Álgebras de divisão sobre $\mathbb{Q}$

Marcos Emanuel Veríssimo do Nascimento

IMECC - Unicamp

m251419@dac.unicamp.br

Resumo

É atribuído ao matemático William Rowan Hamilton a descoberta dos quatérnions, um conjunto que se mostrou de suma importância para o desenvolvimento histórico da álgebra. Os reais, os complexos e os quatérnions são as únicas álgebras de divisão associativas sobre o corpo dos reais, a menos de isomorfismo, resultado demonstrado por Frobenius. Nesta apresentação, serão utilizadas as chamadas "álgebras de quatérnion" e a linguagem de formas quadráticas para analisar as álgebras de divisão sobre os racionais.

Objetivos

Focaremos em definir os principais conceitos à respeito de álgebras de quatérnion, e mostrar como a norma dessas álgebras relacionam formas quadráticas e a existência de álgebras de divisão sobre um dado corpo. Por fim, iremos utilizar essa ferramenta para de fato mostrar a existência de uma infinidade de álgebras de divisão não isomorfas sobre $\mathbb{Q}$.

1 Definições

Durante o restante do texto, F denotará um corpo arbitrário, com característica diferente de 2.

Definição 1.1. Um conjunto A munido de duas operações binárias $(+, *)$ e de uma operação binária externa (multiplicação por escalar) $\cdot : F \times A \longrightarrow A$ é uma *álgebra associativa sobre* F (ou uma F-álgebra) se as seguintes condições são satisfeitas:

1. $(A, +, \cdot)$ é um espaço vetorial sobre F
2. $(A, +, *)$ é um anel (associativo)
3. $\lambda(xy) = (\lambda x)y = x(\lambda y)\ \forall \lambda \in F$ e $\forall x, y \in A$

Se além disso todo elemento de $A - \{0\}$ for invertível em relação à multiplicação, dizemos que A é uma *álgebra de divisão*

Definição 1.2. Sejam a e b elementos não nulos de F. Uma F-álgebra A de dimensão 4 é chamada de *Álgebra de quatérnion generalizada* sobre F, e é denotada por $A = \left(\frac{a,b}{F}\right)$ se o conjunto $\{1, i, j, k\}$ é uma base de A e a multiplicação bilinear **associativa** é definida pelas condições que 1 é a unidade e

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k \tag{1}$$

(Temos como exemplo base o conjunto dos quatérnions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, que motivou tal definição). Podemos escrever a álgebra definida acima como $A = \left(\frac{a,b}{F}\right) = F \oplus A_+$, em que $A_+ = Fi \oplus Fj \oplus Fk$, e chamamos $z \in A_+$ de *quatérnion puro*.

Definição 1.3. Seja $x = c_0 + z$, $c_0 \in F$ e $z \in A_+$. Chamamos de *conjugado* de x o elemento $\bar{x} = c_0 - z$. Assim, definimos a *norma* de um elemento $x \in A$ por

$$v(x) = x\bar{x} \tag{2}$$

Se $x = c_0 + c_1 i + c_2 j + c_3 k$, então

$$v(x) = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2 \tag{3}$$

Utilizando apenas as definições anteriores, não é difícil mostrar a seguinte proposição:

Proposição 1.1. As seguintes condições são equivalentes para $A = \left(\frac{a,b}{F}\right)$:

1. A é uma álgebra de divisão;
2. $x \in A - \{0\}$ implica $v(x) \neq 0$;
3. Se $(c_0, c_1, c_2) \in F^3$ satisfaz $c_0 = ac_1^2 + bc_2^2$, então $c_0 = c_1 = c_2 = 0$

2 Isomorfismos de álgebras de quatérnion

Agora que já sabemos uma maneira de identificar quando uma álgebra de quatérnion é de divisão, o próximo passo crucial é saber quando duas álgebras de quatérnion são isomorfas:

Lema 2.1. Sejam $A = \left(\frac{a,b}{F}\right)$ e $A' = \left(\frac{a',b'}{F}\right)$ álgebras de quatérnion com as respectivas normas v e v'. A é isomorfa a A' se e somente se existir um isomorfismo de espaços vetoriais ϕ de A_+ até A'_+ tal que $v'(\phi(z)) = v(z)$ para todo $z \in A_+$

