Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Matemática

O TEOREMA DOS QUATROS QUADRADOS

EDUARDO SIMÕES DE MOURA
eduardo_simoesmoura@yahoo.com.br

EDUARDO SIMÕES DE MOURA

O TEOREMA DOS QUATRO QUADRADOS

Monografia apresentada ao corpo docente de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, como requisito parcial para à obtenção do título de Especialista em Matemática.

Orientador: Cristina Marques

Belo Horizonte
2009

Sumário

Resumo

Neste trabalho apresentamos a estrutura (de forma elementar) dos quaternios, algumas propriedades e finalizamos demonstrando o clássico teorema dos quatro quadrados de Lagrange.

CAPíTULO 1

Introdução

Uma das mais antigas descoberta da algebra não comutativa foi a descoberta dos Quartenios de Hamilton no princípio do século XIX.

No espaço tridimensional é conveniente tratar quantidades que tenham magnitude e direção, quantidade de força, deslocamento e intensidade elétrica são alguns exemplos dessas quantidades. A adição de vetores é definida pela regra do paralelogramo.

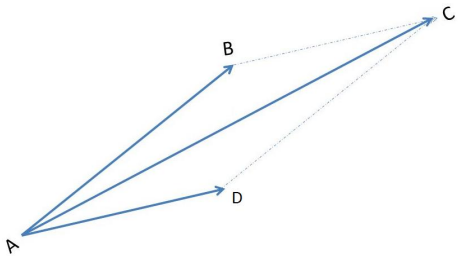

FIGURA 1

Então, no diagrama ABCD é um paralelogramo. $AB + AD = AC$

Para completar a analogia com os sitema de números, é necessária alguma operação análoga a multiplicação. Algumas propriedades devem ser associadas com o produto de dois vetores, tais como a área de um paralelogramo ABCD, quando AB e AD são os vetores o produto é 0 quando os vetores são perpendicular e é máxima quando os vetores estão na mesma direção. Uma interpretação de multiplicação de vetores pode ocorrer quando o vetor AB representa uma força e o vetor AD um deslocamento de A para D do ponto de aplicação. Então o trabalho feito pela força, da mesma forma, será máximo quando AB e AD estão na mesma direção e será 0 quando AB e AD forem perpendiculares.

Hamilton descobriu que colocando junto o produto escalar e o vetorial para produzir um sistema com quatro componentes, a escalar e as três componentes vetoriais, então este sistema apresentaria uma elegante analogia com o sistema numérico ordinal, mas a grande diferença é a não comutatividade da multiplicação.

Tome o plano cartesiano (x, y, z) e denote um vetor unitário paralelo ao eixo ox por i, paralelo a y por j e paralelo a z por k, então um vetor com componentes (x, y, z) será denotado por $xi + yj + zk$.

Se para a regra da multiplicação assumir-mos que:

$$j^2 = k^2 = i^2 = -1, ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$$

então o produto de dois vetores $(xi + yj + zk)(x'i + y'j + z'k)$ terá uma parte escalar que é igual ao produto escalar com o sinal contrário e uma parte vetorial que é igual ao produto vetorial. Então $(xi+yj+zk)(x'i+y'j+z'k) = -(xx' + yy' + zz') + (yz' - y'z)i + (zx' - z'x)j + (xy' - x'y)k$

Os quatérnios assim formados obedecem todas as regras dos números exceto a regra da comutativa da multiplicação. Em particular, e mais importante, eles são associativas.

No capítulo seguinte vamos mostrar mais sobre a estrutura dos quarternios, que será com esses que demonstraremos o teorema dos quatro quadrados.

CAPíTULO 2

Preliminares

Consideremos um subanel particular dos quaternios que sob todos os aspectos, exceção feita a sua não comutatividade, será como um anel euclidiano.

Devido isto será possível caracterizar explicitamente todos os seus ideais à esquerda. Esta caracterização dos ideais a esquerda nos levará rapidamente a uma demonstração do teorema clássico de Lagrange de que todo inteiro positivo é uma soma de quatro quadrados.

