UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT

MÁRIO MÁRCIO DOS SANTOS PALHARES

UMA INTRODUÇÃO AOS QUATÉRNIOS

Três Lagoas – MS

2018

MÁRIO MÁRCIO DOS SANTOS PALHARES

UMA INTRODUÇÃO AOS QUATÉRNIOS

Dissertação apresentado a Universidade Federal de Mato Grosso do Sul, como parte das exigências para a obtenção do título de mestre em Matemática.

Orientador: Prof. Dr. Antonio Carlos Tamarozzi

Três Lagoas – MS

2018

Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

UFMS

MÁRIO MÁRCIO DOS SANTOS PALHARES

UMA INTRODUÇÃO AOS QUATÉRNIOS

Dissertação apresentada a Universidade Federal de Mato Grosso do Sul (UFMS/CPTL), como parte das exigências para a obtenção do título de mestre.

Três Lagoas - MS, 31 de outubro de 2018.

BANCA EXAMINADORA

Prof. Dr. Antonio Carlos Tamarozzi
Orientador
UFMS/CPTL

Allan Edley Ramos de Andrade

Prof. Dr. Allan Edley Ramos de Andrade
Membro
UFMS/CPTL

Edson D. Carvalho

Prof. Dr. Edson Donizete de Carvalho
Unesp/ FEIS
Membro

A Deus, que me sustentou e inspirou em todo o meu caminho, possibilitando todas as minhas conquistas profissionais, acadêmicas e pessoais, sem o qual não faria sentido nenhuma dessas façanhas.

Agradecimento

Quero deixar meus sinceros agradecimentos a todos que, de alguma maneira, me ajudaram a chegar até esta etapa. De forma especial quero agradecer ao meu orientador, Prof. Dr. Antonio Tamarozzi, pela sua dedicação e empenho, capazes de proporcionar um crescimento científico, pessoal, intelectual e acadêmico, vivenciados desde minha graduação.

De mesma forma, quero agradecer também a minha família Heloisa (esposa), Pedro (filho), Paulo (pai), Ronilda (mãe), Paulo, Mariane e Juliany (irmãos), que me apoiaram e dedicaram seu tempo em apoio, facilitando o meu caminho para chegar até aqui.

A esta universidade, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presentes.

Resumo

Os quatérnios foram criados por Hamilton, em 1843 como generalização natural dos números complexos. A intenção inicial de duas unidades imaginárias não pode ser concretizada, mas propiciou a criação de uma estrutura de Anel, não comutativo, com diversas aplicações na Matemática e outras ciências. Neste trabalho, estudamos aspectos importantes do conjunto dos números complexos e algumas de suas representações. Em particular destacamos a representação como um conjunto de matrizes, que pode ser explorado no ensino médio.

Palavras chaves: Números complexos, raízes, anéis.

Abstract

Quaternions were created by Hamilton in 1843 as a natural generalization of complex examples. The initial intention of two imaginary units can not be realized, but it did provide for a non-commutative Ring structure with several applications in Mathematics and other sciences. This work, we study the main parts of the set of examples and some of their representations. In particular, highlight a presentation as a set of matrices, which can be explored in high school.

Keywords: Complex numbers, roots, rings.

Sumário

1. Introdução

Uma das dinâmicas mais surpreendentes da Matemática é adaptar-se aos novos confrontos que surgem para a resolução de um problema ou aprofundamento de uma teoria. Muitas vezes estas adaptações são resolvidas criando-se um novo ambiente de trabalho capaz de possibilitar novas técnicas de trabalho. Matematicamente falando isto representa criar um novo conjunto e possivelmente com novas operações e propriedades, preferencialmente que generalizem o conjunto base que foi estendido.

Nesta óptica que foram construídos os conjuntos dos números complexos e dos quatérnios, objetos deste trabalho. Procuramos apresentar diferentes representações destes conjuntos e, para tanto, fez-se necessário assegurar a teoria algébrica mínima que desse sustentação a estas abordagens.

O objetivo deste trabalho é contribuir para a formação do professor de matemática com a apresentação do conjunto dos quatérnios de forma construtiva, a partir dos números complexos. Como aplicação direta ao ensino médio, desenvolvemos uma representação dos números complexos sobre um conjunto de matrizes 2x2, que possibilita inserir em sala de aula o aspecto lúdico e a interação entre diferentes conteúdos matemáticos.

Inicialmente o capitulo 1 trata das estruturas algébricas básicas de Grupos, Anéis e Corpos, bem como, técnicas de trabalho como homomorfismos e isomorfismos. O objetivo é propiciar o aparato algébrico necessário para os principais pontos abordados neste trabalho.

No segundo capítulo, desenvolvemos a teoria básica dos números complexos e a caracterização de $\mathbb{C}$ como um corpo. Destacamos algumas abordagens de $\mathbb{C}$ normalmente não exploradas, mas acessíveis ao ensino médio, como a demonstração das duas formulações de De Moivre, relacionadas a potencias racionais de números complexos na forma polar. Mostramos a representação de $\mathbb{C}$ como um corpo de matrizes de ordem 2, através de um isomorfismo e exploramos aspectos interessantes desta identificação.

O terceiro capítulo tem como objetivo principal tratar de uma outra representação de $\mathbb{C}$, que foi obtida a partir de uma extensão do corpo dos números reais. Embora sem o aprofundamento que esta teoria matemática exige, podemos construir esta representação a partir da noção intuitiva de corpo de decomposição de um polinômio. Esta abordagem possibilitou explorar também exemplos interessantes para a teoria dos corpos.

O último capítulo trata do tema principal deste trabalho. Na literatura matemática não há muita variedade de material disponível sobre o tema e também relacionados aos objetivos desta dissertação. Contudo nosso trabalho de pesquisa propiciou apresentar o anel dos quatérnios de maneira construtiva, seguindo praticamente os caminhos e pensamentos de William Rowan Hamilton, o seu criador. Em particular, mostramos a inviabilidade de construir um conjunto fechado, a partir de uma unidade real e duas imaginárias.

2. Estruturas Algébricas

Vamos começar com algumas definições que serão importantes para o desenvolvimento deste trabalho.

2.1 Grupos

Primeiramente iremos falar sobre um conceito que é uma base primordial para a matemática abstrata, o conceito de grupos.

O conceito de grupo foi originado pela teoria de Galois em 1830, onde procurava descrever as simetrias das equações satisfeitas pelas soluções de uma equação polinomial. Assim, os grupos são geralmente usados para analisar a simetria interna de uma estrutura na forma de automorfismos de grupo.

Definição:

Seja G um conjunto não vazio e $*$ uma operação definida sobre G, formando uma estrutura que será representada por $(G,*)$. Dizemos que $(G,*)$ é um grupo se satisfazer os seguintes axiomas:

$(G1)$ Associatividade: Dados $a, b, c \in G$, temos que $(a * b) * c = a * (b * c)$.

$(G2)$ Elemento Neutro: Seja $e \in G$, então e é um elemento neutro se $e * a = a * e = a$ para qualquer $a \in G$.

$(G3)$ Elemento Simétrico: Para qualquer elemento $a \in G$, existe um outro elemento $a' \in G$, tal que, $a * a' = a' * a = e$, onde e é o elemento neutro.

Caso o grupo satisfaça também o seguinte axioma:

$(G4)$ Comutatividade: Dados $a, b \in G$, então $a * b = b * a$

então $(G,*)$ é chamado de Grupo Abeliano ou Grupo Comutativo.

Exemplo:

Seja os conjuntos $\mathbb{Z}$ e + uma operação definida sobre $\mathbb{Z}$. Vamos mostrar que $(\mathbb{Z}, +)$ é um grupo. Para isto, basta mostrar que os elementos satisfazem os axiomas de grupo.

$(G1)$ Associativa: Dados $a, b, c \in \mathbb{Z}$, temos que $(a + b) + c = a + b + c = a + (b + c)$.

$(G2)$ Elemento Neutro: Temos que 0 é um elemento neutro, pois, $a + 0 = 0 + a = a$ para todo $a \in \mathbb{Z}$.

$(G3)$ Elemento Simétrico: Dado um elemento $a \in \mathbb{Z}$ qualquer, temos que $-a$ é seu simétrico, pois, $a + (-a) = (-a) + a = 0$.

$(G4)$ E como temos que, para qualquer $a, b \in$ que $a + b = b + a$, então $(\mathbb{Z}, +)$ é um grupo abeliano.

2.2 Anéis

O conceito de anel, embora esteja inserido nos estudos da álgebra moderna, teve praticamente todo o seu trabalho desenvolvido por matemáticos nos últimos 80 anos. Adolf Fraenkel (1891-1965) foi um dos pioneiros no tratamento abstrato da teoria dos anéis, onde escreveu o artigo "On the divisors of zero and the decomposition of rings". Porém, Emmy Noether (1882-1935) foi o matemático de maior contribuição para um avanço do estudo na teoria dos anéis.

A teoria dos anéis teve sua importância em várias áreas da matemática, tais como a álgebra homológica, a topologia algébrica e na teoria de código de erros.

Definição:

Um anel é um conjunto A, onde são definidas duas operações, adição e multiplicação, que satisfazem as seguintes condições:

$(A1)$ Comutatividade da soma: Dados $a, b \in A$, então $a + b = b + a$.

$(A2)$ Associatividade da soma: Dados $a, b, c \in A$, então $(a + b) + c = a + (b + c)$.

$(A3)$ Elemento Neutro da soma: Seja $e \in A$ tal que $a + e = e + a = a$.

Nota: o elemento neutro $e = 0$ para adição.

$(A4)$ Elemento simétrico da soma: Para qualquer $a \in A$ existe um elemento $a' \in A$ tal que $a + a' = a' + a = e$.

Nota: o elemento simétrico $a' = -a$ para a adição.

$(M1)$ Associatividade da multiplicação: Dados $a, b, c \in A$, então $(a.b).c = a(b.c)$.

$(M2)$ Distributividade da multiplicação (direita e esquerda): Dados $a, b, c \in A$, temos que

$a.(b + c) = a.b + a.c$ e $(b + c).a = b.a + c.a$.

Caso satisfaça a condição de comutatividade da multiplicação $(M3)$, ou seja, dados $a, b \in A$ onde $a.b = b.a$, então dizemos que A é um anel comutativo.

Usaremos a notação $(A, +, \cdot)$ para representar uma estrutura definido para adição e multiplicação.

Exemplo:

Vamos mostrar agora que $\mathbb{Z}$ também é um anel para as operações usuais de adição e multiplicação, este é um exemplo importante de anel infinito.

Como já vimos no exemplo anterior, $\mathbb{Z}$ é um grupo abeliano para a adição, então já satisfaz as propriedades de associatividade, elemento neutro e elemento simétrico para a adição. Basta agora mostrarmos as duas propriedades seguintes: sem perda de generalidade, vamos assumir $a, b, c \in \mathbb{N}$, o caso geral segue do fato de$(-a)b = a(-b) = -(ab)$.

$(M1)$ Associatividade da multiplicação: Sejam $a, b, c \in \mathbb{Z}$ elementos quaisquer, temos que:

$$(a.b).c = \underbrace{a.b + a.b + \cdots + a.b}_{c\ vezes} = \underbrace{\underbrace{b + b + \cdots + b}_{a\ vezes} + \underbrace{b + b + \cdots + b}_{a\ vezes} + \cdots + \underbrace{b + b + \cdots + b}_{a\ vezes}}_{c\ vezes} =$$

$$\underbrace{b + b + \cdots + b}_{c.a\ vezes} = \underbrace{\underbrace{b + b + \cdots + b}_{c\ vezes} + \underbrace{b + b + \cdots + b}_{c\ vezes} + \cdots \underbrace{b + b + \cdots + b}_{c\ vezes}}_{a\ vezes} =$$

$$\underbrace{b.c + b.c + \cdots + b.c}_{a\ vezes} = a.(b.c).$$

$(M2)$ Distributividade da multiplicação: Sejam $a, b, c \in \mathbb{Z}$ elementos quaisquer, então temos que:

$$a.(b+c) = \underbrace{(b+c)+(b+c)+\cdots(b+c)}_{a\ vezes} = \underbrace{b+c+b+c+\cdots+b+c}_{a\ vezes} =$$

$$\underbrace{b+b+\cdots+b}_{a\ vezes} + \underbrace{c+c+\cdots+c}_{a\ vezes} = a.b + a.c.$$

Como a multiplicação é comutativa para os números inteiros, então temos que $(b+c).a = a.(b+c) = a.b + a.c = b.a + c.a$, o que completa a propriedade distributiva.