2.1 Formas quadráticas

Definição 2.1. Seja A uma álgebra sobre um corpo F. Uma função $Q : A \longrightarrow F$ é uma *forma quadrática* em A se:

1. $Q(ax) = a^2 Q(x)\ \forall a \in F$ e $x \in A$
2. A função $B(x, y) = Q(x, y) - Q(x) - Q(y)$ é uma forma bilinear

Utilizaremos então que a norma $v(z) = \Phi(c_1, c_2, c_3)$, em que Φ é a forma quadrática ternária $-ax_1^2 - bx_2^2 + abx_3^2$ Podemos escrever tal forma quadrática na representação matricial:

$$\Phi(x_1, x_2, x_3) = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} M \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \tag{4}$$

e dizemos que duas formas quadráticas Φ e Φ' são *equivalentes* se existe uma matriz N não singular tal que $M = N^T M' N$. Assim, é possível reescrever o lema da seguinte maneira:

Proposição 2.2. As álgebras de quatérnion $A = \left(\frac{a,b}{F}\right)$ e $A' = \left(\frac{a',b'}{F}\right)$ são isomorfas se e somente se as formas quadráticas $ax_1^2 + bx_2^2 - abx_3^2$ e $a'x_1^2 + b'x_2^2 - a'b'x_3^2$ são equivalentes.

Teorema 2.3 (Teorema do cancelamento de Witt)**.** Se Φ e Ψ são duas formas quadráticas tais que $ax_1^2 + \Phi(x)$ é equivalente a $ax_1^2 + \Psi(x)$, então Φ é equivalente à Ψ.

3 Conclusão

Agora com todas as ferramentas necessárias, iremos finalmente demonstrar a existência de infinitas $\mathbb{Q}$-álgebras de divisão não isomorfas .

Proposição 3.1. Se p é primo congruente a $3 \pmod 4$, então $A = \left(\frac{-1,p}{\mathbb{Q}}\right)$ é álgebra de divisão.

A demonstração segue diretamente do critério apresentado no item 3 da proposição 1.1, tirando o denominador comum e utilizando módulo 4.

Proposição 3.2. Se p e q são primos distintos, ambos congruentes a $3 \pmod 4$, então $\left(\frac{-1,p}{\mathbb{Q}}\right) \ncong \left(\frac{-1,q}{\mathbb{Q}}\right)$

Utilizaremos a proposição 2.2. Após aplicar o teorema 2.3, suponha que $px_1^2 + px_2^2$ é equivalente à $qx_1^2 + qx_2^2$. Então, encontramos a seguinte expressão matricial:

$$\begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} q & 0 \\ 0 & q \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{5}$$

com $a, b, c, d \in \mathbb{Q}$. Ao igualarmos a primeira entrada das matrizes acima e tirarmos o denominador comum entre a e b, encontramos a expressão $(m^2 + n^2)q = pd^2$. Mas, tomando mod p e utilizando que -1 não é resíduo quadrático se $p \equiv 3 \pmod 4$, teremos que p divide m e n, e logo $p|d$. Por fim, dividindo ambos os lados por p^2, segue pelo método do descenso infinito de Fermat que de fato não é possível que exista tal equivalência de formas quadráticas. ■

Assim, devido à existência de infinitos primos congruentes a $3 \pmod 4$, concluímos que existem infinitas álgebras de quatérnion de divisão sobre $\mathbb{Q}$ que não são isomorfas entre si.

Referências

[1] Matej Brešar. *Introduction to Noncommutative Algebra*. Universitext. Springer, 2014.

[2] Keith Conrad. Quaternion algebras. https://kconrad.math.uconn.edu/blurbs/.

[3] Richard S. Pierce. *Associative Algebras*. Graduate Texts in Mathematics. Springer, 1982.

Agradecimentos

Agradeço à Fapesp pelo fomento, ao meu orientador Plamen Emilov Kochloukov pelo grande auxílio e à minha família e amigos pelo apoio constante.