1, 2$. Seja

$$[[b_1^{(l)}, b_2^{(l)}], b_3^{(l)}] = \begin{bmatrix} 0 & u^{(l)} & * & * & * \\ 0 & 0 & v^{(l)} & * & * \\ 0 & 0 & 0 & u^{(l)} & * \\ 0 & 0 & 0 & 0 & v^{(l)} \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

e seja $c_j = \mathbf{r}_j + d_j$, onde $r_j \in J$ e $d_j \in I$ para todo j. Então com cálculos da mesma forma que foram feitos na demonstração do Teorema 1 é imediato verificar que o elemento

$$d = [[b_1^{(1)}, b_2^{(1)}], b_3^{(1)}] c_1^2 c_2^2 \cdots c_k^2 [[b_1^{(2)}, b_2^{(2)}], b_2^{(2)}][[b_1^{(1)}, b_2^{(1)}], b_3^{(1)}][[b_1^{(2)}, b_2^{(2)}], b_2^{(2)}]$$

é da forma

$$\begin{bmatrix} 0 & 0 & 0 & 0 & f + \overline{M_n} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{3.6}$$

com $f = u^{(1)}r_1^2 \cdots r_k^2 v^{(2)} u^{(1)} v^{(2)}$. Como os quadrados são centrais na álgebra $\overline{R}$ (Proposição 5), $f = r_1^2 \cdots r_k^2 (u^{(1)}v^{(2)})^2$. Se $k < n$ nós temos que $f \in \overline{M_n}$ então $d = 0$ para todo $b_i^{(l)}, c_j \in B_n$. Logo, B_n satifaz todas as identidades $w_k = 0\,(k < n)$.

Para provar que B_n não satisfaz a identidade $w_{n+1} = 0$ considere o elemento

$$d' = [[D, \widetilde{\xi_1}], \widetilde{\xi_2}]\mathbf{s}_1^2 \cdots \mathbf{s}_{n+1}^2 [[D, \widetilde{\xi_3}], \widetilde{\xi_4}][[D, \widetilde{\xi_1}], \widetilde{\xi_2}][[D, \widetilde{\xi_3}], \widetilde{\xi_4}],$$

onde $\widetilde{\xi_i} = \xi_i \otimes \mathbf{1}$, $s_i = 1 \otimes (1 + a_i + V)$ (lembre-se que $\{a_i \mid i \in \mathbb{N}\}$ é um conjunto de geradores livres para G) e $\mathbf{s}_i$ é uma matriz da forma (3.4) correspondente a s_i. Esse cálculo se faz da mesma forma que o anterior para calcular 3.5 e então é direto verificar que d' é da forma 3.6 com

$$f = \xi_1^2 \xi_2^2 \xi_3^2 \xi_4^2 \otimes ((1 + a_1^2) \cdots (1 + a_{n+1}^2) + V).$$

Pela Proposição 4, $(1 + a_1^2) \cdots (1 + a_{n+1}^2) \notin M_n$, então $f \notin \overline{M_n} = \mathbb{K} \otimes_{\mathbb{F}} M_n$ e $d' \neq 0$. Assim, B_n não satisfaz a identidade $w_{n+1} = 0$, como queríamos demonstrar.

Falta agora provar que, para cada $n > 0$, a álgebra B_n satisfaz a identidade $x^6 = 0$. Nós precisaremos do seguinte lema.

Lema 7. *A álgebra J satisfaz a identidade $x^4 = 0$.*

Demonstração. Seja f um elemento arbitrário de $\overline{R}$, $f = \sum_{i \geq 0} \alpha_i \otimes h_i$, onde $\alpha_i \in \mathbb{K}, h_i \in R$. Então, como já foi explicado,

$$f^2 = \sum_{i \geq 0} \alpha_i^2 \otimes h_i^2 + \sum_{0 \leq i < j} \alpha_i \alpha_j \otimes [h_i, h_j].$$

Como R satisfaz as identidades $[[x, y], z] = 0$ e $[x, y^2] = 0$, segue que os elementos $\alpha_i^2 \otimes h_i^2$ e $\alpha_i \alpha_j \otimes [h_i, h_j]$ são centrais em $\overline{R}$ para todo i, j. Portanto

$$f^4 = \sum_{i \geq 0} \alpha_i^4 \otimes h_i^4 + \sum_{0 \leq i < j} \alpha_i^2 \alpha_j^2 \otimes [h_i, h_j]^2.$$

Note que sobre um corpo de característica 2 nós temos que

$$[[x, xy], y] + x[[x, y], y] = [x^2 y + xyx, y] + x[xy + yx, y]$$
$$= x^2 y^2 + yx^2 y + xyxy + yxyx + x^2 y^2 + xyxy + xyxy + xy^2 x$$
$$= yx^2 y + xyxy + yxyx + xy^2 x = (xy)^2 + xyyx + yxxy + (yx)^2 = [x, y]^2.$$

Como R satisfaz a identidade $[[x, y], z] = 0$, segue que R satisfaz a identidade $[x, y]^2 = 0$ também. Portanto, $[h_i, h_j]^2 = 0$ para todo i, j e $f^4 = \sum_{i \geq 0} \alpha_i^4 \otimes h_i^4$.

