
**Sobre polinômios centrais em uma e duas variáveis para $M_2(K)$
quando K é um corpo finito**
**On central polynomials in one and two variables for $M_2(K)$
when K is a finite field**

Júlio César dos Reis

Departamento de Ciências Exatas, UESB, Vitoria da Conquista, Brasil
E-mail: julio@uesb.edu.br.

Resumo

Sejam K um corpo finito com q elementos e $M_2(K)$ a álgebra das matrizes de ordem dois sobre K . Conhecemos alguns exemplos de polinômios centrais, mas a base dos polinômios centrais de $M_2(K)$ é desconhecida. Neste artigo, exibimos um polinômio central $c(x)$ em uma variável para $M_2(K)$ tal que todo polinômio central em uma variável é um múltiplo de $c(x)$.

Também exibimos uma conjectura para a base dos polinômios centrais para $M_2(K)$.

Palavras-chave polinômio central, matrizes, corpos finitos, T-espaco, pi-álgebra.

Abstract

Let K be a finite field with q elements and let $M_2(K)$ be the matrix algebra of order two over K . We know some examples of central polynomials but the basis of central polynomials of $M_2(K)$ is unknown. In this paper we exhibit a central polynomial $c(x)$ in one variable for $M_2(K)$ such that every central polynomial in one variable is a multiple of $c(x)$.

We also exhibit a conjecture for the basis of the central polynomials for $M_2(K)$.

Keywords central polynomial, matrices, finite fields, T-space pi-algebra.

1 Introdução

Em 1956, Kaplansky [14] propõe uma lista de problemas em aberto em Teoria de Anéis e entre os problemas está a existência de polinômios centrais para a álgebra de matrizes $M_n(K)$ com $n > 2$.

A resposta afirmativa é dada por Formanek [9] e por Razmyslov [22] que criam, independentemente, dois métodos para a construção de polinômios centrais para $M_n(K)$. Mais tarde, outros polinômios centrais para $M_n(K)$ são construídos, veja por exemplo [6, 12, 13, 21].

Descrever os polinômios centrais de uma álgebra é um problema muito importante na teoria das álgebras com identidades polinomiais (ou PI-teoria). Apesar da importância existem poucos resultados nessa linha. Por exemplo, para a álgebra das matrizes $M_n(K)$ com entradas num corpo K conhece-se geradores para os polinômios centrais apenas para $n = 2$ e com hipóteses adicionais sobre K : se K tem característica zero (ver[20]) e quando K é infinito e tem característica diferente de 2 (veja [3]). Não se conhece a base dos polinômios centrais para $M_2(K)$ quando K é um corpo finito.

Neste artigo exibimos um polinômio central $c(x)$ em uma variável para $M_2(K)$ tal que todo polinômio central para $M_2(K)$ em uma variável é um múltiplo de $c(x)$. Também exibimos uma conjectura para a base dos polinômios centrais para $M_2(K)$ acrescentando a hipótese de que K tem característica diferente de 2.

2 Preliminares

Estamos interessados em polinômios centrais para uma álgebra A sobre um corpo K . Um polinômio $c(x_1, \dots, x_m) \in K\langle X \rangle$ sem termo constante é chamado um polinômio central para a álgebra A se $c(x_1, \dots, x_m)$ não é uma identidade polinomial de A e $c(a_1, \dots, a_m) \in Z(A)$ para todos $a_1, \dots, a_m \in A$, em que $Z(A)$ é o centro de A .

Para esclarecer a definição anterior é importante definir $K\langle X \rangle$ como a álgebra associativa livre, livremente gerada por X sobre K , em que $X = \{x_1, x_2, x_3, \dots\}$ é um conjunto enumerável. Na prática, pensaremos em $K\langle X \rangle$ como a álgebra dos polinômios em variáveis não comutativas $x_1, x_2, x_3, \dots$. Também veremos $c(a_1, a_2, \dots, a_n)$ como o elemento de A que se obtém substituindo x_i por $a_i \in A$ em c .

Um exemplo de polinômio central é dado quando $A = E$, em que E é a álgebra de Grassmann (ou exterior). Nesse caso, $c_3(x_1, x_2) = [x_1, x_2]$ é um polinômio central, em que $[x_1, x_2] = x_1x_2 - x_2x_1$ é o comutador usual. Outro exemplo é dado para $A = M_2(K)$. Temos que $c_2(x_1, x_2) = [x_1, x_2]^2$ é um polinômio central para $M_2(K)$.