Seja Q o anel com divisão dos quaternios reais. Em Q vamos agora introduzir uma operação de conjugação $*$, colocando a

Definição: Para $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ em Q, o adjunto de x, indicado por $x*$,é definido por

$$x = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$$

Observação 1 :

$$\begin{aligned} x \cdot x* &= (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) \\ &= \alpha_0^2 - \alpha_0\alpha_1 i - \alpha_0\alpha_2 j - \alpha_0\alpha_3 k + \alpha_1\alpha_0 - \alpha_1 i\alpha_1 i - \alpha_1 i\alpha_2 j - \alpha_1\alpha_3 k + \alpha_2 j\alpha_0 \\ &- \alpha_2 j\alpha_1 i - \alpha_2 j\alpha_2 j - \alpha_2 j\alpha_3 k + \alpha_3 k\alpha_0 - \alpha_3 k\alpha_1 i - \alpha_3 k\alpha_2 j - \alpha_3 k\alpha_3 k \\ &= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \end{aligned}$$

Observação 2 : $x + x* = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = 2\alpha_0^2$

Lema 1: A conjugação em Q satisfaz;

$$i) x** = x, \ \forall \ x \ \in Q.$$

Demonstração: se $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, então, $x* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ donde $x** = (x*)* = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$

$$ii)(\delta x + \lambda y)* = \delta x* + \lambda y*, \forall \ x, y \in Q \text{ e } \forall \ \delta, \lambda \in \mathbb{R}.$$

Demonstração: Sejam $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ e $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k \in Q$ e sejam δ, λ nos reais. Assim

$$\begin{aligned} (\delta x + \lambda y) &= \\ &= \delta(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + \lambda(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) \\ &= (\lambda\alpha_0 + \delta\beta_0) + (\lambda\alpha_1 + \delta\beta_1)i + (\lambda\alpha_2 + \delta\beta_2)j + (\lambda\alpha_3 + \delta\beta_3)k \end{aligned}$$

Pela definição de $*$,

$$\begin{aligned}(\delta x + \lambda y)* = & \\ &= (\lambda\alpha_0 + \delta\beta_0) - (\lambda\alpha_1 + \delta\beta_1)i - (\lambda\alpha_2 + \delta\beta_2)j - (\lambda\alpha_3 + \delta\beta_3)k \\ &= (\delta\alpha_0 + \lambda\beta_0 - \delta\alpha_1 i - \lambda\beta_1 i - \delta\alpha_2 j - \lambda\beta_2 j - \delta\alpha_3 k - \lambda\beta_3 k) \\ &= \delta\alpha_1 - \delta\alpha_1 i - \delta\alpha_2 j - \delta\alpha_3 k + \lambda\beta_0 - \lambda\beta_1 i - \lambda\beta_2 j - \lambda\beta_3 k \\ &= \delta(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) + \lambda(\beta_0 - \beta_1 i - \beta_2 j - \beta_3 k) \\ &= \delta x * + \lambda y*\end{aligned}$$

$$iii)(xy)* = y * x * \forall x, y \in Q.$$

Demonstração: Em vista de ii) basta fazer para um base de Q sobre os reais. Demonstraremos para a base particular 1, i, j e k. Ora, $ij = k \Rightarrow (ij)* = k* = -k = ji = (-j)(-i) = j * i*$.

Analogamente $(ik)* = k * i*$, $(ij)* = j * i*$. Além disso, $(i^2)* = (-1) = (i*)^2$ e analogamente para k e j. Como iii) vale para todos elementos da base, e ii) vale, temos que iii) é verdadeira para todas as combinações lineares dos elementos da base com coeficientes reais. Logo iii) vale para todo $x, y \in Q$.