Agora suponha que $f \in J$. Então, como visto anteriormente $f = \alpha_0 \otimes 1 + \sum_{i\geq 1} \alpha_i \otimes h_i$ onde $\alpha_0 \in \delta$ e, para todo $i > 0$, $\alpha_i \in \mathbb{K}$ e $h_i = g_i + 1 + V$ para algum $g_i \in G$. Por outro lado vimos que para $f \in \overline{R}$, $f^4 = \sum_{i\geq 0} \alpha_i^4 \otimes h_i^4$. Então se $f \in J$ podemos assumir nessa última equação que, por exemplo, $\alpha_0 \in \delta, h_0 =, h_i = (g_i + 1) + V (i > 0)$, onde $g_i \in G$ para todo i. Segue que

$$f^4 = \alpha_0^4 \otimes 1 + \sum_{i\geq 1} \alpha_i^4 \otimes h_i^4.$$

Como $\alpha_0 \in \delta$, temos que $\alpha_0^4 = 0$. Por outro lado já checamos anteriormente (conferir seção de preliminares) que $g^4 = 1$ para todo $g \in G$, então

$$h_i^4 = (g_i + 1)^4 + V = (g_i^4 + 1) + V = 0 + V$$

para todo $i \geq 1$.

Daí $f^4 = 0$ para todo $f \in J$. E o lema está demonstrado.

□

Seja x um elemento arbitrário de B_n. Então $x = \mathbf{r} + x'$, onde $\mathbf{r}$ é da forma 3.4 com $r \in J$ e $x' \in I$. Como x' é da forma 3.5 temos que

$$x = \begin{bmatrix} 0 & u & w & * & * \\ 0 & r & v & * & * \\ 0 & 0 & 0 & u & w \\ 0 & 0 & 0 & r & v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

com $r \in J, u, v, w \in \overline{R}$. Lembre-se que $[t, s^2] = [t, s, s] = 0$, e isso junto com o Lema 7 nos dá que

$$r^4 = 0 \qquad \text{e} \qquad s^2 t = t s^2$$

para todo $r \in J$ e $s, t \in \overline{R}$. Vamos calcular diretamente x^6, para isso substituímos as entradas $*$ do elemento x para a, b, c e d de forma que

$$x = \begin{bmatrix} 0 & u & w & a & b \\ 0 & r & v & c & d \\ 0 & 0 & 0 & u & w \\ 0 & 0 & 0 & r & v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

logo

$$x^2 = \begin{bmatrix} 0 & ur & uv & uc+wu+ar & ud+w^2+av \\ 0 & r^2 & rv & rc+vu+cr & rd+vw+cv \\ 0 & 0 & 0 & ur & uv \\ 0 & 0 & 0 & r^2 & rv \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Sejam

$$\begin{aligned} \delta_1 &= uc+wu+ar, \\ \delta_2 &= ud+w^2+av, \\ \delta_3 &= rc+vu+cr, \\ \delta_4 &= rd+vw+cv, \end{aligned}$$

então

$$x^2 = \begin{bmatrix} 0 & ur & uv & \delta_1 & \delta_2 \\ 0 & r^2 & rv & \delta_3 & \delta_4 \\ 0 & 0 & 0 & ur & uv \\ 0 & 0 & 0 & r^2 & rv \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Portanto da mesma forma que calculamos x^2 obtemos de imediato que

$$x^4 = \begin{bmatrix} 0 & ur^3 & ur^2v & ur\delta_3+uvur+\delta_1r^2 & ur\delta_4+(uv)^2+\delta_1rv \\ 0 & 0 & r^3v & r^2\delta_3+rvur+\delta_3r^2 & r^2\delta_4+rvuv+\delta_3rv \\ 0 & 0 & 0 & ur^3 & ur^2v \\ 0 & 0 & 0 & 0 & r^3v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Sejam

