VALORIZAÇÕES EM ÁLGEBRAS DE QUATÉRNIOS SOBRE O CORPO DOS RACIONAIS

Jucineide Silva Santos[1]; Maurício de Araújo Ferreira[2]

1. Bolsista PIBIC/FAPESB, Graduanda em Licenciatura em Matemática, Universidade Estadual de Feira de Santana, e-mail: jucy.mat.uefs@hotmail.com

2. Orientador, Departamento de Ciências Exatas, Universidade Estadual de Feira de Santana, e-mail: Mauriciodearaujo@yahoo.com.br

PALAVRAS- CHAVES: Álgebra com divisão; quatérnios sobre o corpo dos racionais; símbolo de Hilbert.

INTRODUÇÃO

A eficiência da Teoria de Valorizações no estudo de corpos levou naturalmente a tentativa de generalizá-la para estruturas mais gerais como álgebras de divisão e álgebras centrais simples, que podemos chamar de valorizações não comutativas. Hoje conhecidas como valorizações invariantes. Esta teoria só teve um desenvolvimento significativo a partir dos trabalhos de Wadsworth, quando ele estabeleceu em Wadsworth (1986), um critério para a existência de valorizações invariantes em álgebras de divisão.

Pesquisas recentes tem se dedicado a seguinte questão: Se (K,v) é um corpo valorizado e D é um anel de divisão de dimensão finita sobre K então existe uma valorização w em D que estende v? Um caso que merece especial atenção é quando K é o corpo de números racionais e em particular quando D é uma álgebra de quatérnios, isto é, uma álgebra de divisão de dimensão 4 sobre K. Neste caso, não podemos esperar que toda valorização p-ádica de K se estenda para D. Contudo, podemos esperar uma resposta mais fraca para a pergunta acima, qual seja, para quais primos p, a valorização p-ádica de K se estende para D?

Na busca de conhecer sobre quais condições os quatérnios sobre o corpo dos racionais têm uma estrutura de álgebra com divisão, surgiram questões do tipo: Será que existem distintas álgebras de quatérnios de divisão sobre os racionais? Se existem, quantas? Existe um critério para decidir quando uma álgebra de quatérnios sobre os racionais é uma álgebra com divisão? Se existe, qual. Respostas para essas perguntas podem ser encontradas neste trabalho.

METODOLOGIA

Por se tratar de uma pesquisa de cunho teórico, foi feito um levantamento bibliográfico para aprendermos os resultados existentes nas literaturas que discutem o assunto bem como conhecer as técnicas utilizadas para obtê-los. Depois disso partimos para construção exemplos de casos particulares e para investigação do comportamento dos mesmos. Nesses exemplos foram observados alguns padrões os quais nos forneceram indícios para generalização. Após encontrarmos uma generalização buscamos uma prova para esses casos mais gerais. Com isso conseguimos encontrar resultados importantes sobre os quatérnios tendo como base o corpo dos racionais.

RESULTADOS E/OU DISCUSSÃO

Depois da descoberta dos quatérnios de Hamilton, que é um espaço vetorial sobre o corpo dos números reais de dimensão quatro e que é também uma álgebra com divisão, matemáticos tentaram tomar coeficientes em outros corpos para tentar exibir quatérnios que mantivesse a estrutura de anel com divisão, mas não foi possível. O próprio Hamilton tentou exibir quando tomou coeficientes no corpo dos complexos e acabou por descobrir os biquatérnios, mas estes não são aneis com divisão. Quando os coeficientes são tomados no corpo dos racionais, temos uma álgebra com divisão, entretanto se trata de uma subálgebra dos quatérnios de Hamilton.

L.E.Dickson depois de se debruçar sobre a questão de como poderia se definir os elementos estruturais dentro de uma álgebra de dimensão finita sobre um corpo arbitrário F, conseguiu em 1912 mostrar como construir um novo tipo de anel com divisão, surgindo assim os quatérnios generalizados.

Definição1.: *Seja F um corpo de característica diferente de dois e sejam u e v elementos não nulos de F. O anel dos quatérnios generalizados* $(u,v)_F$ *é o F- espaço vetorial*

$$(u,v)_F = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a,b,c,d \in F\}$$

em que a multiplicação é definida da forma:

$$\boldsymbol{i^2} = u, \qquad \boldsymbol{j^2} = v, \qquad \boldsymbol{k^2} = -uv$$

$$\boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}$$

Com os quatérnios generalizados surge a questão sobre quais corpos e sobre quais condições os quatérnios têm uma estrutura de álgebra com divisão. Aqui será tomado como corpo de base os racionais.

Para darmos prosseguimento, precisaremos dos seguintes resultados:

Teorema 1.: *Se a álgebra de quatérnios* $(u,v)_F$ *não é um anel com divisão então ela é isomorfa à álgebra de matrizes* $M_2(F)$.

Lema 1.: *Se a equação* $uX^2 + vY^2 = 1$ *tem solução em F, então* $(u,v)_F$ *é isomorfa a álgebra de matrizes* $M_2(F)$.

Ver as demonstrações em [6].

Com base no teorema 1 e no lema1, dois teoremas importantes para obtenção de quatérnios sobre racionais com divisão foram desenvolvidos. Os teoremas podem ser assim enunciados:

Teorema 2.: $p \equiv 3 \; mod \; 4$ se e somente se $(-1,p)_Q$ é uma álgebra com divisão.