Definição: Se $x \in Q$, então a norma de x, indicada por $N(x)$, é definida por $N(x) = x \cdot x* = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$

Observação 3: se $x \neq 0$, notemos que $x^{-1} = \dfrac{x*}{N(x)}$ e $x \cdot \dfrac{x*}{N(x)} = \dfrac{N(x)}{N(x)} = 1$.

Lema 2: $\forall x, y \in Q, N(xy) = N(x)N(y)$.

Demonstração: Pela própria definição de norma $N(xy) = xy(xy)*$. Pela parte iii) do Lema 1 $(xy)* = y * x*$, então $N(xy) = xyy * x* = xN(y)x* = xx * N(y) = N(x)N(y)$.

Observação 4: $N(x)$ é um número real e portanto comuta com todos elementos de Q.

Lema 3 (Identidade de Lagrange). Se α_0, α_1, α_2, α_3 e β_0, β_1, β_2, β_3 são números reais, então

$$(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)(\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2)$$

$= (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3)^2 + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)^2 + (\alpha_0\beta_2 - \alpha_1\beta_0 + \alpha_2\beta_0 + \alpha_3\beta_1)^2 + (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)^2$.

Demonstração: Sejam $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ e $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k \in Q$. Então

$$\begin{aligned} xy = & \\ &= \alpha_0\beta_0 + \alpha_0\beta_1 i + \alpha_0\beta_2 j + \alpha_0\beta_3 k + \alpha_1\beta_0 i - \alpha_1\beta_1 + \alpha_1\beta_2 k - \alpha_1\beta_3 j \\ &+ \alpha_2\beta_0 j - \alpha_2\beta_1 k - \alpha_2\beta_2 + \alpha_2\beta_3 i + \alpha_3\beta_0 k + \alpha_3\beta_1 j - \alpha_3\beta_2 i - \alpha_3\beta_3 \\ &= (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i \\ &+ (\alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1)j + (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)k. \end{aligned}$$

Como $N(xy) = N(x)N(y)$ pelo lema anterior e considerando $N(x) = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)$ e $N(y) = (\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2)$ fica fácil demonstrar a identidade de lagrange.

Agora é o momento de introduzir o anel dos Quaternios de Hurwitz.

Seja

$$\zeta = \{\frac{1}{2}(1 + i + j + k)\}$$

e seja

$$H = \{m_0\zeta + m_1 i + m_2 j + m_3 k; m_0, m_1, m_2, m_3 \in Z\}$$

Lema 4: Seja H um subanel de Q. Se $x \in H$ então $x* \in H$ e $N(x)$ é um número inteiro positivo $\forall x$.

Lema 5: (**Algoritmo da divisão à esquerda**) Sejam a e $b \in H$ com $b \neq 0$. Então existem c e $d \in H$ tais que $a = cb + d$ e $N(d) < N(b)$.

Demonstração: O primeiro caso bem particular $a \in H$ (arbitrário) e b um inteiro positivo n. Suponhamos $a = t_0\zeta + t_1 i + t_2 j + t_3 k$ onde t_0, t_1, t_2, t_3 são inteiros a serem determinados.

Queremos escolhe-los de maneira tal que $N(a - cn) < N(n) = n^2$. Ora, $(c = x_0\zeta + x_1 i + x_2 j + x_3 k)$

$$\begin{aligned} a - cn = & \\ &= (t_0(\frac{1 + i + j + k}{2}) + t_1 i + t_2 j + t_3 k) - nx_0(\frac{(1 + i + j + k}{2}) - nx_1 i - nx_2 j - nx \\ &= \frac{1}{2}(t_0 - nx_0) + \frac{1}{2}(t_0 + 2t_1 - n(t_0 + 2x_1))i + \frac{1}{2}(t_0 + 2t_2 - n(t_0 + 2t_2 - n(t_0 + 2x_2 \\ &+ \frac{1}{2}(t_0 + 2t_3 - n(t_0 + 2x_3))k. \end{aligned}$$

Se podéssemos escolher x_0, x_1, x_2, x_3 de uma maneira tal que $\lceil t_0 - nx_0 \rceil \leqq \frac{1}{2}n$