2.3 Anéis $\mathbb{Z}_n$

Os conjuntos $\mathbb{Z}_n$, das classes de resto módulo n são exemplos importantes de anéis finitos, com as seguintes operações: dados $\bar{a}, \bar{b} \in \mathbb{Z}_n$,

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a}.\bar{b} = \overline{a.b}.$$

A verificação das propriedades de um anel é semelhante ao caso de $\mathbb{Z}$ e podem ser encontrados em [4]

Podemos observar que o elemento neutro para a soma, desse conjunto, será o $\bar{0}$ e, dado um elemento $\bar{a} \in \mathbb{Z}_n$ qualquer, seu elemento simétrico será o $\overline{n-a}$.

Da mesma maneira, o elemento neutro para a multiplicação será dado por $\bar{1}$.

Exemplo:

Para o conjunto $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, temos que $\bar{0}$ é o elemento neutro para a soma. Em relação aos simétricos aditivos, temos:

Para $\bar{1}$, seu simétrico é $\overline{3-1} = \bar{2}$;

Para $\bar{2}$, seu simétrico é $\overline{3-2} = \bar{1}$.

Para a multiplicação, o elemento neutro é dado por $\bar{1}$ e o elemento simétrico, para $\bar{2}$, é dado pelo elemento $\bar{2}$.

2.4 Produto direto de anéis

Seja A e B anéis, onde, por conveniência, admitiremos munidos das mesmas operações representados por $+$ e $\cdot$ .Podemos definir o produto cartesiano $A \times B$, no qual será definido as seguintes operações $+$ e $\cdot$:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b).(c, d) = (a.c, b.d).$$

Pode-se verificar (veja [4]) que relativo a essas operações $A \times B$ torna-se um anel chamado produto direto dos anéis A e B. Assim são construídos os anéis da forma, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Q}$, $\mathbb{Z} \times \mathbb{Q}$, $\mathbb{R} \times \mathbb{R}$, $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Q}$, etc.

2.5 Anéis de Matrizes

Vamos denotar por $M_n(\mathbb{R})$ o conjunto de todas as matrizes quadradas de ordem n. Pode-se mostrar que, relativo às operações usuais de adição e multiplicação de matrizes esse conjunto forma um anel infinito.

2.6 Anel de Integridade

Definição: Dizemos que $(A, +, \cdot)$ é anel de integridade quando se tratar de um anel com as seguintes propriedades adicionais

$(M4)$ Identidade multiplicativa: Existe $e_1 \in A$ tal que, para qualquer $a \in A$ temos $a.e_1 = e_1.a = a$.

$(M5)$ Ausência de divisores do zero: $a, b \in A$, $a.b = 0$ se, e somente se, $a = 0$ ou $b = 0$.

$(M6)$ Comutatividade da multiplicação: Dados $a, b \in A$ quaisquer, temos que $a.b = b.a$.

Exemplo 1

Em $(\mathbb{Z}, +, \cdot)$ temos $e_1 = 1$ e para todos $a, b \in \mathbb{Z}$ temos que $a.b = 0$ se, e somente se, $a = 0$ ou $b = 0$, então também é um anel de integridade.

Exemplo 2

O anel $\mathbb{Z}_6$ não é de integridade, pois $\overline{2}$ e $\overline{3}$ são elementos não nulos, mas $\overline{2}.\overline{3} = \overline{6} = \overline{0}$.

Exemplo 3

O anel $\mathbb{Z} \times \mathbb{Z}$ não é de integridade, pois $(1,0)$ e $(0,1)$ são elementos não nulos de $\mathbb{Z} \times \mathbb{Z}$ porém o produto resulta no elemento neutro do anel.

2.7 Corpo

Definição:

Um corpo é um conjunto não vazio F , munido das operações indicadas por + e . onde são satisfeitas as seguintes propriedades:

$(A1)$ Comutatividade da soma: Dados $a, b \in A$, então $a + b = b + a$.

$(A2)$ Associatividade da soma: Dados $a, b, c \in A$, então $(a + b) + c = a + (b + c)$.

$(A3)$ Elemento Neutro da soma: Seja $e \in A$ tal que $a + e = e + a = a$.

Nota: o elemento neutro $e = 0$ para adição.

$(A4)$ Elemento simétrico da soma: Para qualquer $a \in A$ existe um elemento $a' \in A$ tal que $a + a' = a' + a = e$.

Nota: o elemento simétrico $a' = -a$ para a adição.

$(M1)$ Associatividade da multiplicação: Dados $a, b, c \in A$, então $(a.b).c = a(b.c)$.

$(M2)$ Distributividade da multiplicação (direita e esquerda): Dados $a, b, c \in A$, temos que

$a.(b + c) = a.b + a.c$ e $(b + c).a = b.a + c.a$.

$(M3)$ Comutatividade para multiplicação: Para qualquer $a, b \in A$ onde temos que $a.b = b.a$.

$(M4)$ Identidade multiplicativa: Existe $e_1 \in A$ tal que para qualquer $a \in A$ temos $a.e_1 = e_1.a = a$.

$(M5)$ Inverso multiplicativo: Para cada $a \in F - \{0\}$ existe um elemento $a' \in F$ tal que $a.a' = a'.a = e_1$.

Notas: Para a multiplicação, o elemento inverso $a' = a^{-1}$.

Pode-se mostrar facilmente que todo corpo é um anel de integridade. Enquanto que $(\mathbb{Z}, +, \cdot)$ não é um corpo, pois apesar de ser um anel de integridade, apenas os elementos 1 e -1 possuem inversos multiplicativos.

Proposição

Seja $(A, +, \cdot)$ um corpo, então, para qualquer $a, b \in A$, temos que $a.b = 0$ se, e somente se, $a = 0$ ou $b = 0$.

Demonstração:

Vamos supor que $a \neq 0$, assim, aplicando o inverso multiplicativo de a em ambos os lados e usando a propriedade associativa, temos

$$a^{-1}.(a.b) = a^{-1}.0 \Leftrightarrow (a^{-1}.a).b = 0 \Leftrightarrow e_1.b = 0 \Leftrightarrow b = 0.$$

O mesmo ocorre quando consideramos $b \neq 0$ e aplicamos o inverso multiplicativo em ambos os lados, juntamente com a propriedade associativa,

$$(a.b).b^{-1} = 0.b^{-1} \Leftrightarrow a.(b.b^{-1}) = 0 \Leftrightarrow a.e_1 = 0 \Leftrightarrow a = 0.$$

Observação: Segue da proposição anterior que todo corpo é um anel de integridade.

Exemplo 1

2.8 Os corpos numéricos

Pode-se verificar facilmente que $\mathbb{R}$ e $\mathbb{Q}$ são corpos relativos as operações usuais.

Exemplo 2

Vimos que o $\mathbb{Z}_6$ não é um anel de integridade, logo não pode ter estrutura de um corpo.

Por outro lado, pode-se ver facilmente que $(\mathbb{Z}_2, +, \cdot)$ é um corpo. Na verdade vale o seguinte resultado:

Proposição:

$\mathbb{Z}_n$ é um anel de integridade se, e somente se n é primo.

Demonstração:

A verificação é clássica e pode ser encontrada em [4] .

Exemplo 3

Em geral um subconjunto de matrizes não forma um corpo visto que pode possuir divisores do zero, e, portanto, não é anel de integridade. Por exemplo, as matrizes

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

são não nulas em $M_2(\mathbb{R})$, mas observemos que:

$$A.B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Na sequência deste trabalho, construímos um conjunto de matrizes que tem estrutura de um corpo relativo as operações usuais.

2.9Homomorfismo de anéis

Definição:

Dados dois anéis $(A, +, \cdot)$ e $(B, \oplus, \odot)$ e uma aplicação ψ tal que $\psi: A \longrightarrow B$. Dizemos que ψ é um homomorfismo se $\psi(a + b) = \psi(a) \oplus \psi(b)$ e $\psi(a.b) = \psi(a) \odot \psi(b)$ para quaisquer $a, b \in A$.

Exemplo 1

Sejam os anéis $(\mathbb{Z}, +, \cdot)$ e $(M_2(\mathbb{Z}), +, \cdot)$ e a aplicação $\psi: \mathbb{Z} \longrightarrow M_2(\mathbb{Z})$, definido por $\psi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, para todo $a \in \mathbb{Z}$. Vamos verificar se satisfaz as condições de homomorfismo.

Dados $a, b \in \mathbb{Z}$ quaisquer, então temos que:

$$\psi(a+b) = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \psi(a) + \psi(b).$$

$$\psi(a.b) = \begin{pmatrix} a.b & 0 \\ 0 & a.b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \psi(a).\psi(b).$$

Portanto, ψ é um homomorfismo.

2.10 Isomorfismo de anéis

Definição:

Dados dois anéis $(A, +, \cdot)$ e $(B, \oplus, \odot)$ e uma aplicação ψ tal que $\psi: A \longrightarrow B$. Se ψ for homomorfismo e for bijetora, então, dizemos que ψ é um isomorfismo entre A e B. Quando existe um isomorfismo entre A e B, dizemos que A e B são isomorfos.

Exemplo 1

Sejam os anéis $A = (\mathbb{R}, +, \cdot)$ e $B = (\mathbb{R}, \oplus, \odot)$, onde $+$ e $\cdot$ operações usuais e $x \oplus y = x + y + 1$ e $x \odot y = x + y + xy$, e a aplicação $\psi: A \longrightarrow B$ definida por $\psi(x) = x - 1$. Vamos verificar se A é isomorfo a B.

Primeiramente vamos verificar se ψ é homomorfismo:

$$\psi(a+b) = (a+b) - 1 = a + b - 1 = (a-1) + (b-1) + 1 = \psi(a) \oplus \psi(b)$$

$$\begin{aligned} \psi(a.b) = (a.b) - 1 &= a.b - 1 + a + b - a - b - 1 + 1 \\ &= (a-1) + (b-1) + (a.b - a - b + 1) \\ &= (a-1) + (b-1) + (a-1).(b-1) = \psi(a) \odot \psi(b). \end{aligned}$$

Portanto, ψ é homomorfismo.

Vamos analisar agora se ψ é bijetora:

Dado $y \in B = \mathbb{R}$ e considerando $x = y + 1 \in \mathbb{R}$, temos que $\psi(x) = x - 1 = (y+1) - 1 = y$, assim, ψ é sobrejetora.

Dados $x, y \in A = \mathbb{R}$ sendo $x \neq y$, logo $x - 1 \neq y - 1$ o que implica que $\psi(x) \neq \psi(y)$, portanto ψ é injetora.

Concluímos assim que ψ é bijetora, e consequentemente, isomorfismo.

3. Números Complexos

3.1 Definição e História dos Complexos

Definição:

Um número complexo é um número z que pode ser escrito na forma $z = a + bi$, sendo a e b números reais e i denota a unidade imaginária que satisfaz $i^2 = -1$,. Devido a esta condição a unidade imaginária é denotada por $\sqrt{-1}$. As componentes a e b são chamados de, respectivamente, parte real e parte imaginária de z.

René Descartes (1596-1650), em uma passagem do Discurso do Método, escreveu a seguinte frase: “Nem sempre as raízes verdadeiras (positivas) ou falsas (negativas) de uma equação são reais. Às vezes elas são **imaginárias**”. Por esse motivo, até hoje, o número $\sqrt{-1}$ é chamado de número imaginário, termo que se consagrou juntamente com a expressão “número complexo”. Anos depois, Leonhard Euler, dentre as inúmeras contribuições matemáticas, propôs substituir $\sqrt{-1}$ por i, onde usamos essa simbologia até os dias atuais. O conjunto dos complexos foi denotado pelo símbolo $\mathbb{C}$.

3.2 Operações Elementares

Sejam $z = a + bi$ e $w = c + di$ sendo $z, w \in \mathbb{C}$, então definiremos as relações e operações elementares da seguinte maneira:

Identidade

Dizemos que dois números complexos, z e w quaisquer, são iguais se, e somente se, $a = c$ e $b = d$.

Soma

Definimos a soma entre dois números complexos da seguinte maneira:

$$z + w = (a + bi) + (c + di) = a + bi + c + di = a + c + bi + di = (a + c) + (b + d)i.$$

Produto

O produto entre dois números complexos é definida da seguinte maneira:

$$z.w = (a + bi)(c + di) = ac + adi + bci + bdi^2.$$

Por definição, $i^2 = -1$, substituindo, temos:

$$z.w = ac + adi + bci + bd(-1) = ac - bd + adi + bci = (ac - bd) + (ad + bc)i.$$

Inverso multiplicativo (para z* $\neq$ 0*)

O inverso multiplicativo de um número z qualquer pode ser expresso como $\frac{1}{z}$, desta forma

$$\frac{1}{z} = \frac{1}{a + bi} = \frac{1}{a + bi} . \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2}.$$

Assim, $\frac{1}{z} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$, ou seja, o inverso de z também é um elemento de $\mathbb{C}$.

3.1 O Corpo $\mathbb{C}$

Vamos analisar agora se $\mathbb{C}$ satisfaz as condições de um corpo para as operações $+$ e $\cdot$ Para as verificações, usaremos $z, w, x \in \mathbb{C}$, sendo $z = a + bi$, $w = c + di$ e $x = e + fi$

$(A1)$ Comutatividade da soma:

$$z + w = (a + c) + (b + d)i = (c + a) + (d + b)i = w + z.$$

$(A2)$ Associatividade da soma:

$$\begin{aligned}(z + w) + x &= [(a + c) + (b + d)i] + x = [(a + c) + e] + [(b + d) + f]i \\ &= [a + (c + e)] + [b + (d + f)i] = z + [(c + e) + (d + f)i] = z + (w + x).\end{aligned}$$

$(A3)$ Elemento Neutro da soma:

Temos que o elemento neutro é da forma

$$e = 0 + 0i$$

pois,

$$z + e = (a + 0) + (b + 0)i = a + bi = z.$$

$(A4)$ Elemento simétrico da soma:

O elemento simétrico de um número z qualquer é dado por $-z = -a - bi$, pois

$$z + (-z) = (a - a) + (b - b)i = 0 + 0i = e.$$

$(M1)$ Associatividade da multiplicação:

$$\begin{aligned}(z.w).x &= [(ac - bd) + (ad + bc)i].x \\ &= [(ac - bd)e - (ad + bc)f] + [(ac - bd)f + (ad + bc)e]i \\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i \\ &= [a(ce - df) - b(de + cf)] + [b(ce - df) + a(cf + de)]i \\ &= z.[(ce - df) + (de + cf)i] = z.(w.x).\end{aligned}$$

$(M2)$ Distributividade da multiplicação (direita e esquerda):

Vamos fazer primeiramente a multiplicação pela esquerda:

$$\begin{aligned}z.(w + x) &= z.[(c + e) + (d + f)i] = [a(c + e) - b(d + f)] + [a(d + f) + b(c + e)]i \\ &= ac + ae - bd - bf + adi + afi + bci + bei \\ &= [(ac - bd) + (ad + bc)i] + [(ae - bf) + (af + be)i] = zw + zx.\end{aligned}$$

Fazendo agora a multiplicação pela direita, temos

$$\begin{aligned}(w + x).z &= [(c + e) + (d + f)i].z = [(c + e)a - (d + f)b] + [(c + e)b + (d + f)a]i \\ &= ca + ea - db - fb + cbi + ebi + dai + fai \\ &= [(ca - db) + (cb + da)i] + [(ea - fb) + (eb + fa)i] = wz + xz.\end{aligned}$$

$(M3)$ Comutatividade para multiplicação:

$$z.w = (ac - bd) + (ad + bc)i = (ca - db) + (cb + da)i = w.z.$$

$(M4)$ Identidade multiplicativa:

Basta tomarmos $e_1 = 1 = 1 + 0i$, pois, para qualquer $z \in \mathbb{C}$ temos que

$$w.e_1 = (a.1 - b.0) + (a.0 + 1.b)i = a + bi = w.$$

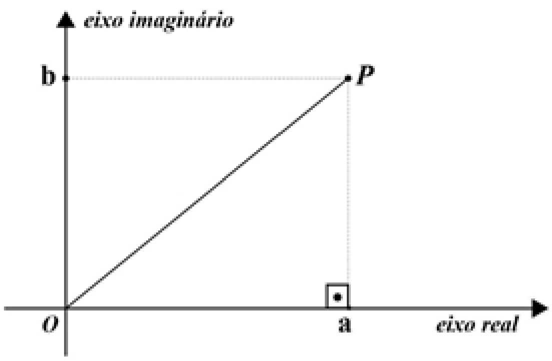
$(M5)$ Inverso multiplicativo:

A existência do inverso multiplicativo já foi mostrada no item anterior.

Portanto, verificamos que $(\mathbb{C}, +, \cdot)$ é um corpo.

3.2Plano Complexo

O plano complexo, também chamado de Plano de Argand-Gauss ou Diagrama de Argand, é obtido com a associação do número complexo $z = a + bi$ ao par ordenado (a,b), ou seja, o eixo das abcissas representa a parte real e o eixo das ordenadas representam a parte imaginária. O ponto $P = (a,b)$ é chamado de imagem ou afixo de z.



Conjugado

Definimos o conjugado de z como

$$\bar{z} = a - bi.$$

Observação

O conjugado de um número complexo é seu simétrico no plano complexo em relação ao eixo real.

Proposição

A soma ou o produto de um número complexo com seu conjugado tem a parte imaginária nula.

Demonstração.

Soma de um complexo por seu conjugado

$$z + \bar{z} = (a + bi) + (a - bi) = (a + a) + (b - b)i = 2a.$$

Produto de um complexo por seu conjugado

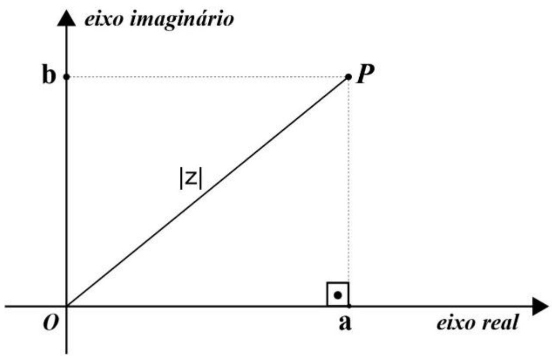
$$z.\bar{z} = (a + bi).(a - bi) = [a.a - b.(-b)] + (-ab + ab)i = a^2 + b^2.$$

Módulo

O módulo de um número complexo é a distância entre o afixo de $z = a + bi$ até a origem do sistema de coordenadas. Representamos o módulo de z como $|z|$, sendo calculado da seguinte maneira

$$|z| = \sqrt{a^2 + b^2}$$

podendo ser facilmente deduzida aplicando o teorema de Pitágoras, pois analisando a sua forma cartesiana, conseguirmos observar a formação de um triângulo retângulo sendo os catetos a e b e a hipotenusa $|z|$.



Podemos também representar o quadrado do módulo de um número complexo como o produto entre o seu conjugado e com ele mesmo, ou seja,

$$|z|^2 = z.\bar{z}.$$

Essa relação pode ser obtida de forma direta em relação a propriedade de multiplicação pelo conjugado visto no item anterior.

Usando a definição de módulo, podemos verificar que o inverso multiplicativo pode ser também representado por

$$\frac{1}{z} = \frac{a - bi}{a^2 + b^2} = \frac{a - bi}{\left(\sqrt{a^2 + b^2}\right)^2} = \frac{\bar{z}}{|z|^2}\,.$$

O módulo possui as seguintes propriedades, para todos z ,w • $\mathbb{C}$

i) $|\bar{z}| = |z|$.

Demonstração:

$$|\bar{z}| = |a - bi| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = |a + bi| = |z|.$$

ii) $|z.w| = |z|.|w|$.

Demonstração:

$$|z.w| = |(a + bi).(c + di)| = |a + bi|.|c + di| = |z|.|w|.$$

iii) $|z + w| \leq |z| + |w|$ (Desigualdade Triangular).

Demonstração:

Do fato que $z \leq |z|$ e $w \leq |w|$ para qualquer z e w, então temos que

$$-|z| \leq z \leq |z| \text{ e } -|w| \leq w \leq |w|.$$

Logo,

$$-|z| - |w| \leq z + w \leq |z| + |w|.$$

Portanto, pela definição de módulos, temos que

$$|z + w| \leq |z| + |w|.$$

iv) $|z| = 0$ se, e somente se, $z = 0$.

Demonstração:

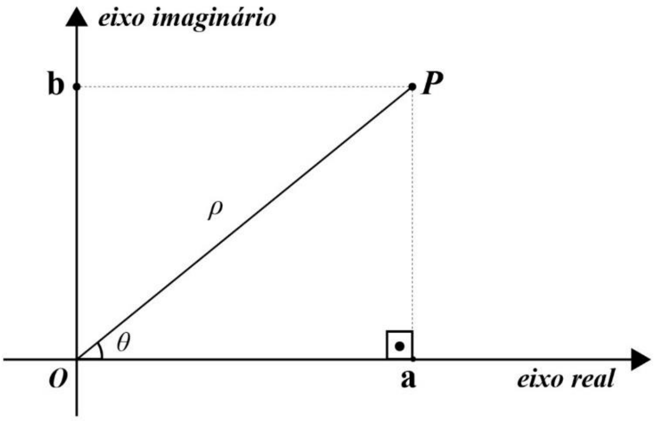
$$|z| = 0 \Leftrightarrow \sqrt{a + bi} = 0 \Leftrightarrow a + bi = 0 \Leftrightarrow z = 0.$$

3.3Formas Polares

Para o estudo das formas polares, vamos considerar o número complexo $z = a + bi$ não nulo. Analisando o plano complexo, ilustrado pelo gráfico abaixo, podemos verificar que o ponto formado pela parte real de z, a origem e o afixo formam um triângulo retângulo. Vamos chamar de θ o ângulo $a\hat{O}P$ e de ρ o valor do módulo de z, daí valem as seguintes propriedades trigonométricas:

$$\operatorname{sen}\theta = \frac{c.o}{hip} = \frac{b}{\rho} \Rightarrow b = \rho.\operatorname{sen}\theta.$$

$$\cos\theta = \frac{c.a}{hip} = \frac{a}{\rho} \Rightarrow a = \rho.\cos\theta.$$



Substituindo os valores obtidos de a e b, podemos reescrever o número complexo da seguinte forma

$$z = \rho.\cos\theta + \rho.\operatorname{sen}\theta\,.\,i = \rho(\cos\theta + i\operatorname{sen}\theta).$$

A representação geométrica no gráfico polar é representada pelo eixo horizontal, chamado de eixo polar, e um ponto fixo chamado polo de referência (ou origem). Assim, o número complexo z é representada por um vetor polar P, cuja coordenada é (ρ, θ), distando ρ do polo de referência e formando um ângulo θ com o eixo polar. Temos a relação entre dois polos, por isso à chamada de relação polar.

Nos estudos de formas polares é tomado o seguinte padrão:

- Para ângulos positivos, tomamos o sentido anti-horário o segmento em relação ao eixo polar;
- Para ângulos negativos, tomamos o sentido horário o segmento em relação ao eixo polar.

Exemplo 1

Vamos colocar o número $z = \sqrt{3} + 3i$ na forma polar.

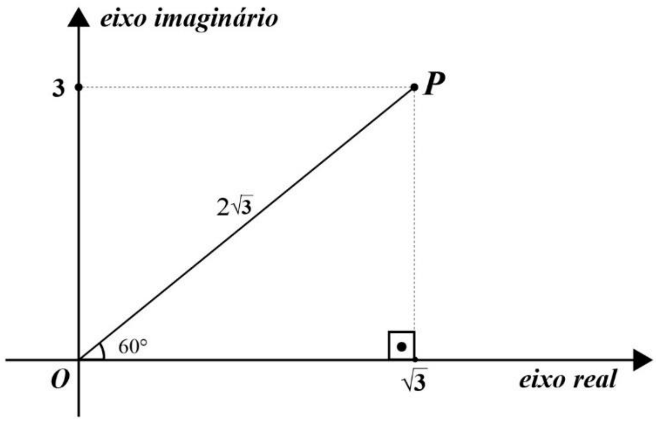
Primeiramente, vamos calcular ρ.

$$\rho = |z| = \sqrt{\left(\sqrt{3}\right)^2 + 3^2} = \sqrt{3+9} = \sqrt{12} = 2\sqrt{3}.$$

Agora, através das relações métricas definidas acima, temos

$$\operatorname{sen}\theta = \frac{b}{\rho} = \frac{3}{2\sqrt{3}} = \frac{3}{2\sqrt{3}} \cdot \frac{\sqrt{3}}{\sqrt{3}} = \frac{3\sqrt{3}}{2.3} = \frac{\sqrt{3}}{2} \Leftrightarrow \theta = \frac{\pi}{3}.$$

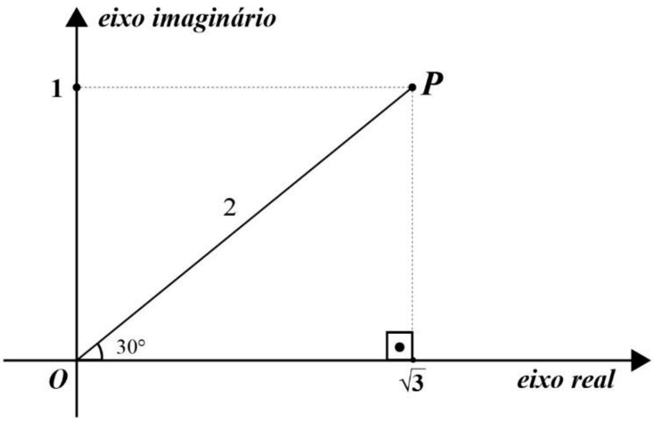
Portanto, o ponto representado por z é o vetor polar $P\left(2\sqrt{3}, \frac{\pi}{3}\right)$.