Demonstração. i) Se $Y = 0$ é imediato, ou seja, não tem não tem solução e portanto a álgebra $(-1,p)_Q$ é de divisão.

ii) Para $Y \neq 0$

(=>) Como $p \equiv 3 \; mod \; 4$, p é da forma $4k + 3$, então

$$-1X^2 + pY^2 = 1 \Leftrightarrow -1X^2 + (4k+3)Y^2 = 1$$

$$(4k+3)Y^2 = 1 + X^2 \Leftrightarrow (4k+3) = \frac{1+X^2}{Y^2}$$

$$(4k+3) = \left(\frac{1}{Y}\right)^2 + \left(\frac{X}{Y}\right)^2$$

A equação acima não tem solução, pois, os primos da forma $4k+3$ não podem ser escritos como soma de quadrados.

(<=) Se a álgebra $(-1,p)_Q$ é de divisão a equação $-1X^2 + pY^2 = 1$ não tem solução, sendo assim

$$-1X^2 + pY^2 = 1 \Leftrightarrow pY^2 = 1 + X^2$$

$$p = \frac{1+X^2}{Y^2} \Leftrightarrow p = \left(\frac{1}{Y}\right)^2 + \left(\frac{X}{Y}\right)^2$$

Para que a equação não tenha solução p não pode ser escrito com soma de quadrados o que resta como solução que p seja da forma $4k+3$, ou seja, $p \equiv 3 \bmod 4$. Logo a álgebra $(-1,p)_Q$ é de divisão se $p \equiv 3 \bmod 4$.

■

***Teorema* 3.:** Se $p = 2$ ou $p \equiv 1 \bmod 4$ então $(-1,-p)_Q$ é uma álgebra com divisão.

Demonstração. i) Se $Y = 0$ é imediato, ou seja, não tem não tem solução.

ii) Se $p = 2$, temos

$$-1X^2 - pY^2 = 1 \Leftrightarrow -1X^2 - 2Y^2 = 1$$

$$-(X^2 + 2Y^2) = 1$$

Como a soma de dois quadrados é sempre positiva, temos que a equação acima não tem solução.

iii) Se $p \equiv 1 \bmod 4$, p é um primo que pode ser escrito com soma de quadrados, digamos $p = \alpha^2 + \beta^2$

$$-1X^2 - pY^2 = 1 \Leftrightarrow -1X^2 - (\alpha^2 + \beta^2)Y^2 = 1$$

$$-(\alpha^2 + \beta^2)Y^2 = 1 + X^2 \Leftrightarrow -(\alpha^2 + \beta^2) = \frac{1+X^2}{Y^2}$$

$$-(\alpha^2 + \beta^2) = \left(\frac{1}{Y}\right)^2 + \left(\frac{X}{Y}\right)^2$$

Novamente temos que a soma de dois quadrados é sempre positiva e por isso temos que a equação acima não tem solução.

■

Com esses dois últimos teoremas podemos afirmar que existe infinitas álgebras de quatérnios sobre os racionais que são de divisão, já que existem infinitos p primos.

Para quaisquer que sejam u e v podemos calcular para quais primos p, a valorização p-ádica dos racionais se extende para os quatérnios sobre os racionais, e assim decidirmos se temos uma álgebra de quatérnios com divisão, para tanto utilizaremos o símbolo de Hilbert.

O símbolo de Hilbert é computado da seguinte forma:

Para o corpo Q_p, que é um completamento do corpo dos racionais via valorização p-ádica. Se a,b se escreve sob a forma $p^\alpha u$, $p^\beta v$, onde u e v pertencem ao grupo U das unidades p-ádicas, temos

$$(a,b) = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \quad se\ p \neq 2$$

$$(a,b) = (-1)^{\varepsilon(u)\varepsilon(v)+ \alpha\omega(v)+ \beta\omega(u)} \ \ se\ p = 2$$

Lembremos que $\left(\frac{u}{p}\right)$ denota o símbolo de Legendre.

A computação do símbolo de Hilbert tem dois únicos resultados, $(a,b) = 1$ quando não é uma álgebra de divisão e $(a,b) = -1$ se for uma álgebra de divisão. Com isso encontramos uma maneira saber para quais primos p a valorização p-ádica dos racionais se extende para os quatérnios e de decidir quando uma álgebra quatérnios sobre os racionais é uma álgebra com divisão.

CONSIDERAÇÕES FINAIS

As novas descobertas feitas nesta pesquisa sobre os quatérnios sobre o corpo dos números racionais darão contribuições importantes à teoria dos anéis com divisão estudada por grandes matemáticos. E também no ramo da Física tendo em vista sua vasta aplicabilidade nesta área do conhecimento.

REFERÊNCIA BIBLIOGRÁFICA

[1] BIRKHOFF, Garrett; MACLANE, Saunders. Álgebra Moderna Básica. 4ª edição. Rio de Janeiro: Guanabara Dois S. A, 1980.

[2] FELZENSZWALB, B. Álgebras de Dimensão Finitas. In: 12º Colóquio Brasileiro de Matemática. Rio de Janeiro, IMECC. 1979.

[3] POLCINO, César; Anéis com divisões: Uma introdução de sua história. In: Anais da 18ª Escola de Álgebra, Campinas -São Paulo, 2004.

[4] SERRE, Jean Pierre; A course in Arithmetic. New York: Springer, 1996.

[5] SCHILLING, O. F. G., The Theory of Valuations. Math. Surveys and Monograph, 4, Amer. Math. Soc. Providence,1950.

[6] WADSWORTH, A. R.: Extending valuations to finite-dimensional division algebras. Proc. Amer. Math. Soc. v. 98(1986), no. 1, 20--22.

[7] WADSWORTH, A. R.: Valuation theory on finite dimensional division algebras. Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999), 385--449, Fields Inst. Commun, 32, Amer. Math. Soc., Providence, RI, 2002.