Como já citado na introdução, uma pergunta natural é se existem polinômios centrais para a álgebra das matrizes $M_n(K)$, com $n > 2$, pergunta feita por Kaplansky em 1956. A resposta afirmativa é dada primeiramente por Formanek e Razmyslov e depois por vários outros autores que criam métodos para a construção de polinômios centrais para $M_n(K)$.

Outra pergunta natural é quais são todos os polinômios centrais para $M_n(K)$ com $n > 2$, ou seja, queremos descrever os polinômios centrais para $M_n(K)$. Para responder a esta pergunta, pensemos na estrutura do conjunto $CP(A)$ dos polinômios centrais de uma álgebra A . Claramente $CP(A)$ é um subespaço de $K\langle X \rangle$. Mais ainda, $CP(A)$ é invariante sob todos os endomorfismos de $K\langle X \rangle$, por isso, $CP(A)$ é dito ser um T-espaço. Como intersecção de T-espaços é um T-espaço, podemos falar que um conjunto $S \subset K\langle X \rangle$ gera um T-espaço C se a intersecção de todos os T-espaços que contêm S é C . Neste caso S é dito ser uma base de C .

Outra maneira de entender a base dos polinômios centrais é pensar que a base dos polinômios centrais é o conjunto de “alguns” polinômios centrais com os quais, fazendo as operações permitidas, consigamos todos os polinômios centrais. Quais são as operações permitidas entre polinômios centrais? É possível somar, multiplicar por um elemento de K (pelo fato de ser subespaço) e trocar as variáveis por qualquer elemento de $K\langle X \rangle$ (por ser invariante por endomorfismos). Esta maneira é análoga a ideia de base de espaço vetorial: nos perguntamos por um número “pequeno” de vetores que (com as operações permitidas) gerem todos os outros.

Encontrar bases para os polinômios centrais de uma álgebra é um problema muito importante na teoria das álgebras com identidades polinomiais. Nessa generalidade o problema está muito longe de ser resolvido. Se pensarmos numa álgebra específica, por exemplo, a álgebra das matrizes $M_n(K)$ são conhecidas as bases dos polinômios centrais apenas para $n = 2$ e com hipóteses adicionais sobre K : se K tem característica zero (veja [20]) e quando K é infinito e tem característica diferente de 2 (ver [3]). Não se conhece a base dos polinômios centrais para $M_2(K)$ quando K é um corpo finito.

Como pouco se sabe sobre polinômios centrais “ordinários”, estudam-se outros tipos de polinômios centrais: A-polinômios centrais e polinômios centrais graduados são alguns dos exemplos. Fixaremos nossa atenção no último exemplo: polinômios centrais graduados.

2.1 Polinômios centrais graduados

A noção de polinômio central graduado surge quando adicionamos uma graduação em A e em $K\langle X \rangle$.

Dado um grupo G , organizamos o conjunto $X = \{x_1, x_2, \dots, x_n, \dots\}$ das variáveis de forma a termos $X = \bigcup_{g \in G} X_g$ e $X_g \cap X_h = \emptyset$, para todo $g \neq h \in G$. Usamos a notação, $\alpha(x_i) = g$ para dizer que $x_i \in X_g$. Definimos $\alpha(x_1 x_2 \dots x_n) = \alpha(x_1) + \alpha(x_2) + \dots + \alpha(x_n)$ e $\alpha(1) = 0$. Se m é um monômio de $K\langle X \rangle$, então $\alpha(m)$ é o G -grau de m . Seja $K\langle X \rangle_g$ o subespaço de $K\langle X \rangle$ gerado pelos monômios m de G -grau g , em que $g \in G$. Assim $K\langle X \rangle = \bigoplus_{g \in G} K\langle X \rangle_g$ com $K\langle X \rangle_g K\langle X \rangle_h \subseteq K\langle X \rangle_{g+h}$ para todo $g, h \in G$.

Também graduamos a álgebra $A = \bigoplus_{g \in G} A_g$ com $A_g A_h \subseteq A_{g+h}$ para quaisquer $g, h \in G$. Um polinômio central graduado para A é um polinômio (que não é identidade polinomial graduada) sem termo constante $f(x_1, \dots, x_n)$ tal que $f(a_1, \dots, a_n) \in Z(A)$, para todos $a_i \in A_{\alpha(x_i)}$, com $i \in \{1, 2, \dots, n\}$ e $Z(A)$ é o centro de A . Em outras palavras, é um polinômio central (como antes) mas que respeita a graduação na hora de substituir as variáveis.