Exemplo 2

Faremos agora o caso contrário, escrever o ponto $P\left(2, \frac{\pi}{6}\right)$ da forma polar para a forma geral. Usando as propriedades descritas acima, temos

$$z = \rho(\cos\theta + \operatorname{sen}\theta\, i) = 2\left(\cos\frac{\pi}{6} + \operatorname{sen}\frac{\pi}{6} i\right) = 2\left(\frac{\sqrt{3}}{2} + \frac{1}{2} i\right) = \sqrt{3} + i.$$



3.4 Operações com formas polares dos complexos

Vamos definir agora as operações de multiplicação e divisão para os números em formas polares. Para as demonstrações a seguir vamos realizar as operações entre os vetores polares $P_1\ (\rho_1, \theta_1)$ e $P_2(\rho_2, \theta_2)$ sendo representado por, respectivamente, z,$w \in \mathbb{C}$ da forma $z = a + bi$ e $w = c + di$.

Multiplicação

Sabemos que $z.w = (ac - bd) + (ad + bc)i$ e segundo as relações trigonométricas já calculadas no tópico anterior, podemos facilmente concluir que

$$z.w = (\rho_1 \cos\theta_1\, \rho_2 \cos\theta_2 - \rho_1 \operatorname{sen}\theta_1\, \rho_2 \operatorname{sen}\theta_2) + (\rho_1 \cos\theta_1\, \rho_2 \operatorname{sen}\theta_2 + \rho_1 \operatorname{sen}\theta_1\, \rho_2 \cos\theta_2)i$$
$$= \rho_1\rho_2(\cos\theta_1 \cos\theta_2 - \operatorname{sen}\theta_1 \operatorname{sen}\theta_2) + \rho_1\rho_2(\operatorname{sen}\theta_2 \cos\theta_1 + \operatorname{sen}\theta_1 \cos\theta_2)i.$$

Pelas propriedades das somas de arcos, temos que

$$z.w = \rho_1\rho_2 \cos(\theta_1 + \theta_2) + \rho_1\rho_2 \operatorname{sen}(\theta_1 + \theta_2)\, i = \rho_1\rho_2(\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)).$$

Concluímos então que

$$P_1(\rho_1, \theta_1). P_2(\rho_2, \theta_2) = P(\rho_1\rho_2, \theta_1 + \theta_2).$$

Divisão

Vamos considerar o caso

$$\frac{z}{w}=\frac{a+bi}{c+di}\cdot\frac{c-di}{c-di}=\frac{ac-adi+bci+ad}{c^2+d^2}=\frac{ac+ad}{c^2+d^2}+\frac{(bc-ad)i}{c^2+d^2}\cdot$$

Segundo as relações trigonométricas, temos

$$\begin{aligned}\frac{z}{w}&=\frac{\rho_1\cos\theta_1\,\rho_2\cos\theta_2+\rho_1\operatorname{sen}\theta_1\,\rho_2\operatorname{sen}\theta_2}{(\rho_2\cos\theta_2)^2+(\rho_2\operatorname{sen}\theta_2)^2}+\frac{(\rho_1\operatorname{sen}\theta_1\,\rho_2\cos\theta_2-\rho_1\cos\theta_1\,\rho_2\operatorname{sen}\theta_2)i}{(\rho_2\cos\theta_2)^2+(\rho_2\operatorname{sen}\theta_2)^2}\\&=\frac{\rho_1\rho_2(\cos\theta_1\cos\theta_2+\operatorname{sen}\theta_1\operatorname{sen}\theta_2)+\rho_1\rho_2(\operatorname{sen}\theta_2\cos\theta_1-\operatorname{sen}\theta_1\cos\theta_2)i}{\rho_2^2(\cos^2\theta_2+\operatorname{sen}^2\theta_2)}\\&=\frac{\rho_1\rho_2}{\rho_2^2}(\cos(\theta_1-\theta_2)+i\operatorname{sen}(\theta_1-\theta_2))\\&=\frac{\rho_1}{\rho_2}(\cos(\theta_1-\theta_2)+i\operatorname{sen}(\theta_1-\theta_2)).\end{aligned}$$

Concluímos assim que

$$\frac{P_1(\rho_1,\theta_1)}{P_2(\rho_2,\theta_2)}=P\left(\frac{\rho_1}{\rho_2},\theta_1-\theta_2\right).$$

Exemplo 1

Vamos considerar $z=i$, assim, podemos verificar que sua forma polar seria representada pelo ponto $P(1{,}90°)$.

Calculando z^2, temos

$$P^2=(1{,}90°).(1{,}90°)=(1.1{,}90°+90°)=(1{,}180°).$$

Como o ponto $(1{,}180°)$ representa o número -1, ou seja, $z^2=i^2=-1$.

Exemplo 2

Vamos mostrar usando as propriedades de operações polares que $z^0=1$ para qualquer $z\in\mathbb{C}$.

Sabemos que

$$z^0=z^{1-1}=\frac{z^1}{z^1}=\frac{z}{z}\cdot$$

Escrevendo z em sua forma polar, temos que existe $\rho\in\mathbb{R}^+$ e $0\le\theta\le 2\pi$ tais que

$$z=\rho(\cos\theta+i\operatorname{sen}\theta).$$

logo, usando a propriedade de divisão de números complexos em forma polar

$$z^0 = \frac{\rho(\cos\theta + i\,\text{sen}\,\theta)}{\rho(\cos\theta + i\,\text{sen}\,\theta)} = \frac{\rho}{\rho}(\cos(\theta-\theta) + i\,\text{sen}(\theta-\theta)) = 1(\cos 0 + i\,\text{sen}\,0) = 1(1) = 1.$$

Provamos assim que $z^0 = 1$ para qualquer que seja $z \in \mathbb{C}$.

3.5 Identificação de $\mathbb{C}$ como um conjunto de matrizes

Nesta seção vamos obter uma representação de $\mathbb{C}$ como conjunto de matrizes. Onde todo número complexo poderá ser identificado a uma matriz. Inclusive poderemos identificar as unidades real e imaginária como matrizes deste conjunto.

Iniciemos observando que matrizes, de uma forma geral, para a operação de multiplicação não são comutativas. Por exemplo, dadas as matrizes $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, temos

$$A.B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

enquanto que

$$B.A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

mostrando que $A.B \neq B.A$.

Por outro lado, a não comutatividade não é um padrão, porque considerando por exemplo $A = \begin{pmatrix} 2 & 3 \\ -3 & 2 \end{pmatrix}$ e $B = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$, temos que:

$$A.B = \begin{pmatrix} 2 & 3 \\ -3 & 2 \end{pmatrix} . \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -4 & 7 \\ -7 & -4 \end{pmatrix}$$

e

$$B.A = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} . \begin{pmatrix} 2 & 3 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} -4 & 7 \\ -7 & -4 \end{pmatrix}$$

ou seja $A.B = B.A$.

Vamos definir uma forma geral para que duas matrizes em $M_2(\mathbb{R})$ sejam comutativas. Consideremos $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, temos

$$A.B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

e

$$B.A = \begin{pmatrix} e & f \\ g & h \end{pmatrix} . \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ae + cf & be + df \\ ag + ch & bg + dh \end{pmatrix}.$$

Assim, para ser comutativas, deveremos ter que $A.B = B.A$, logo

$$\begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} = \begin{pmatrix} ae + cf & be + df \\ ag + ch & bg + dh \end{pmatrix}.$$

Portanto, temos que

$$\begin{cases} ae + bg = ae + cf \Leftrightarrow bg = cf & (1) \\ af + bh = be + df \Leftrightarrow f(a - d) = b(e - h) & (2) \\ ce + dg = ag + ch \Leftrightarrow -g(a - d) = -c(e - h) & (3) \\ cf + dh = bg + dh \Leftrightarrow cf = bg & (4) \end{cases}$$

Se subtrairmos a equação (3) da equação (2) teremos

$$f(a - d) + g(a - d) = b(e - h) + c(e - h) \Leftrightarrow (f + g)(a - d) = (b + c)(e - h).$$

Assim, podemos ver que uma solução particular seria tomarmos

$$\begin{cases} a = d \\ b = -c \\ e = h \\ f = -g \end{cases}$$

Concluindo assim que $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ e $B = \begin{pmatrix} e & f \\ -f & g \end{pmatrix}$. Vamos fazer o teste agora:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} . \begin{pmatrix} e & f \\ -f & e \end{pmatrix} = \begin{pmatrix} ae - bf & af + be \\ -be - af & ae - bf \end{pmatrix}$$

e

$$\begin{pmatrix} e & f \\ -f & e \end{pmatrix} . \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ae - bf & af + be \\ -be - af & ae - bf \end{pmatrix}.$$

Algo notório é que o produto tem a mesma forma que seus fatores, ou seja os elementos da diagonal principal são iguais e os da diagonal segundaria são opostos , de fato

$$\begin{pmatrix} ae-bf & af+be \\ -be-af & ae-bf \end{pmatrix} = \begin{pmatrix} ae-bf & af+be \\ -(af+be) & ae-bf \end{pmatrix}.$$

De forma análoga, podemos verificar que o mesmo acontece para adição

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ -b-f & a+e \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ -(b+f) & a+e \end{pmatrix}.$$

Constatamos que ao fazer as operações de adição e multiplicação para duas matrizes dessa forma, seus resultados são de mesmas características, assim, conseguimos determinar um conjunto $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$ onde é fechado para a adição e multiplicação, além de ser um conjunto comutativo também para as duas operações. Com bastante características semelhantes a uma estrutura de corpo, vamos verificar se todas as condições são satisfeitas.

Para quaisquer elementos $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ e $\begin{pmatrix} e & f \\ -f & e \end{pmatrix}$ de M temos,

$(A1)$ Comutatividade da soma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} c+a & d+b \\ -d-b & c+a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

$(A2)$ Associatividade da soma

$$\begin{aligned} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix} \right) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c+e & d+f \\ -d-f & c+e \end{pmatrix} \\ &= \begin{pmatrix} a+(c+e) & b+(d+f) \\ -b+(-d-f) & a+(c+e) \end{pmatrix} = \begin{pmatrix} (a+c)+e & (b+d)+f \\ (-b-d)-f & (a+c)+e \end{pmatrix} \\ &= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix} = \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) + \begin{pmatrix} e & f \\ -f & e \end{pmatrix}. \end{aligned}$$

$(A3)$ Elemento neutro da soma.

Basta tomarmos $a = b = 0$, assim, a matriz $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ é elemento neutro desse conjunto.

$(A4)$ Elemento simétrico da soma.

Como $-a$ é o simétrico de a, e $-b$ é o simétrico de b, então a matriz simétrica de $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ será a matriz $\begin{pmatrix} -a & -b \\ b & -a \end{pmatrix}$.

$(M1)$ Associatividade da multiplicação.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \cdot \begin{pmatrix} e & f \\ -f & e \end{pmatrix} \right) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} ce - df & cf + de \\ -de - cf & ce - df \end{pmatrix}$$

$$= \begin{pmatrix} ace - adf - bde - bcf & acf + ade + bce - bdf \\ -bce + bdf - ade - acf & ace - adf - bde - bcf \end{pmatrix}$$

$$= \begin{pmatrix} (ac - bd)e - (ad + bc)f & (ac - bd)f + (ad + bc)e \\ (-ad - bc)e - (ac - bd)f & (-ad - bc)f + (ac - bd)e \end{pmatrix}$$

$$= \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix} \cdot \begin{pmatrix} e & f \\ -f & e \end{pmatrix} = \left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \right) \cdot \begin{pmatrix} e & f \\ -f & e \end{pmatrix}.$$

$(M2)$ Distributividade da multiplicação.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} e & f \\ -f & e \end{pmatrix} \right) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c + e & d + f \\ -d - f & c + e \end{pmatrix}$$

$$= \begin{pmatrix} a(c + e) + b(-d - f) & a(d + f) + b(c + e) \\ -b(c + e) + a(-d - f) & -b(d + f) + a(c + e) \end{pmatrix}$$

$$= \begin{pmatrix} ac + ae - bd - bf & ad + af + bc + be \\ -ad - af - bc - be & ac + ae - bd - bf \end{pmatrix}$$

$$= \begin{pmatrix} (ac - bd) + (ae - bf) & (ad + bc) + (af + be) \\ (-bc - ad) + (-be - af) & (-bd + ac) + (-bf + ae) \end{pmatrix}$$

$$= \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix} + \begin{pmatrix} ae - bf & af + be \\ -be - af & -bf + ae \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} + \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} e & f \\ -f & e \end{pmatrix}.$$

$(M3)$ Comutatividade para multiplicação.