$$\begin{aligned} \Delta_1 &= ur\delta_3+uvur+\delta_1r^2, \\ \Delta_2 &= ur\delta_4+(uv)^2+\delta_1rv, \\ \Delta_3 &= r^2\delta_3+rvur+\delta_3r^2, \\ \Delta_4 &= r^2\delta_4+rvuv+\delta_3rv, \end{aligned}$$

então

$$x^4 = \begin{bmatrix} 0 & ur^3 & ur^2v & \Delta_1 & \Delta_2 \\ 0 & 0 & r^3v & \Delta_3 & \Delta_4 \\ 0 & 0 & 0 & ur^3 & ur^2v \\ 0 & 0 & 0 & 0 & r^3v \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Como $x^6 = x^4x^2$ temos que

$$x^6 = \begin{bmatrix} 0 & 0 & 0 & ur^3\delta_3 + ur^2vur + \Delta_1r^2 & ur^3\delta_4 + ur^2vuv + \Delta_1rv \\ 0 & 0 & 0 & r^3vur + \Delta_3r^2 & r^3vuv + \Delta_3rv \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note agora que

$$\begin{aligned} & ur^3\delta_3 + ur^2vur + \Delta_1r^2 \\ &= ur^3\delta_3 + ur^2vur + (ur\delta_3 + uvur + \delta_1r^2)r^2 \\ &= ur^3(rc + vu + cr) + uvur^3 + ur^3\delta_3 + uvur^3 \\ &= ur^3vu + ur^3cr + ur^3(rc + vu + cr) = 0. \end{aligned}$$

Procedendo analogamente para as expressões acima verifica-se que x^6 é um elemento da forma 3.6 com $f = ur^3vw + wur^3v + urvurv$. Como

$$f = [ur^3v, w] + (urv)^2 = (ur^3v + w)^2 + (ur^3v)^2 + w^2 + (urv)^2,$$

temos que $f \in \overline{M_n}$ para todo $n > 0$ então $x^6 = 0$.

Portanto a álgebra B_n satisfaz a identidade $x^6 = 0$. Isso completa a prova do teorema.

Referências Bibliográficas

[1] Bahturin, Yu.A., Olshanskiy, A.Yu., *Identical relations in finite Lie rings*, Mat. Sb., **96** (1975), 543-559.

[2] Belov, A.Ya., *On non-Specht Varieties*, Fundam. Prikl. Mat., **5** (1999), 47-66 (Russo).

[3] Belov, A.Ya., *Counterexamples to the Specht problem*, Mat. Sb., **191** (2000), 13–24; English translation in Sb. Math., **191** (2000), 329–340.

[4] Drensky, V.S., Free Algebras and PI-Algebras, Springer, Singapore, 2000.

[5] Grishin, A.V., *Examples of T-Spaces and T-ideals of Characteristic 2 without the Finite Basis Property*, Fundam. Prikl. Mat., **5** (1999), 101-118 (Russo).

[6] Grishin, A.V., *On non-Spechtianness of the variety of associative rings that satisfy the identity* $x^{32} = 0$, Electronic Research Announcements of the American Mathematical Society, **6** (2000), 50–51 (electronic).

[7] Gupta, C.K., Krasilnikov, A.N., *A simple example of a non-finitely based system of polynomial identities*, Communications in Algebra, **30** (2002), 4851-4866.

[8] Gupta, C.K., Krasilnikov, A.N., *A non-finitely based system of polynomial identities which contains the identitiy* $x^6 = 0$, Quarterly Journal of Mathematics, **53** (2002), 173-183.

[9] Kemer, A.R., Ideals of Identities of Associative Algebras, Translations of Math. Monographs **87**, AMS, Providence, RI, 1991.

[10] Neumann, B.H., *Identical relations in groups. I*, Mathematische Annalen, **114** (1937), 506-525.

[11] Oates, S., Powell, M.B., *Identical relations in finite groups*, Journal of Algebra, **1** (1964), 11-39.

[12] Rotman, J.J., Advanced Modern Algebra, Prentice Hall; 2nd printing 2003.

[13] Shchigolev, V.V., *Examples of infinitely based T-ideals*, Fundam. Prikl. Mat. **5** (1999), 307-312 (Russo).

[14] Shchigolev, V.V., *Construction of non-finitely based T-ideals*, Communications in Algebra, **29** (2001), 3935-3941.

[15] Specht, W., *Gesetze in Ringen. I*, Mathematische Zeitschrift, **52** (1950), 557-589.

[16] Popov, A.P., *Some Finitely Based Varieties of Rings*, C. R. Acad. Bulgare Sci., **32** (1979), 855-858.

[17] Krasilnikov, A.N., *Identities of Triangulable Matrix Representations of Groups*, Trans. Moscow Math. Soc. **1990** (1991), 233-249.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo