UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA
Autorizada pelo Decreto Federal nº 77.496 de 27/04/76
Recredenciamento pelo Decreto nº17.228 de 25/11/2016
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
COORDENAÇÃO DE INICIAÇÃO CIENTÍFICA

XXIX SEMINÁRIO DE INICIAÇÃO CIENTÍFICA DA UEFS
SEMANA NACIONAL DE CIÊNCIA E TECNOLOGIA - 2025

Identificando álgebras cíclicas de divisão como subanéis de anéis de grupo

Ana Libni Santos Vasconcelos Ferreira[1]; Mauricio de Araujo Ferreira[2]
1.Ana Libni Santos Vasconcelos Ferreira, PIBIC/FAPESB, MATEMATICA, e-mail: analibnivasconcelos@gmail.com
2.Mauricio de Araujo Ferreira, DEPARTAMENTO DE CIÊNCIAS EXATAS, e-mail: maferreira@uefs.br

PALAVRAS-CHAVE: Anéis de grupo; álgebras cíclicas; extensões galoisianas cíclicas.

INTRODUÇÃO

Este trabalho deu continuidade à pesquisa "Anéis de quatérnios de divisão como subgrupos de anéis de grupo sobre o corpo dos racionais", cujo principal resultado demonstrou que a álgebra $(u, v)\_K$, com $u, v \in K\backslash\{0\}$, é isomorfa a um subanel de KL, sendo L um grupo de ordem 64 construído para esse fim. Sendo assim, o objetivo central desses trabalho foi ampliar esse resultado, investigando a presença de álgebras cíclicas em anéis de grupo. Como os quatérnios correspondem ao caso particular de grau n = 2 (dimensão 4), buscou-se generalizar para o caso n = 3, isto é, álgebras de dimensão 9.

METODOLOGIA

A pesquisa é de natureza teórica, assim, resultados foram obtidos por meio da compreensão das propriedades das estruturas estudadas e da análise de casos particulares. Os padrões observados nesses exemplos fornecem indícios para desenvolvimento de uma prova para casos mais gerais. As principais referências foram Dummit e Foote (1991) Milies e Sehgal (2002), Rotman (1994) e Gille e Szamuely, (2006), que embasaram o desenvolvimento da pesquisa e suas conclusões.

RESULTADOS E DISCUSSÃO

Este trabalho de pesquisa tem como objetivo central construir explicitamente uma álgebra cíclica de grau 3 sobre Q e, em seguida, localizá-la como um subanel dentro de um anel de grupo a fim de investigar a relação entre estas estruturas.

Para alcançar tal objetivo, utilizamos conceitos da Teoria de Galois. Uma álgebra cíclica $(K/F, \sigma, a)$ é definida a partir de uma extensão de corpos K/F. É essencial que esta extensão seja galoisiana e cíclica, ou seja, que K seja o corpo de raízes de um polinômio com coeficientes em F, e que seu grupo de Galois, $G(K/F)$, seja um grupo cíclico. O grupo de Galois $G(K/F)$é o conjunto de todos os F-automorfismos de K, isto é, automorfismos ϕ: $K \to K$ que fixam todos os elementos de F.

A pesquisa focou-se no caso mais simples não trivial: uma álgebra cíclica de dimensão 9 sobre Q. Isso requer construir uma extensão cíclica $K/\mathbb{Q}$ de grau 3. O

desafio inicial, portanto, foi encontrar um polinômio irredutível de grau 3 em $\mathbb{Q}[X]$ cujo corpo de raízes fosse uma extensão de grau 3 de $\mathbb{Q}$.

CONSTRUÇÃO DA EXTENSÃO CÍCLICA K/Q

A abordagem bem-sucedida para obter uma extensão de grau 3 partiu do estudo das raízes sétimas da unidade. Seja $\theta \in C$ uma raiz primitiva 7-ésima da unidade. A partir de θ, definimos os seguintes elementos:

$$u = \theta + \theta^6, \quad v = \theta^2 + \theta^5, \quad w = \theta^3 + \theta^4.$$

A partir disso, demonstrou-se que u, v, w satisfazem as seguintes relações

$$u + v + w = -1$$

$$uv + uw + vw = -2$$

$$uvw = 1.$$

Consequentemente, u, v, w são as raízes do polinômio:

$$f(X) = X^3 - X^2 + 2X - 1$$

que é irredutível $\mathbb{Q}[X]$, o que implica que o corpo $K = \mathbb{Q}(u)$ é de dimensão 3 sobre $\mathbb{Q}$e, em particular, temos que $\{1, u, u^2\}$ é uma base de K sobre $\mathbb{Q}$. Além disso, foram verificadas as seguintes relações entre as raízes, como $v = u^2 - 2$ e $w = v^2 - 2$. A primeira relação, implica que $v \in \mathbb{Q}(u) = K$. A segunda, implica que $w \in \mathbb{Q}(v)$, e como $v \in K$, temos também $w \in K$. Isso prova que K contém todas as três raízes de $f(X)$, sendo, portanto, seu corpo de raízes. Concluímos que $K/\mathbb{Q}$ é uma extensão galoisiana de grau 3.

O GRUPO DE GALOIS E O AUTOMORFISMO GERADOR

Para mostrar que a extensão é cíclica, definimos um $\mathbb{Q}$-automorfismo $\sigma: K \to K$. Seu definido pela sua ação na base $\{1, u, u^2\}$ como

$$\sigma(1) = 1, \quad \sigma(u) = v, \quad \sigma(u^2) = v^2.$$

Como σ mapeia uma base de K para outra, isto é, o conjunto $\{1, v, v^2\}$ que também é uma base de K, temos que σ é um isomorfismo de espaços vetoriais. Segue que σ é um $\mathbb{Q}$-automorfismo de K , e, portanto, um elemento de $G(K/\mathbb{Q})$. Além disso, a ação de σ nas raízes u, v, w é cíclica, pois $\sigma(u) = v$, por definição. E, sabendo que $\sigma(v) = w$ e aplicando σ à relação $v = v^2 - 2$, como σ fixa os elementos de $\mathbb{Q}$, temos:

$$\sigma(v) = \sigma(u^2 - 2) = \sigma(u^2) - \sigma(2) = v^2 - 2 = w$$

De modo análogo, temos que $\sigma(w) = u$. Logo, vimos que $\sigma(u) = v$, $\sigma(v) = w$ e $\sigma(w) = u$. Assim, σ permuta os elementos da base B de forma circular. Portanto, $\sigma^2(u) = w$ e $\sigma^3(u) = u$, implicando que $\sigma^3 = Id$. Deste modo, o grupo de Galois é, então, $G(K/\mathbb{Q}) = \{Id, \sigma, \sigma^2\} = \langle\sigma\rangle$, que é um grupo cíclico de ordem 3. Portanto, $\mathbb{Q}(u)$ é a extensão galoisiana que satisfaz as condições desejadas.

DEFINIÇÃO E ESTRUTURA DA ÁLGEBRA CÍCLICA

Definimos a álgebra cíclica $D = (K/\mathbb{Q}, \sigma, a)$, que é um espaço vetorial de dimensão 3 sobre o corpo K, com base $\{1, i, i^2\}$. Assim, um elemento de D tem a forma $\alpha + \beta i + \gamma i^2$, com $\alpha, \beta, \gamma \in$ K. A estrutura de anel é definida por duas regras de multiplicação fundamentais. a primeira é o produto entre elementos da base, dado por

$$i \cdot i = i^2 \qquad e \qquad i \cdot i^2 = i^2 \cdot i = a,$$

onde a é um elemento do corpo F, do qual K é uma extensão. A segunda, é o produto de coeficientes por elementos da base, onde

$$\alpha \cdot i = i \cdot \sigma(\alpha) \qquad \text{e} \qquad \alpha i^2 = i^2 \sigma^2(\alpha), \quad \text{para todo } \alpha \in K.$$

E essas regras se estendem a todos os elementos de D por meio da distributividade e associatividade. Assim a temos que D é uma álgebra de dimensão $[K: \mathbb{Q}] \cdot 3 = 3 \cdot 3 = 9$ sobre $\mathbb{Q}$. É importante destacar que, para ser uma álgebra de divisão, todo elemento não nulo deve ter um inverso. Neste contexto, definimos a norma por $N(\alpha) = \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha)$, e, temos que D é uma álgebra de divisão, se e somente se, o elemento a não for a norma de nenhum elemento $\alpha \in K$. Isto é, se existir algum $\alpha \in K$tal que $N(\alpha) = a$, então a álgebra não será de divisão. Sendo assim, verificamos que se $a = 1$, D não é de divisão, pois, tomando o elemento identidade $\alpha = 1 \in K$, temos

$$N(1) = 1 \cdot \sigma(1) \cdot \sigma^2(1) = 1 \cdot 1 \cdot 1 = 1.$$

Já o caso $a = 2$, verificamos que $N(\alpha) \neq 2$ para qualquer $\alpha \in K$. Logo, D é de divisão.