Esta propriedade já foi demonstrada.

$(M4)$ Identidade multiplicativa.

Sabemos que a matriz identidade é o elemento neutro das matrizes para a multiplicação, e como $I_d \in M$, então existe matriz o elemento identidade multiplicativo.

$(M5)$ Inverso multiplicativo.

Para verificar a existência do inverso primeiro é necessário que o determinante da matriz não seja nulo, assim, dado um elemento $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M$, temos que:

$$detA = \begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 - (-b^2) = a^2 + b^2.$$

Portanto, temos que o determinante de uma matriz pertencente ao conjunto M só será nulo se for uma matriz nula. Assim, todas as matrizes, exceto a matriz nula, possuem inverso multiplicativo.

Vamos calcular a matriz inversa da matriz $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, onde iremos representa-la por $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} . \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Leftrightarrow \begin{pmatrix} ae + bg & af + bh \\ -be + ag & -bf + ah \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Logo,

$$\begin{cases} ae + bg = 1 \ \ (1) \\ ag - be = 0 \ \ (2) \\ af + bh = 0 \ \ (3) \\ ah - bf = 1 \ \ (4) \end{cases}$$

Como $A \neq 0$ então a e b não podem ser nulos simultaneamente, ou seja, se $a = 0$ então $b \neq 0$, ou vice e versa. Podemos ter o caso ainda dos dois não serem nulos, porem para a demonstração vamos considerar $a \neq 0$, então temos de (2) que

$$g = \frac{b}{a} e.$$

Substituindo em (1) temos que

$$ae + b\left(\frac{b}{a} e\right) = 1 \Leftrightarrow a^2 e + b^2 e = a \Leftrightarrow c(a^2 + b^2) = a \Leftrightarrow e = \frac{a}{a^2 + b^2} \cdot$$

Assim, substituindo o valor de e em g teremos

$$g = \frac{b}{a}\left(\frac{a}{a^2 + b^2}\right) = \frac{b}{a^2 + b^2} \cdot$$

Fazendo agora, o mesmo processo em (3), teremos que

$$f = -\frac{b}{a}h.$$

Substituindo em (4) teremos

$$ah - b\left(-\frac{b}{a}h\right) = 1 \Leftrightarrow a^2h + b^2h = a \Leftrightarrow h(a^2 + b^2) = a \Leftrightarrow h = \frac{a}{a^2 + b^2}.$$

Vamos substituir agora o valor de h em f, logo

$$f = -\frac{b}{a}\left(\frac{a}{a^2 + b^2}\right) = -\frac{b}{a^2 + b^2}.$$

Concluímos que a matriz inversa de A é a matriz

$$\begin{pmatrix} \frac{a}{a^2 + b^2} & -\frac{b}{a^2 + b^2} \\ \frac{b}{a^2 + b^2} & \frac{a}{a^2 + b^2} \end{pmatrix}.$$

Portanto, temos que o conjunto $(M, +, .)$ é um corpo.

Em relação aos elementos que compõem o conjunto M, ainda podemos fazer a seguinte observação:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Enquanto temos a matriz identidade $I_d = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, temos a matriz $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ que a denotaremos por I.

Observemos que

$$I^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -I_d.$$

Podemos encontrar então um comportamento semelhante entre os elementos dos corpos M e $\mathbb{C}$. Na álgebra abstrata esta constatação é feita estabelecendo-se um isomorfismo entre estes dois conjuntos. A determinação de uma $f\colon \mathbb{C} \longrightarrow M$ com esta propriedade é bastante natural, de fato para $a + bi$ arbitrário de $\mathbb{C}$, definamos $f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Vamos verificar se essa associação é um isomorfismo, ou seja, um homomorfismo bijetor.

Dados $z, w \in \mathbb{C}$ sendo $z = a + bi$ e $w = c + di$, temos

$$f(z+w) = f\big((a+c)+(b+d)i\big) = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
$$= f(a+bi) + f(c+di) = f(z) + f(w).$$

$$f(z.w) = f\big((ac-bd)+(ad+bc)i\big) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
$$= f(a+bi) + f(c+di) = f(z) + f(w).$$

Portanto a relação é um homomorfismo, basta verificar agora se é bijetora.

Seja $z \neq w$, então temos que $a \neq c$ ou $b \neq d$, assim, em qualquer um dos casos temos que

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \Leftrightarrow f(z) \neq f(w).$$

Da mesma forma, dado $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M$ qualquer, se considerarmos $z = a + bi \in \mathbb{C}$ temos $f(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, portanto é uma relação injetora e sobrejetora e assim, bijetora.

Logo, podemos concluir que M e $\mathbb{C}$ são isomorfos.

3.6 Fórmula de De Moivre

A conhecida "fórmula de De Moivre" permite simplificações nos cálculos operacionais com números complexos na forma polar. A "fórmula de De Moivre" permite ainda o calculo de raízes de números complexos.

Proposição:

Dado $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta) \in \mathbb{C}$, então para qualquer $n \in \mathbb{Q}$ vale a seguinte igualdade

$$z^n = \rho^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta))$$

Demonstração:

Como $z \in \mathbb{C}$, escrevendo em sua forma polar temos que $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$, com $\rho \in \mathbb{R}^+$ e $0 \leq \theta \leq 2\pi$.

Como $n \in \mathbb{Q}$, então existem $m, p \in \mathbb{Z}$, com $p \neq 0$, tais que $n = \frac{m}{p}$. Para essa demonstração primeiramente vamos considerar $p = 1$ e $m \geq 0$. Para isto vamos utilizar o método de indução para fazer a demonstração que é válido para qualquer $m \geq 0$. Assim, para $n = 0$ temos:

$$z^0 = \rho^0(\cos(0.\theta) + i\,\mathrm{sen}(0.\theta)) = 1(\cos 0 + i\,\mathrm{sen}\, 0) = 1.(1 + 0) = 1$$

O que é válido pois, $z^0 = 1$ para qualquer $z \in \mathbb{C}$. Vamos considerar agora que essa relação é válida para m, ou seja,

$$z^m = \rho^m(\cos(m\theta) + i\,\mathrm{sen}(m\theta))$$

e mostraremos a validade para $m + 1$. Temos

$$z^{m+1} = z^m.z = [\rho^m(\cos(m\theta) + i\,\mathrm{sen}(m\theta))].[\rho(\cos\theta + i\,\mathrm{sen}\,\theta)].$$

Pela propriedade de multiplicação de números complexos em forma polar, temos que

$$z^{m+1} = \rho^{m+1}\big(\cos\big((m+1)\theta\big) + i\,\mathrm{sen}\big((m+1)\theta\big)\big).$$

Provamos assim que vale para qualquer $m \geq 0$. Consideraremos agora a ideia de $m < 0$, onde podemos definir

$$z^m = \frac{1}{z^{-m}}.$$

Como $-m > 0$, então podemos afirmar que

$$z^{-m} = \rho^{-m}(\cos(-m\theta) + i\,\mathrm{sen}(-m\theta))$$

e podemos também considerar

$$1 = 1 + 0i = 1(\cos 0 + i \sin 0).$$

Temos então que

$$z^m = \frac{1(\cos 0 + i \sin 0)}{\rho^{-m}(\cos(-m\theta) + i\,\mathrm{sen}(-m\theta))}.$$

Pela propriedade de divisão de complexos em forma polar, temos que

$$z^m = \frac{1}{\rho^{-m}}\big(\cos\big(0-(-m\theta)\big) + i\,\mathrm{sen}\big(0-(-m\theta)\big)\big) = \rho^m(\cos(m\theta) + i\,\mathrm{sen}(m\theta))$$

provando assim que essa propriedade á válida para qualquer $m \in \mathbb{Z}$.

Vamos considerar agora $p \neq 1$, assim, temos

$$z^{\frac{m}{p}} = \left(z^{\frac{1}{p}}\right)^m$$

como já provamos que é válido para z^m, basta provarmos se vale também para $z^{\frac{1}{p}}$ para qualquer $p \in \mathbb{Z}$.

Iremos fazer a seguinte consideração para os próximos cálculos

$$z^{\frac{1}{p}} = z_w.$$

Como z e z_w são números complexos, então os escreveremos em sua forma polar, assim, para $p_w \in \mathbb{R}^+$ e $0 \leq \theta_w \leq 2\pi$, teremos

$$z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta) \qquad (1)$$
$$z_w = \rho_w(\cos\theta_w + i\,\mathrm{sen}\,\theta_w) \quad (2)$$

Sabemos que

$$z_w^p = \left(z^{\frac{1}{p}}\right)^p = z^{\frac{p}{p}} = z^1 = z \qquad (3)$$

assim, como já provado anteriormente para potências de complexos na forma polar, temos através de (2) que

$$z_w^p = \rho_w^p(\cos(p\theta_w) + i\,\mathrm{sen}(p\theta_w))\ (4).$$

Substituindo (1) e (4) em (3) temos

$$\rho(\cos\theta + i\,\mathrm{sen}\,\theta) = \rho_w^p(\cos(p\theta_w) + i\,\mathrm{sen}(p\theta_w)).$$

Assim, pela igualdade de números complexos temos que

$$\rho = \rho_w^p \Leftrightarrow p_w = \rho^{\frac{1}{p}}$$
$$\cos\theta = \cos(p\theta_w)$$
$$\sin\theta = \sin(p\theta_w)$$

E portanto,

$$z^{\frac{1}{p}} = w = \rho^{\frac{1}{p}}(\cos\left(\frac{1}{p}\theta\right) + i\,\mathrm{sen}\left(\frac{1}{p}\theta\right).$$

Assim, teremos

$$z^n = z^{\frac{m}{p}} = \left(z^{\frac{1}{p}}\right)^m = \left[\rho^{\frac{1}{p}}\left(\cos\left(\frac{1}{p}\theta\right) + i\,\mathrm{sen}\left(\frac{1}{p}\theta\right)\right)\right]^m = \rho^{\frac{m}{p}}\left(\cos\left(\frac{m}{p}\theta\right) + i\,\mathrm{sen}\left(\frac{m}{p}\theta\right)\right)$$
$$= \rho^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta)).$$

o que completa a validade da "fórmula de De Moivre" para qualquer $n \in \mathbb{Q}$.

4. Adjunção de Raízes

4.1 Introdução

Consideremos a equação abaixo, cujos coeficientes são claramente números racionais

$$x^2 - 2 = 0.$$

No entanto em $\mathbb{Q}$ esta equação não admite as soluções conhecidas que são $x = \sqrt{2}$ ou $x = -\sqrt{2}$, ou seja, a equação dada é completamente "resolúvel" no corpo dos números reais $\mathbb{R}$ e não em $\mathbb{Q}$. Uma pergunta interessante seria questionar sobre a existência de um "corpo menor" que $\mathbb{R}$, onde a equação fosse completamente "resolúvel".

Estas questões fazem parte de uma teoria algébrica mais profunda, a chamada "Teoria de Galois", cuja abordagem inclui o "corpo de decomposição de um polinômio", que consiste no menor corpo K, onde um determinado polinômio f , de grau n, pode ser fatorado como produto de fatores lineares, ou seja $f(x) = (x-a_1).(x-a_2)...(x-a_n)$, onde $a_1, a_2, ..., a_n$ são elementos de K.

Em uma tentativa de construção do corpo de decomposição K do polinômio $f(x) = x^2 - 2$ a partir do corpo base $\mathbb{Q}$, vamos anexar o elemento que falta: $\sqrt{2}$. Logo K deve incluir também $-\sqrt{2}$, pois uma das características de um corpo é a existência do inverso para a soma, temos também que, pelo fechamento da multiplicação, deve incluir também os múltiplos de $\sqrt{2}$, logo, para qualquer $b \in \mathbb{Q}$, temos que $b\sqrt{2} \in K$. Pelo fechamento, a soma de tais elementos com um racional a também deve pertencer a K, ou seja, $a + b\sqrt{2} \in K$, para todos $a, b \in \mathbb{Q}$. Em relação ao produto, temos fechamento de tais elementos, porque para $a, b, c, d \in \mathbb{Q}$ arbitrários temos

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = ac + 2bd + (ad + bc)\sqrt{2}.$$

Com efeito, pode-se justificar que realmente $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ é o menor corpo onde a equação é resolvível. Devido aos objetivos deste trabalho, vamos nos contentar apenas com a obtenção intuitiva que descrevemos acima e também a verificação de que este conjunto é um corpo, conforme apresentamos a seguir.