$\lceil t_0 - 2t_1 - n(t_0 + 2x_1) \rceil \leqq n$
$\lceil t_0 + 2t_2 - n(t_0 + 2x_2) \rceil \leqq n$
$\lceil t_0 + 2t_3 - n(t_0 + 2x_3) \rceil \leqq n$, então teriamos
$N(a-cn) = \dfrac{(t_0 - nx_0)^2}{4} + ... \leqq \dfrac{1}{4}n^2 + \dfrac{1}{4}n^2 + \dfrac{1}{4}n^2 + \dfrac{1}{4}n^2 < n^2$. Que é o resultado desejado. Mas agora afirmamos que isso sempre é possível ser feito.

Passemos o caso geral em que a e b são elementos arbitrários ($b \neq 0$).

Pelo lema 4, $n = bb*$ é inteiro positivo. Assim existe $c \in H$ tal que $ab* = cn + d_1$ onde $N(d_1) < N(n)$. Assim $N(ab* - cn) < N(n)$ mas $n = bb*$ então $N(ab* - cbb*) < N(n) \Longrightarrow N((a - cb)b*) < N(n) = N(bb*)$ que pelo lema 2 $N(a - cb)N(b*) < N(b)N(b*)$ com $N(b*) > 0$ daí $N(a - ab) < N(b)$ colocando $d = ac - b$ e $a = cb + d$ onde $N(d) < N(b)$.

Lema 6 Seja L um ideal à esquerda de H. Então existe um elemento $u \in L$ tal que todo elemento em L é múltiplo à esquerda de u, em outras palavras, existe um $u \in L$ tal que todo $x \in L$ é da forma $x = ru$ onde $r \in H$.

Demonstração: Se $L = (0)$ então $u = 0$ obviamente. Se L possui elementos não nulos. A norma dos elementos não nulos são números inteiros positivos (pelo lema 4), logo existe $u \in L$ tal que $N(u) = \min\{N(x) \text{ com } x \in L\}$. Se $x \in L$ pelo lema 5, $x = cu + d$ onde $N(d) < N(u)$. Contudo de L temos que $N(d) = 0$, pois, norma de u é mínima, então $d = 0$, logo $x = cu$.

Lema 7 Se $a \in H$ então $a^{-1} \in H \Longleftrightarrow N(a) = 1$

Demonstração: ($\Longrightarrow$) Se a a^{-1} est ao em H, pelo Lema 4 $N(a)$ e $N(a^{-1})$ são inteiros positivos $N(a)N(a^{-1}) = N(aa^{-1}) = N(1) = 1$, pois, $ab = 1; a, b \in Z_+$, logo $a = b = 1$.

$\Longleftarrow$ Se $a \in H$ e $N(a) = 1$ então $aa* = N(a) = 1 \Longrightarrow a* = a^{-1}$, mas, $a*$ (pelo Lema 4) pertence a H $a^{-1} \in H$.

CAPíTULO 3

O Teorema dos Quatro Quadrados

Teorema: Todo inteiro pode ser expresso como soma de quadrados de quatro inteiros.

Demonstração: Dado n um inteiro positivo afirmamos no teorema que $n = x_0^2 + x_1^2 + x_2^2 + x_3^2$ para quatro inteiros x_0, x_1, x_2, x_3. Como todo inteiro decomõe-se como produto de números primos, se todo número primo pudesse ser representado com uma soma de quatro quadrados,(pela identidade de Lagrange), todo número poderia ser escrito como soma de quatro quadrados. Reduzimos o problema aos números primos n. Certamente 2 pode ser escrito como $1^2 + 1^2 + 0^2 + 0^2$, assim sem perda de generalidade, podemos supor n primo ímpar, ou seja, $m = p$.Consideremos os quaternios W_p sobre Z_p (inteiros $modP$)

$$W_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k; \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in Z_p\}$$