Novamente, podemos colecionar os polinômios centrais graduados e ver que o conjunto $C_G(A)$ de todos os polinômios centrais graduados de A é um subespaço vetorial de $K\langle X \rangle$ que é fechado sob os endomorfismos graduados de $K\langle X \rangle$ e será chamado de T_G -espaço. Podemos nos perguntar por bases para os polinômios centrais graduados. Neste caso, os resultados conhecidos são mais gerais: conhecemos bases dos polinômios centrais graduados para $M_n(K)$, quando K é infinito, considerando graduações sobre Z e Z_n (ver [2]) e sobre graduações elementares (ver [8]), quando K tem característica zero.

2.2 Identidades polinomiais

Como já dissemos, escrever os polinômios centrais de uma álgebra é um problema importante na teoria das álgebras com identidades polinomiais. Um polinômio $p(x_1, \dots, x_m) \in K\langle X \rangle$ é dito ser uma identidade polinomial para a álgebra A se $p(a_1, \dots, a_m) = 0$ para todos $a_1, \dots, a_m \in A$.

Outro problema muito importante na PI teoria é encontrar bases para as identidades polinomiais de uma álgebra. Apenas para citar a álgebra das matrizes, já são conhecidas bases das identidades polinomiais de $M_2(K)$ quando K tem característica zero ([23, 7]) ou quando K é infinito e tem característica diferente de 2 ([15]). É interessante notar que não se conhece a base das identidades polinomiais para $M_3(K)$ nem mesmo em característica zero.

Quando K é finito são conhecidas bases das identidades polinomiais de $M_2(K)$ [19], $M_3(K)$ [10] e $M_4(K)$ [11].

Também para as identidades polinomiais existe a versão graduada e novamente temos uma quantidade um pouco maior de resultados.

Quando K é um corpo finito são conhecidas bases das identidades polinomiais graduadas de $M_2(K)$ levando em conta todas as graduações possíveis sobre Z_2 (ver [16] para característica diferente de 2 e [24] para característica 2).

Quando K é um corpo de característica zero ou infinito de característica maior que 2, são conhecidas bases das identidades polinomiais graduadas de $M_n(K)$ (considerando graduações usuais sobre os grupos Z , Z_n e $Z_n \times Z_n$).

Ainda com K infinito e de característica 2, é conhecida uma base das identidades polinomiais graduadas de $M_2(K)$, considerando uma graduação não usual sobre o grupo Z_2 (ver [17]).

Voltemos a falar de polinômios centrais.

3 Resultado principal

Nesta seção, descrevemos o resultado principal deste artigo.

Em [5, exercício 7.3.21] temos que se K é um corpo finito com q elementos e $p(x) \in K[x]$ é um polinômio irredutível de grau n , então

$$c(x) = \prod_{m=1}^{n-1} (x^{q^m} - x)^{(q^n-1)n} \left(\frac{x^{q^n} - x}{p(x)} \right)^{(q^n-1)n}$$

é um polinômio central para $M_n(K)$.

Fixando $n = 2$. Para $q = 2$ temos $c(x) = (x^2 - x)^{12}$, um polinômio de grau 24, para $q = 3$ temos polinômios de grau 160 e no caso geral, temos polinômios de grau $2(q^4 + q^3 - 3q^2 - q + 2)$.

Uma pergunta natural é: existem polinômios centrais em uma variável para $M_2(K)$ com grau menor? A resposta é sim, e é dada pela próxima proposição.

Proposição 3.1 *Seja K um corpo finito com q elementos. O polinômio*

$$c(x) = (x^q - x)^2$$

é um polinômio central de $M_2(K)$.

Demonstração:

Denotamos K por $GF(q)$. Sabemos que é suficiente considerar a forma de Jordan. As possíveis formas de Jordan são $J_1(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^q \end{pmatrix}$ ou $J_2(a) = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ em que $\alpha \in GF(q^2)$ e $a \in K$. Sabemos que $a^q = a$ e $qa = 0$. Um cálculo simples mostra a proposição. ■

O resultado principal deste artigo é mais forte.

Teorema 1 *Seja K um corpo finito com q elementos. Todo polinômio central em uma variável de $M_2(K)$ é um múltiplo de $c(x) = (x^q - x)^2$.*

Para provar este teorema usaremos os lemas seguintes.