4.2 - O corpo $\mathbb{Q}[\sqrt{2}]$

Nesta seção provaremos que $\mathbb{Q}[\sqrt{2}]$ é um corpo, para tanto consideraremos, elementos arbitrários $x, y \in \mathbb{Q}[\sqrt{2}]$, sendo $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ com $a, c, b, d \in \mathbb{Q}$.

Temos que:

$$x + y = a + b\sqrt{2} + c + d\sqrt{2} = (a + c) + (b + d)\sqrt{2} \text{ e}$$

$$x \cdot y = (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Como $ac + 2bd$ e $ad + bc$ são números racionais, então $\mathbb{Q}[\sqrt{2}]$ é um conjunto fechado para as operações usuais.

Uma vez que associatividade da soma, associatividade da multiplicação, distributividade da multiplicação e comutatividade para multiplicação vale para $\mathbb{R}$, estas propriedades também são válidas para $\mathbb{Q}[\sqrt{2}]$. Vamos verificar as demais propriedades de um Corpo.

$(A3)$ Elemento Neutro da Soma

O elemento $0 + 0\sqrt{2}$ é neutro para a soma, pois

$$0 + 0\sqrt{2} + a + b\sqrt{2} = (0 + a) + (0 + b)\sqrt{2} = a + b\sqrt{2}$$

$(A4)$ Elemento simétrico da soma:

O elemento $-a - b\sqrt{2}$ é simétrico de $a + b\sqrt{2}$, pois

$$-a - b\sqrt{2} + a + b\sqrt{2} = (-a + a) + (-b + b)\sqrt{2} = 0 + 0\sqrt{2}$$

$(M4)$ Identidade multiplicativa.

O elemento $1 = 1 + 0\sqrt{2}$ é a identidade multiplicativa, pois

$$(1 + 0\sqrt{2}) \cdot (a + b\sqrt{2}) = a + b\sqrt{2} + 0\sqrt{2} + 0 = a + b\sqrt{2}$$

$(M5)$ Inverso multiplicativo.

Observemos inicialmente que

$x = 0$ œ $a + b\sqrt{2} = 0 \qquad a = -b\sqrt{2}$

E como $\sqrt{2}$ • $\mathbb{Q}$, a igualdade acima só é possível se $a = b = 0$. Pela mesma justificativa $a - b\sqrt{2} = 0$ apenas se $a = b = 0$. Assim, tomando $a \neq 0$ e $b \neq 0$, podemos validar os cálculos do inverso de *x* abaixo

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Assim, o inverso multiplicativo de $a + b\sqrt{2}$ é o elemento $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ que também é pertencente ao conjunto $\mathbb{Q}[\sqrt{2}]$.

Concluímos assim que o conjunto $\mathbb{Q}[\sqrt{2}]$ possui todas as propriedades de um corpo.

4.3 Adjunção de mais raízes

O processo de adjunção de mais raízes pode não seguir uma maneira tão natural quanto descrevemos no item anterior, no caso de uma raiz. Consideremos, por exemplo, o caso da adjunção de $\sqrt{2}$ e $\sqrt{3}$ ao corpo $\mathbb{Q}$. A notação padrão para o corpo nesta adjunção é $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Seguindo a construção que elaboramos é natural esperar que este conjunto seja dado por

$$\{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}.$$

Porém, este conjunto não se sustenta algebricamente. Observemos que, dados $x = a + b\sqrt{2} + c\sqrt{3}$ e $y = d + e\sqrt{2} + f\sqrt{3}$, temos:

$$\begin{aligned} x \cdot y &= (a + b\sqrt{2} + c\sqrt{3}) \cdot (d + e\sqrt{2} + f\sqrt{3}) \\ &= ad + ae\sqrt{2} + af\sqrt{3} + bd\sqrt{2} + 2be + bf\sqrt{6} + cd\sqrt{3} + ce\sqrt{6} + 3cf \\ &= (ad + 2be + 3cf) + (ae + bd)\sqrt{2} + (af + bf)\sqrt{3} + (bf + ce)\sqrt{6} \end{aligned}$$

e como $\sqrt{6}$ não pertence ao nosso conjunto, ele não é fechado para a multiplicação.

Por outro lado se considerarmos para $\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]$ o conjunto dos elementos da forma $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ onde a,b,c,d • $\mathbb{Q}$,temos para dois elementos arbitrários $x=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ e $y=e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6}$, que:

$$
\begin{aligned}
x+y &= a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}+e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6}\\
&= (a+e)+(b+f)\sqrt{2}+(c+g)\sqrt{3}+(d+h)\sqrt{6}.
\end{aligned}
$$

$$
\begin{aligned}
x\cdot y &= \left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right)\cdot\left(e+f\sqrt{2}+g\sqrt{3}+h\sqrt{6}\right)\\
&= ae+af\sqrt{2}+ag\sqrt{3}+ah\sqrt{6}+be\sqrt{2}+2bf+bg\sqrt{6}+bh\sqrt{12}+ce\sqrt{3}\\
&\quad +cf\sqrt{6}+3cg+ch\sqrt{18}+de\sqrt{6}+df\sqrt{12}+dg\sqrt{18}+6dh\\
&= ae+af\sqrt{2}+ag\sqrt{3}+ah\sqrt{6}+be\sqrt{2}+2bf+bg\sqrt{6}+2bh\sqrt{3}+ce\sqrt{3}\\
&\quad +cf\sqrt{6}+3cg+3ch\sqrt{2}+de\sqrt{6}+2df\sqrt{3}+3dg\sqrt{2}+6dh\\
&= (ae+2bf+3cg+6dh)+(af+be+3ch+3dg)\sqrt{2}\\
&\quad +(ag+2bh+ce+2df)\sqrt{3}+(ah+bg+cf+de)\sqrt{6}.
\end{aligned}
$$

Portanto é um conjunto fechado para as operações usuais.

Na verdade, é valido que $\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]=\mathbb{Q}\left[\sqrt{2}\right]\left[\sqrt{3}\right]$, ou seja ao corpo $\mathbb{Q}\left[\sqrt{2}\right]$ foi ajuntado a raiz $\sqrt{3}$. Assim,

$$\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]=\left\{a+b\sqrt{3,}\ \mid a\,,b\in\ \mathbb{Q}\left[\sqrt{2}\right]\right\}$$

e como a e b na definição do conjunto acima são elementos da forma $x+y\sqrt{2}$, pode-se constatar realmente que $\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\ \mid a,b,c\,,d\quad \mathbb{Q}\,\right\}$.

4.4 O corpo $\mathbb{C}$ *como uma adjunção de* $\mathbb{R}$

Nesta seção utilizamos a ideia desenvolvida acima para obter uma representação dos números complexos através da adjunção da raiz de um polinômio com coeficientes reais.

O polinômio $P(x)=x^2+1$ não pode ser decomposto em fatores lineares sobre o corpo $\mathbb{R}$ porque suas raízes não são reais. Tal como o exemplo trabalhado acima, o corpo de decomposição de $P(x)$ é $\mathbb{R}\left[\sqrt{-1}\right]=\left\{a+b\sqrt{-1}\ \middle|\ a,b\in\mathbb{R}\right\}$. Podemos observar que essa adjunção gera o conjunto $\mathbb{C}$, dado que a identificação $i = \sqrt{-1}$ acarreta $i^2 = -1$. Logo, $\mathbb{C}$ $=\mathbb{R}[i]$.

Observemos que $P(x)$ também pode ser visto como um polinômio de coeficientes em $\mathbb{Q}$. Logo podemos construir o corpo de decomposição, considerando $\mathbb{Q}$ como corpo base, o que dá origem ao corpo $\mathbb{Q}[i]$ de todos os números complexos com partes real e imaginaria racionais.

5. *Quatérnios*

5.1 História

Historicamente a ideia inicial da criação dos quatérnios era generalizar os números complexos em três dimensões. Hamilton considerou a seguinte expressão $a + bi + cj$ com a, b, c números reais e $i^2 = j^2 = -1$.

Para mostrar que é um conjunto fechado para a soma, não se teve dificuldades, pois:

$$(a + bi + cj) + (a' + b'i + c'j) = (a + a') + (b + b')i + (c + c')j.$$

Como a, a', b, b', c e c' são números reais e os reais são fechados para a soma, então podemos facilmente concluir que a soma de dois números complexos de três dimensões será fechada.

O problema encontrado por Hamilton foi para a multiplicação, pois, ao multiplicar dois números quaisquer complexos de três dimensões, teríamos o seguinte número:

$$\begin{aligned} &(a + bi + cj).(a' + b'i + c'j) \\ &= a.a' + ab'i + ac'j + a'bi + bb'i^2 + bc'ij + a'cj + b'cij + cc'j^2 \\ &= (a.a' - bb' - cc') + (ab' + a'b)i + (ac' + a'c)j + (bc' + b'c)ij. \end{aligned}$$

Em um caso particular, teríamos que o quadrado de um número seria expresso da seguinte maneira:

$$(a^2 - b^2 - c^2) + 2abi + 2acj + 2bcij.$$

Destaca-se então a inconsistência deste produto haja vista o aparecimento do termo *ij* não presente na expressão proposta para os quatérnios. Uma saída seria incorporar o termo *ij* na expressão de um quatérnio, o que porem não vinha de encontro a proposta de Hamilton, conforme descrevemos a seguir.

Hamilton em seus estudos tinha comprovado a seguinte propriedade: “o produto do módulo de dois números complexos resulta ser o módulo do produto destes números”, o que ele chamou de Lei dos Módulos.

A verificação desta propriedade não é difícil como apresentamos a seguir:

Sejam dois números complexos $z = a + bi$ e $w = c + di$. Queremos provar que $|z|.|w| = |z.w|$.

$$|z|.|w| = \sqrt{a^2+b^2}.\sqrt{c^2+d^2} = \sqrt{(a^2+b^2).(c^2+d^2)} = \sqrt{a^2c^2+a^2d^2+b^2c^2+b^2d^2}$$
$$= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2}$$
$$= \sqrt{(ac)^2 - 2(ac)(bd) + (bd)^2 + (ad)^2 + 2(ad)(bc) + (bc)^2}$$
$$= \sqrt{(ac-bd)^2 + (ad+bc)^2} = |(ac-bd) + (ad+bc)i|$$
$$= |ac + adi + bci + bdi^2| = |a(c+di) + bi(c+di)| = |\ (a+bi)(c+di)|$$
$$= |z.w|.$$

Em um caso particular podemos afirmar que $|z^2| = |z|^2$.

Hamilton desejando expandir esta ideia para os “complexos’ de três dimensões assim procedeu

$$|(a+bi+cj)^2| = |(a^2-b^2-c^2) + 2abi + 2acj + 2bcij| \ \ (*)$$
$$= \sqrt{(a^2-b^2-c^2)^2 + (2ab)^2 + (2ac)^2 + (2bc)^2}$$
$$= \sqrt{a^4 - a^2b^2 - a^2c^2 - a^2b^2 + b^4 + b^2c^2 - a^2c^2 + b^2c^2 + c^4 + 4a^2b^2 + 4a^2c^2 + 4b^2c^2}$$
$$= \sqrt{a^4 + 2a^2b^2 + b^4 + 6b^2c^2 + 2a^2c^2 + c^4}$$

e, por outro lado

$$|a+bi+cj|^2 = \left(\sqrt{a^2+b^2+c^2}\right)^2 = a^2+b^2+c^2.$$

Logo, teríamos a seguinte igualdade:

$$\sqrt{a^4 + 2a^2b^2 + b^4 + 6b^2c^2 + 2a^2c^2 + c^4} = a^2+b^2+c^2 \Leftrightarrow$$

$$a^4 + 2a^2b^2 + b^4 + 6b^2c^2 + 2a^2c^2 + c^4 = (a^2+b^2+c^2)^2 \Leftrightarrow$$

$$a^4 + 2a^2b^2 + b^4 + 6b^2c^2 + 2a^2c^2 + c^4 = a^4 + 2a^2b^2 + 2a^2c^2 + 2b^2c^2 + b^4 + c^4 \Leftrightarrow$$

$$a^4 - a^4 + 2a^2b^2 - 2a^2b^2 + b^4 - b^4 + 6b^2c^2 - 2b^2c^2 + 2a^2c^2 - 2a^2c^2 + c^4 - c^4 = 0$$

$4b^2c^2 = 0 \Leftrightarrow (bc)^2 = 0 \Leftrightarrow bc = 0 \Leftrightarrow b = 0$ ou $c = 0$.