W_p é um anel finito, além disso, como $p \neq 2$, W_p é não comutativo pois $ij = -ji \neq ji$. Assim, pelo teorama de Wedderburn, ele não pode ser um anel de divisão, ele possui um ideal à esquerda que não é o (0) e não é W_p. Portanto o ideal bilateral V em H definido por $V = \{x_0\zeta + x_1 i + x_2 j + x_3 k; p|x_i\}$, não pode ser maximal à esquerda de H, pois, $\frac{H}{V} \cong W_p$. Se V fosse maximal, $\frac{H}{V} \cong W_p$ seria um corpo logo teria somente dois ideais (o) e W_p. Assim existe um ideal à esquerda L de H satisfazendo: $L \neq H$, $L \neq V$ e $L \supset V$. Pelo lema 6, existe um elemento u tal que todo elemento de L é múltiplo à esquerda de u. Como $p \in V$, $p \in L$ donde $p = cu$ para algum $c \in H$. Como $u \in V$, c não pode possuir inverso em H, pois, caso contrário, $u = c^{-1}p$ estaria em V. Assim $N(c) > 1$(pelo lema 7). Como $L \neq H$, u não pode ter um inverso em H donde $N(u) > 1$. Como $p = cu$, $p^2 = N(p) = N(cu) = N(c)N(u)$, mas, $N(c)$ e $N(u)$ são inteiros e c e u estão em H, ambos são maiores que 1 e ambos dividem p^2. A única saída possível e que $N(c) = N(u) = p$. Como $u \in H$, $u = m_o\zeta + m_1 i + m_2 j + m_3 k$ onde m_o, m_1, m_2 e $m_3 \in Z$, assim, $2u = 2m_o\zeta + 2m_1 i + 2m_2 j + 2m_3 k = m_0(1 + i + j + k) + 2m_1 i + 2m_2 j + 2m_3 k = m_0 + m_0 i + m_0 j + m_0 k + 2m_1 i + 2m_2 j + 2m_3 k = m_0 + (m_0 + 2m_1)i + (m_0 + 2m_2)j + (m_0 + 2m_3)k$, $\Longrightarrow N(2u) = m_0^2 + (m_0 + 2m_1)^2 + (m_0 + 2m_2)^2 + (m_0 + 2m_3)^2$.

Para terminar a demonstração introduzimos um velho artifício de Euller: Se $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$ onde x_0, x_1, x_2, x_3 são inteiros para certos inteiros $a = y_0^2 + y_1^2 + y_2^2 + y_3^2$.

Demonstração do artifício de Euller: Como $2a$ é par temos que, ou todos são pares, ou todos são ímpares, ou 2 pares e 2 ímpares. De qualquer forma, em todos os três casos, podemos reordenar e agrupa-los de maneira tal que

$$y_0 = \frac{x_0 + x_1}{2}, y_1 = \frac{x_0 - x_1}{2}, y_2 = \frac{x_2 + x_3}{2}, y_3 = \frac{x_2 - x_3}{2}$$

sejam todos inteiros. Mas, $y_0^2 + y_1^2 + y_2^2 + y_3^2 = \frac{(x_0 + x_1)^2}{2} + \frac{(x_0 - x_1)^2}{2} + \frac{(x_2 + x_3)^2}{2} + \frac{(x_2 - x_3)^2}{2} = \frac{1}{2}(x_0^2 + x_1^2 + x_2^2 + x_3^2) = \frac{1}{2}2a = a$.

Como $4p$ é soma de quatro quadrados ($4p = N(2u)$) pela observação a pouco feita, $2p$ também o é; como $2p$ é uma soma de quatro quadrados p tamb'em é. Assim $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$ para alguns inteiros a_0, a_1, a_2, a_3.

Referências Bibliográficas

[1] David S. Dummit & Richard M. Foote, *Abstract Algebra*, John Wiley Sons, Inc., 2004.

[2] Thomas W. Hungerford, *Algebra: An Introduction*, Thomson Brooks/Cole, 1996.