Lema 1 *Seja $f(x) \in K[x]$ um polinômio, em que K é um corpo arbitrário. Se $f(x)$ é um polinômio central para $M_2(K)$, então $f(a) = 0$ para todo $a \in K$.*

Demonstração: Veja que $f(ae_{11}) = f(a)(e_{11})$. Lembrando que f não tem termo constante e que e_{ij} é a matriz com a entrada (i, j) igual a 1 e todas as outras, zero. Então $f(a) = 0$. ■

Lema 2 *Sejam $f(x) \in K[x]$ um polinômio, em que K é um corpo arbitrário e $B \in M_2(K)$ uma matriz da forma $B = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, com $a \in K$. Então $f(B) = \begin{pmatrix} f(a) & f'(a) \\ 0 & f(a) \end{pmatrix}$, em que $f'(a)$ é a derivada formal de f .*

Demonstração: Seja $f(x) = a_mx^m + a_{m-1}x^{m-1} + \dots + a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ um polinômio de grau m . A derivada formal de f é $f'(x) = ma_mx^{m-1} + (m-1)a_{m-1}x^{m-2} + \dots + 3a_3x^2 + 2a_2x + a_1$. Agora é só usar indução sobre m . ■

Um resultado conhecido sobre um corpo finito K com q elementos diz que para $f(x) \in K[x]$ se $f(a) = 0$ para todo $a \in K$, então $f(x)$ é múltiplo de $x^q - x$. (Veja [18], por exemplo).

Agora estamos prontos para provar o Teorema 1.

Demonstração: (do Teorema 1) Seja $f(x) \in K[x]$ um polinômio central para $M_2(K)$. Pelo Lema 1 temos $f(x) = (x^q - x)g(x)$. Seja $B \in M_2(K)$ como no Lema 2. Como $f(x)$ é um polinômio central, $f'(a) = 0$ para todo $a \in K$. Como $f'(x) = -g(x) + (x^q - x)g'(x)$ e $f'(a) = 0$ temos $g(a) = 0$ para todo $a \in K$. Consequentemente $g(x) = (x^q - x)h(x)$, isto é, $f(x) = (x^q - x)^2h(x)$. ■

Algumas observações:

- a) O Lema 1 é verdadeiro para $M_n(K)$;
- b) O Lema 2 tem uma versão mais geral, mas hipóteses adicionais sobre o corpo K são necessárias.

4 Conjectura

Como já sabemos, desconhecemos a base dos polinômios centrais para $M_2(K)$ quando K é um corpo finito. O fato de $c(x) = (x^q - x)^2$ ser um importante polinômio central para $M_2(K)$, nos leva a procurar outros polinômios centrais.

Proposição 4.1 *Seja K um corpo finito com q elementos e de característica diferente de 2. Então $c_1(x_1, x_2) = (x_1^q - x_1)(x_2^q - x_2) + (x_2^q - x_2)(x_1^q - x_1)$ é um polinômio central para $M_2(K)$.*

Demonstração: Novamente, basta considerar as formas de Jordan $J_1(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^q \end{pmatrix}$ ou $J_2(a) = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ nas quais $\alpha \in GF(q^2)$ e $a \in K$. Assim temos para $c_1(J_2(a), J_2(b)) = c_1(J_1(\alpha), J_2(b)) = c_1(J_2(b), J_1(\alpha)) = 0$ e $c_1(J_1(\alpha), J_1(\beta)) = 2(\alpha^q - \alpha)(\beta^q - \beta)I_2$, em que I_2 é a matriz identidade de ordem 2. Portanto, c_1 é um polinômio central para $M_2(K)$. ■

Se considerarmos a notação de [19], temos que a identidade polinomial $f_2(x, y)$ que faz parte da base das identidades polinomiais de $M_2(K)$, quando K é um corpo finito, é da forma $f_2(x, y) = c_1(x, y) - [c_1(x, y)]^q$.

Assim a primeira parte de nossa conjectura é que $c_1(x_1, x_2)$ seja parte da base dos polinômios centrais para $M_2(K)$, quando K é um corpo finito e de característica diferente de 2.

A segunda parte da conjectura é que para completar a base dos polinômios centrais para $M_2(K)$ falta um polinômio central, de preferência um polinômio que use explicitamente o fato da matriz ter ordem dois, como por exemplo, $c_2(x_1, x_2) = [x_1, x_2]^2$ que já vimos ser um polinômio central para $M_2(K)$.