Como em qualquer um dos casos voltaríamos a ter apenas duas dimensões, uma condição para que essa igualdade seja verdadeira seria considerar $ij = 0$. Porém Hamilton não considerava essa condição correta conforme [5].

"Às vezes, tenho sido tentado a considerar ij = 0. Mas eu acho
estranho e desconfortável, e percebi que a mesma exclusão do termo
desejado, poderia ser obtido assumindo algo que parecia menos violento,
isto é, ji = -ij. Desta forma eu considerei que ij = k, ji = -k,
reservando a consideração de se k era nulo ou não."

Esse procedimento de Hamilton surgiu em reconsiderar o cálculo $(*)$ na qual foi assumido a comutatividade $ij = ji$. Não valendo a comutatividade, $(*)$ torna-se

$$\begin{aligned} |(a+bi+cj)^2| &= |(a^2-b^2-c^2)+2abi+2acj+bcij+bcji| \\ &= |(a^2-b^2-c^2)+2abi+2acj+bc(ij+ji)|. \end{aligned}$$

Por esta razão ele considerou $ij = -ji$, caso em que suprimiria o termo $bc(ij+ji)$, observe que isto evitaria a necessidade de que ij ou ji fossem nulos.

Assim, foi denominado que $ij = -ji = k$ para resolver o produto de dois números complexos de três dimensões.

$$\begin{aligned} (a+bi+cj).(x+yi+zj) &= ax+ayi+azj+bxi+byi^2+bzij+cxj+cyji+czj^2 \\ &= (ax-by-cz)+(ay+bx)i+(az+cx)j+bzk-cyka \\ &= (ax-by-cz)+(ay+bx)i+(az+cx)j+(bz-cy)k. \end{aligned}$$

Mas como não estava ainda claro a necessidade da quarta dimensão Hamilton considerou $k = 0$. Ainda resta verificar se é satisfeita a lei dos módulos para o produto de dois elementos arbitrários. Temos,

$$\begin{aligned} |(a+bi+cj)|.|(x+yi+zj)| &= \sqrt{a^2+b^2+c^2}.\sqrt{x^2+y^2+z^2} \\ &= \sqrt{a^2x^2+a^2y^2+a^2z^2+b^2x^2+b^2y^2+b^2z^2+c^2x^2+c^2y^2+c^2z^2} \end{aligned}$$

e por outro lado, o módulo do produto torna-se

$$|(ax-by-cz)+(ay+bx)i+(az+cx)j| = \sqrt{(ax-by-cz)^2+(ay+bx)^2+(az+cx)^2}$$

$$= \sqrt{a^2x^2-2abyx-2acxz+b^2y^2+2bcyz+c^2z^2+a^2y^2+2abxy+b^2x^2+a^2z^2+2acxz+c^2x^2}$$

$$= \sqrt{a^2x^2+b^2y^2+c^2z^2+a^2y^2+b^2x^2+a^2z^2+c^2x^2+2bcyz}.$$

Assim, para satisfazer a lei dos módulos temos que ter a seguinte igualdade:

$$\sqrt{a^2x^2+a^2y^2+a^2z^2+b^2x^2+b^2y^2+b^2z^2+c^2x^2+c^2y^2+c^2z^2}$$

$$= \sqrt{a^2x^2+b^2y^2+c^2z^2+a^2y^2+b^2x^2+a^2z^2+c^2x^2+2bcyz}$$

$$\Leftrightarrow a^2x^2+a^2y^2+a^2z^2+b^2x^2+b^2y^2+b^2z^2+c^2x^2+c^2y^2+c^2z^2$$

$$= a^2x^2+b^2y^2+c^2z^2+a^2y^2+b^2x^2+a^2z^2+c^2x^2+2bcyz$$

$$\Leftrightarrow a^2x^2-a^2x^2+a^2y^2-a^2y^2+a^2z^2-a^2z^2+b^2x^2-b^2x^2+b^2y^2$$

$$-b^2y^2+b^2z^2+c^2x^2-c^2x^2+c^2y^2+c^2z^2-c^2z^2-2bcyz=0$$

$$\Leftrightarrow b^2z^2+c^2y^2-2bcyz=0 \Leftrightarrow (bz)^2-2(bz)(cy)+(cy)^2=0$$

$$\Leftrightarrow (bz-cy)^2=0 \Leftrightarrow bz-cy=0 \Leftrightarrow bz=cy.$$

Assim, podemos analisar que a igualdade não pode ser satisfeita por qualquer número, o que é contra a lei dos módulos, que afirma que a igualdade sempre será verdadeira, para quaisquer números. Em um dos passos na resolução dessa igualdade, chegamos a igualdade de $(bz-cy)^2=0$, onde é justamente o coeficiente de k no produto onde consideramos $k=0$, ou seja, considerar k nulo não foi o suficiente.

Por praticamente dez anos Hamilton ficou nesse impasse, pois se considera $k \neq 0$ o produto gera uma outra dimensão, e se considera $k=0$ não satisfaz a lei dos módulos.

No entanto, algo surpreendente aconteceu durante um passei com sua esposa pela ponte Royal Canal, em Dublin, em 16 de outubro de 1843, cuja qual hoje é chamada de “Quaternion Bridge”. Hamilton percebeu que todos os seus problemas poderiam ser facilmente resolvidos simplesmente considerando uma dimensão a mais, ou seja, usar quatro dimensões e não três como ele estava tentando. Hamilton escreve uma carta para um de seus filhos, quinze anos depois, contando o acontecimento do fato.

"Amanhã será o décimo quinto aniversário dos quatérnios. Eles surgiram
em 16 de outubro de 1843, quando eles vieram à vida, ou luz, já cresceu
Eu estava andando com a Sra. Hamilton para Dublin, e chegamos a Broughman Bridge. Quer dizer, então, fechei o circuito galvânico
de pensamento e as faíscas que caíram foram as equações
fundamentos entre i, j, k; exatamente como eu os usei desde então.
Eu tirei, naquele momento, um caderno de bolso, que ainda existe, e
Fiz uma anotação sobre a qual, naquele exato momento, senti
que seria valioso estender meu trabalho por pelo menos dez (ou
Pode ser daqui a quinze anos. É justo dizer que isso aconteceu porque

Eu senti, naquele momento, que um problema havia sido resolvido, um desejo intelectual aliviado, eu gostaria de ter seguido pelo menos quinze
anos anteriores. Eu não pude resistir ao impulso de pegar minha faca e queimar
uma pedra da ponte de Brougham a fórmula fundamental com os símbolos
i, j, k:

$$i^2 = j^2 = k^2 = ijk = -1$$

que continha a solução para o problema, que desde então tem sobrevivido como uma inscrição."

Atualmente, do outro lado da ponte está uma placa comemorativa da grande descoberta e com a definição dos quatérnios.

"aqui, enquanto caminhava no dia 16 de outubro de 1843, o senhor William Rowan Hamilton, num lampejo de genialidade, descobriu a fórmula fundamental para a multiplicação de quaterniões e cortou uma pedra desta ponte."

Hamilton denominou esta nova expressão como quatérnios, sendo números hipercomplexos com a forma de $a + bi + cj + dk$, onde a, b, c e d são números reais e i, j e k são as partes imaginárias que satisfazem as seguintes relações $i^2 = j^2 = -1$ e $k = ij = -ji$, sendo assim, podemos concluir que $k^2 = (ij)(ij) = (-ji).(ij) = -j.(i.i).j = -j.(-1).j = j.j = j^2 = -1$.

Temos que agora, falta apenas verificar se satisfaz a lei dos módulos. Pra isso, vamos calcular primeiramente o módulo do produto:

$$
\begin{aligned}
&|(a + bi + cj + dk).(x + yi + zj + wk)| \\
&\quad = |ax + ayi + azj + awk + bxi + byi^2 + bzij + bwik + cxj + cyji + czj^2 \\
&\quad + cwjk + dxk + dyki + dzkj + dwk^2| \\
&\quad = |ax + ayi + azj + awk + bxi - by + bzk + bwik + cxj - cyk - cz \\
&\quad + cwjk + dxk + dyki + dzkj - dw| \\
&\quad = |(ax - by - cz - dw) + (ay + bx)i + (az + cx)j \\
&\quad + (aw + dx + bz - cy)k + bwik + cwjk + dyki + dzkj|.
\end{aligned}
$$

Para continuar os cálculos precisamos saber os valores de ik e jk. Como Hamilton não tinha a certeza que a propriedade associativa era aplicada nos quatérnios, ele concluiu que:

"... provavelmente temos esse $ik = -j$, porque $ik = iij = i^2j = -j$ e i2 = -1; deste modo, podemos esperar encontrar que $kj = ijj = ij^2 = -i$. "

Pela propriedade associativa, poderíamos definir $ki = (-ji)i = -j(ii) = -j(-1) = j$. Porém Hamilton achou melhor usar a seguinte argumentação:

"... dela eu considerei que $ki = j$ e $jk = i$, porque parecia evidente que, se $ji = -ij$, devemos também ter que $kj = -jk$ e $ik = -ki$."

Resumindo as suposições de Hamilton, temos:

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

Assim, podemos concluir que

$|(ax - by - cz - dw) + (ay + bx)i + (az + cx)j + (aw + dx + bz - cy)k + bwik + cwjk +$
$dyki + dzkj| = |(ax - by - cz - dw) + (ay + bx + cw - dz)i + (az + cx + dy - bw)j +$
$(aw + dx + bz - cy)k| =$
$\sqrt{(ax - by - cz - dw)^2 + (ay + bx + cw - dz)^2 + (az + cx + dy - bw)^2 + (aw + dx + bz - cy)^2} =$
$\sqrt{(ax)^2 - 2axby - 2axcz - 2axdw + (by)^2 + 2bycz + 2bydw + (cz)^2 + 2czdw + (dw)^2 + (ay)^2}$
$\overline{+2aybx + 2aycw - 2aydz + (bx)^2 + 2bxcw - 2bxdz + (cw)^2 - 2cwdz + (dz)^2 + (az)^2 + 2azcx}$
$\overline{+2azdy - 2azbw + (cx)^2 + 2cxdy - 2cxbw + (dy)^2 - 2dybw + (bw)^2 + (aw)^2 + 2awdx + 2awbz}$
$\overline{-2awcy + (dx)^2 + 2dxbz - 2dxcy + (bz)^2 - 2bzcy + (cy)^2} =$
$\sqrt{(ax)^2 + (by)^2 + (cz)^2 + (dw)^2 + (ay)^2 + (bx)^2 + (cw)^2 + (dz)^2 + (az)^2 + (cx)^2 + (dy)^2 + (bw)^2}$
$\overline{+(aw)^2 + (dx)^2 + (bz)^2 + (cy)^2} =$
$\sqrt{a^2(x^2 + y^2 + z^2 + w^2) + b^2(x^2 + y^2 + z^2 + w^2) + c^2(x^2 + y^2 + z^2 + w^2) + d^2(x^2 + y^2 + z^2 + w^2)} =$
$\sqrt{(a^2 + b^2 + c^2 + d^2)(x^2 + b^2 + z^2 + w^2)} = |a + bi + cj + dk|.|x + yi + zj + wk|.$

Mostrando assim que os quatérnios satisfaz a lei dos módulos. O conjunto dos quatérnios foi denotado por $\mathbb{H}$, em homenagem a Hamilton.

5.2 Operações Básicas

Para as próximas demonstrações vamos usar q, p e $t \in \mathbb{H}$, onde $q = q_1 + q_2i + q_3j + q_4k$, $p = p_1 + p_2i + p_3j + p_4k$ e $t = t_1 + t_2i + t_3j + t_4k$ sendo $q_1, q_2, q_3, q_4, p_1, p_2, p_3, p_4, t_1, t_2, t_3$ e t_4 números reais e i, j e k números imaginários.

Identidade:

Temos que $p = q$ se, e somente se $p_1 = q_1, p_2 = q_2, p_3 = q_3$ e $p_4 = q_4$.