METODOLOGIA DE IDENTIFICAÇÃO NO ANEL DE GRUPO

A segunda fase da pesquisa consistiu em encontrar um grupo finito G tal que álgebra cíclica de divisão $(K/Q, \sigma, 2)$ pudesse ser vista como um subanel de QG. A estratégia foi focar no caso mais simples, a álgebra $(K/Q, \sigma, 1)$, onde $i^3 = 1$. A tarefa se resume a encontrar, dentro de QG, elementos que se comportem como u, v, w e i que satisfaçam as mesmas relações do produto. Neste contexto, a definição de produto semidireto se mostrou muito útil por ser uma ferramenta ideal para construir grupos não abelianos com as propriedades desejadas. Para o caso em questão, buscamos um grupo G que contenha um elemento de ordem 3 (para representar i) e outros elementos (para representar as raízes u, v, w) cuja conjugação pelo elemento de ordem 3 simule a ação do automorfismo σ.

Foi construído o grupo $G = C_7 \rtimes_\sigma C_3$, onde $C_7 = \langle c \rangle$ e $C_3 = \langle i \rangle$. O produto semidireto é definido por um homomorfismo $\theta : C_3 \to Aut(C_7)$. Como $Aut(C_7) \cong Z_6$ é cíclico, existe um homomorfismo não trivial que mapeia o gerador de C_3 em um automorfismo de ordem 3 em $Aut(C_7)$. Escolhemos o automorfismo $\sigma_\beta(\theta) = \theta^2$. Assim, obtemos o grupo $C_7 \rtimes_\sigma C_3$ de ordem 21 e não é abeliano, pois σ é não trivial, com a seguinte apresentação

$$C_7 \rtimes_\sigma C_3 = \langle c, i \mid c^7 = i^3 = e, ic = c^2 i \rangle.$$

Por fim, verificamos que as relações do produto entre os elementos da base de são preservadas no anel de grupo $\mathbb{Q}(C_7 \rtimes_\sigma C_3)$, uma vez que em $(K/Q, \sigma, 1)$ temos as seguintes relações: $iu = \sigma(u)i, \quad iv = \sigma(v)i, \quad iw = \sigma(w)i.$

Logo, em $\mathbb{Q}(C_7 \rtimes_\sigma C_3)$, pela relação $ic = c^2 i$, verificamos que

$$iu = i(c + c^6) = ic + ic^6 = c^2 i + c^{12} i = c^2 i + c^5 i = (c^2 + c^5)i = vi = \sigma(u)i$$

Analogamente, verificamos que as outras relações da base eram satisfeitas. Assim, identificamos a álgebra $(K/\mathbb{Q}, \sigma, 1)$ como subanel do anel de grupo $\mathbb{Q}(C_7 \rtimes_\sigma C_3)$.

CONSIDERAÇÕES FINAIS

O trabalho focou no estudo de anéis de grupo e na construção de extensões galoisianas cíclicas sobre os racionais. A metodologia incluiu a construção de uma extensão cíclica de grau 3 sobre $\mathbb{Q}$ e o uso do produto semidireto para gerar grupos não abelianos a partir de grupos de menor ordem. Como resultado dos estudos, identificamos a álgebra $(K/\mathbb{Q}, \sigma, 1)$ como subanel do anel de grupo $\mathbb{Q}(C_7 \rtimes_\sigma C_3)$. Por fim, na busca pela identificação da álgebra cíclica $(K/\mathbb{Q}, \sigma, 2)$, em um anel de grupo, observamos que um caminho promissor consiste em considerar um grupo G que possua um subgrupo $H = \langle j^3 \mid j^3 = 1 \rangle$, de modo que o gerador j de H satisfaça a relação $j^3 = 2$ no anel de grupo $\mathbb{Q}G$. Assim, essa abordagem se apresenta como uma possibilidade interessante a ser explorada em pesquisas futuras.

REFERÊNCIAS

DUMMIT, D. S.; FOOTE, R. M. Abstract Algebra. 3rd Edition. Prentice Hall, 1991.

GILLE, P. and SZAMUELY, T. Central simple algebras and Galois cohomology, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, 2006.

MILIES, C. P.; SEHGAL, S. K., An introduction to group rings. Algebras and applications. Volume 1. Springer, 2002.

ROTMAN, J. J. An Introduction to the Theory of Groups. Springer, 1994.