Portanto nossa conjectura assume a seguinte forma.

Conjectura 1 *Seja K um corpo finito com q elementos e de característica diferente de 2. Então a base dos polinômios centrais para $M_2(K)$ é formada por $c_1(x_1, x_2) = (x_1^q - x_1)(x_2^q - x_2) + (x_2^q - x_2)(x_1^q - x_1)$ e por $c_2(x_1, x_2) = [x_1, x_2]^2$.*

5 Agradecimentos

O autor gostaria de agradecer a Plamen Koshlukov pelas boas conversas e pelas valiosas sugestões.

Referências

- [1] S. S. Azevedo, P. Koshlukov, A basis for the graded identities of matrix algebra of order two over a finite field of characteristic $p \neq 2$, *Finite Fields Appl.* 8 (2002) 597–609.
- [2] A. Brandão Júnior, Graded central polynomials for the algebra $M_n(K)$, *Rend. Circ. Mat. Palermo* 57 (2008) 265–278.
- [3] J. Colombo, P. Koshlukov, Central polynomials in the matrix algebra of order two, *Linear Algebra Appl.*, 377 (2004) 53–67.
- [4] J. Colombo, P. Koshlukov, Identities with involution for the matrix algebra of order two in characteristic p , *Israel J. Math.*, 146 (2005) 337–355.
- [5] V. Drensky, *Free Algebras and PI-Algebras*, Springer, Singapore, 2000.

-
- [6] V. Drensky, New central polynomials for the matrix algebra, *Israel J. Math.*, 92 (1995) 235-248.
 - [7] V. Drensky, A minimal basis for the identities of a second-order matrix algebra over a field of characteristic 0, *Algebra Logic*, 20 (1981) 188-194.
 - [8] L.F. Fonseca, On the graded central polynomials for elementary gradings in matrix algebra, *Rend. Circ. Mat. Palermo* 63 (2013) 125-132.
 - [9] E. Formanek, Central polynomials for matrix ring, *Journal of Algebra*, 23 (1972) 129-132.
 - [10] G. K. Genov, Basis of identities of a third order matrix algebra over a finite field , *Algebra Logic* 20 (1981) 241-257.
 - [11] G. K. Genov, P. N. Siderov, A basis for identities of the algebra of fourth-order matrices over a finite field. I,II *Serdica Math. J.* 8 (2001) 313-323, 351-366.
 - [12] A. Giambruno, A. Valenti, Central polynomials and matrix invariants, *Israel J. Math.*, 96 (1996) 281-297.
 - [13] P. Halpin, Central and weak identities for matrices, *Commun. Algebra*, 11 (1983) 2237-2248.
 - [14] I. Kaplansky, Problems in the theory of rings, em Conference on Linear Algebra (National Research Council) pp. 1-3, Washington, 1957.
 - [15] P. Koshlukov, Basis of the identities of the matrix algebra of order two over a field of characteristic $p \neq 2$, *J. Algebra* 241 (2001) 410-434.
 - [16] P. Koshlukov, S. Azevedo, A Basis for the Graded Identities of the Matrix Algebra of Order Two over a Finite Field Characteristic $p \neq 2$, *Finite Fields and Their Applications*, 8 (2002) 597-609.
 - [17] P. Koshlukov, J. Reis, Gradings and graded identities for the matrix algebra of order two in characteristic 2, *Serdica Math. J.*, 38 (2012) 189-198.
 - [18] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
 - [19] Yu. N. Maltsev, E. N. Kuzmin, A Basis for identities of the algebra of second order matrices over a finite fields, *Algebra Logic*, 17 (1978) 17-21.
 - [20] S. Okhitin, Central polynomials og the algebra of second order matrices, *Moscow Univ. Math. Bull.*, 43(4) (1988) 49-51.
 - [21] C. Qing, Cumulating central polynomials and identities for $M_n(F_p)$, *Chinese Annals of Math.*, 11B:3 (1990) 346-348.
 - [22] Y. P. Razmyslov, On a problem of Kaplansky, *Math. USSR Izv.*, 7 (1973) 479-496.
 - [23] Y. P. Razmyslov, Finite basing of the identities of a matrix algebra of second order over a field of characteristic zero, *Algebra Logic*, 10 (1973) 47-63.
 - [24] J. Reis, A Basis for the Graded Identities of the Matrix Algebra of Order Two over a Finite Field of Characteristic 2, *Finite Fields and Their Applications*, submitted.