Adição:

A adição entre dois números quatérnios quaisquer é representado por

$$q + p = q_1 + q_2i + q_3j + q_4k + p_1 + p_2i + p_3j + p_4k$$
$$= (q_1 + p_1) + (q_2 + p_2)i + (q_3 + p_3)j + (q_4 + p_4)k.$$

Produto:

O produto entre dois elementos pertencentes aos quatérnios é feito da seguinte maneira

$q.p = (q_1 + q_2 i + q_3 j + q_4 k).(p_1 + p_2 i + p_3 j + p_4 k)$

$= q_1p_1 + q_1p_2 i + q_1p_3 j + q_1p_4 k + q_2p_1 i + q_2p_2 i^2 + q_2p_3 ij + q_2p_4 ik + q_3p_1 j + q_3p_2 ji + q_3p_3 j^2 + q_3p_4 jk + q_4p_1 k + q_4p_2 ki + q_4p_3 kj + q_4p_4 k^2.$

Usando as propriedades dos quatérnios

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

temos que

$q.p = q_1p_1 + q_1p_2 i + q_1p_3 j + q_1p_4 k + q_2p_1 i - q_2p_2 + q_2p_3 k - q_2p_4 j + q_3p_1 j - q_3p_2 k - q_3p_3 + q_3p_4 i + q_4p_1 k + q_4p_2 j - q_4p_3 i - q_4p_4 = (q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4) + (q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3)i + (q_1p_3 + q_3p_1 + q_4p_2 - q_2p_4)j + (q_1p_4 + q_4p_1 + q_2p_3 - q_3p_2)k.$

Conjugado dos quatérnios:

O conjugado de um número q qualquer é dado por

$$\bar{q} = q_1 - q_2 i - q_3 j - q_3 k.$$

Módulo dos quatérnios:

Assim como os complexos, o quadrado de seu módulo é igual ao produto entre o quatérnio e seu conjugado, temos então

$|q|^2 = q.\bar{q} = (q_1 + q_2 i + q_3 j + q_4 k).(q_1 - q_2 i - q_3 j - q_4 k) = (q_1^2 + q_2^2 + q_3^2 + q_4^2) + (-q_1q_2 + q_1q_2 - q_3q_4 + q_4q_3)i + (-q_1q_3 + q_3q_1 - q_4q_2 + q_2q_4)j + (-q_1q_4 + q_4q_1 - q_2q_3 + q_3q_2)k = q_1^2 + q_2^2 + q_3^2 + q_4^2$

ou ainda, podemos dizer que

$$|q| = \sqrt{q_1^2 + q_2^2 + q_3^2 + q_4^2}.$$

5.3 Estrutura algébrica dos quatérnios

Vamos verificar agora se os quatérnios satisfaz as condições para ser um anel.

$(A1)$ $q + p = (q_1 + p_1) + (q_2 + p_2)i + (q_3 + p_3)j + (q_4 + p_4)k = (p_1 + q_1) + (p_2 + q_2)i + (p_3 + q_3)j + (p_4 + q_4)k = p + q$.

$(A2)$ $(q + p) + t = [(q_1 + p_1) + (q_2 + p_2)i + (q_3 + p_3)j + (q_4 + p_4)k] + t_1 + t_2 i + t_3 j + t_4 k = [(q_1 + p_1) + t_1] + [(q_2 + p_2) + t_2]i + [(q_3 + p_3) + t_3]j + [(q_4 + p_4) + t_4]k = [q_1 + (p_1 + p_1)] + [q_2 + (p_2 + t_2)]i + [q_3 + (p_3 + t_3)]j + [q_4 + (p_4 + t_4)]k = q_1 + q_2 i + q_3 j + q_4 k + (p_1 + q_1) + (p_2 + t_2)i + (p_3 + t_3)j + (p_4 + t_4)k = q + (p + t)$.

$(A3)$ Como $q + 0 = (q_1 + 0) + (q_2 + 0)i + (q_3 + 0)j + (q_4 + 0)k = q_1 + q_2 i + q_3 j + q_4 k = q$, portanto $0 + 0i + 0j + 0k$ é um elemento neutro.

$(M1)$ Vamos verificar a associatividade:

$$
\begin{aligned}
(q.p).t &= [(q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4) + (q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3)i \\
&+ (q_1p_3 + q_3p_1 + q_4p_2 - q_2p_4)j + (q_1p_4 + q_4p_1 + q_2p_3 - q_3p_2)k].(t_1 + t_2i + t_3j \\
&+ t_4k) \\
&= [(q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4).t_1 - (q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3).t_2 \\
&- (q_1p_3 + q_3p_1 + q_4p_2 - q_2p_4).t_3 - (q_1p_4 + q_4p_1 + q_2p_3 - q_3p_2).t_4] \\
&+ [(q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4).t_2 + (q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3).t_1 \\
&+ (q_1p_3 + q_3p_1 + q_4p_2 - q_2p_4).t_4 - (q_1p_4 + q_4p_1 + q_2p_3 - q_3p_2).t_3]i \\
&+ [(q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4).t_3 + (q_1p_3 + q_3p_1 + q_4p_2 - q_2p_4).t_1 \\
&+ (q_1p_4 + q_4p_1 + q_2p_3 - q_3p_2).t_2 - (q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3).t_4]j \\
&+ [(q_1p_1 - q_2p_2 - q_3p_3 - q_4p_4).t_4 + (q_1p_4 + q_4p_1 + q_2p_3 - q_3p_2).t_1 \\
&+ (q_1p_2 + q_2p_1 + q_3p_4 - q_4p_3).t_3 - (q_1p_3 + q_3p_1 + q_4p_2 - q_2p_4).t_2]k \\
&= (q_1p_1t_1 - q_2p_2t_1 - q_3p_3t_1 - q_4p_4t_1 - q_1p_2t_2 - q_2p_1t_2 - q_3p_4t_2 + q_4p_3t_2 \\
&- q_1p_3t_3 - q_3p_1t_3 - q_4p_2t_3 + q_2p_4t_3 - q_1p_4t_4 - q_4p_1t_4 - q_2p_3t_4 + q_3p_2t_4) \\
&+ (q_1p_1t_2 - q_2p_2t_2 - q_3p_3t_2 - q_4p_4t_2 + q_1p_2t_1 + q_2p_1t_1 + q_3p_4t_1 - q_4p_3t_1 \\
&+ q_1p_3t_4 + q_3p_1t_4 + q_4p_2t_4 - q_2p_4t_4 - q_1p_4t_3 - q_4p_1t_3 - q_2p_3t_3 + q_3p_2t_3)i \\
&+ (q_1p_1t_3 - q_2p_2t_3 - q_3p_3t_3 - q_4p_4t_3 + q_1p_3t_1 + q_3p_1t_1 + q_4p_2t_1 - q_2p_4t_1 \\
&+ q_1p_4t_2 + q_4p_1t_2 + q_2p_3t_2 - q_3p_2t_2 - q1\,p_2t_4 - q_2p_1t_4 - q_3p_4t_4 + q_4p_3t_4)j \\
&+ (q_1p_1t_4 - q_2p_2t_4 - q_3p_3t_4 - q_4p_4t_4 + q_1p_4t_1 + q_4p_1t_1 + q_2p_3t_1 - q_3p_2t_1 \\
&+ q_1p_2t_3 + q_2p_1t_3 + q_3p_4t_3 - q_4p_3t_3 - q_1p_3t_2 - q_3p_1t_2 - q_4p_2t_2 + q_2p_4t_2)k \\
&= [q_1(p_1t_1 - p_2t_2 - p_3t_3 - p_4t_4) - q_2(p_1t_2 + p_2t_1 + p_3t_4 - p_4t_3) \\
&- q_3(p_1t_3 + p_3t_1 + p_4t_2 - p_2t_4) - q_4(p_1t_4 + p_4t_1 + p_2t_3 - p_3t_2)] \\
&+ [q_1(p_1t_2 + p_2t_1 + p_3t_4 - p_4t_3) + q_2(p_1t_1 - q_2t_2 - p_3t_3 - p_4t_4) \\
&+ q_3(p_1t_4 + p_4t_1 + p_2t_3p_3t_2) - q4\,(p_1t_3 + p_3t_1 + p_4t_2 - p_2t_4)]i \\
&+ [q_1(p_1t_3 + p_3t_1 + p_4t_3 - p_2t_4) + q_3(p_1t_1 - p_2t_2 - p_3t_3 - p_4t_4) \\
&+ q_4(p_1t_2 + p_2t_1 + p_3t_4 - p_4t_3) - q_2(p_1t_4 + p_4t_1 + p_2t_3 - p_3t_2)]j \\
&+ [q_1(p_1t_4 + p_4t_1 + p_2t_3 - p_3t_2) + q_4(p_1t_1 - p_2t_2 - p_3t_3 - p_4t_4) \\
&+ q_2(p_1t_3 + p_3t_1 + p_4t_2 - p_2t_4) - q_3(p_1t_2 + p_2t_1 + p_3t_4 - p_4t_3)]k \\
&= (q_1 + q_2i + q_3j + q_4k).[(p_1t_1 - p_2t_2 - p_3t_3 - p_4t_4) \\
&+ (p_1t_2 + p_2t_1 + p_3t_4 - p_4t_3)i + (p_1t_3 + p_3t_1 + p_4t_2 - p_2t_4)j \\
&+ (p_1t_4 + p_4t_1 + p_2t_3 - p_3t_2)k = q.[(p_1 + p_2i + p_3j + p_4k).(t_1 + t_2i + t_3j + t_4k)] \\
&= q.(p.t).
\end{aligned}
$$

$(A4)$ Como $q + (-q) = [q_1 + (-q_1)] + [q_2 + (-q_2)]i + [q_3 + (-q_3)]j + [q_4 + (-q_4)]k = 0 + 0i + 0j + 0k$ elemento neutro, então $-q$ é simétrico a q.

$(M2)$ $p.(q+t) = (p_1 + p_2 i + p_3 j + p_4 k).[(q_1 + t_1) + (q_2 + t_2)i + (q_3 + t_3)j + (q_4 + t_4)k] = p_1(q_1 + t_1) + p_1(q_2 + t_2)i + p_1(q_3 + t_3)j + p_1(q_4 + t_4)k + p_2(q_1 + t_1)i - p_2(q_2 + t_2) + p_2(q_3 + t_3)k - p_2(q_4 + t_4)j + p_3(q_1 + t_1)j - p_3(q_2 + t_2)k - p_3(q_3 + t_3) + p_3(q_4 + t_4)i + p_4(q_1 + t_1)k + p_4(q_2 + t_2)j - p_4(q_3 + t_3)i - p_4(q_4 + t_4) = p_1q_1 + p_1t_1 + p_1q_2 i + p_1t_2 i + p_1q_3 j + p_1t_3 j + p_1q_4 k + p_1t_4 k + p_2q_1 i + p_2t_1 i - p_2q_2 - p_2t_2 + p_2q_3 k + p_2t_3 k - p_2q_4 j - p_2t_4 j + p_3q_1 j + p_3t_1 j - p_3q_2 k - p_3t_2 k - p_3q_3 - p_3t_3 + p_3q_4 i + p_3t_4 i + p_4q_1 k + p_4t_1 k + p_4q_2 j + p_4t_2 j - p_4q_3 i - p_4t_3 i - p_4q_4 - p_4t_4 = [(p_1q_1 - p_2q_2 - p_3q_3 - p_4q_4) + (p_1q_2 + p_2q_1 + p_3q_4 - p_4q_3)i + (p_1q_3 + p_3q_1 + p_4q_2 - p_2q_4)j + (p_1q_4 + p_4q_1 + p_2q_3 - p_3q_2)k] + [(p_1t_1 - p_2t_2 - p_3t_3 - p_4t_4) + (p_1t_2 + p_2t_1 + p_3t_4 - p_4t_3)i + (p_1t_3 + p_3t_1 + p_4t_2 - p_2t_4)j + (p_1t_4 + p_4t_1 + p_2t_3 - p_3t_2)k] = pq + pt.$

Por outro lado, sabemos que não vale a propriedade comutativa em $\mathbb{H}$, pois $ij \neq ji$. Assim concluímos que $(\mathbb{H}, +, .)$ é um anel não abeliano.

5.4 Quatérnios em forma de matriz

Vamos mostrar agora que podemos criar uma representação dos quatérnios por um conjunto de matrizes

Consideremos

$$A = \left\{ \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}, a, b, c, d \in \mathbb{R} \right\},$$

vamos estabelecer um homomorfismo $\psi: \mathbb{H} \longrightarrow A$, onde

$$\psi(a + bi + cj + dk) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}.$$

De fato, dados $(a + bi + cj + dk), (x + yi + zj + wk) \in \mathbb{H}$ temos que:

$\psi[(a+bi+cj+dk)+(x+yi+zj+wk)] = \psi[(a+x)+(b+y)i+(c+z)j+$

$(d+w)k] = \begin{pmatrix} a+x & -(b+y) & -(c+z) & -(d+w) \\ b+y & a+x & -(d+w) & c+z \\ c+z & d+w & a+x & -(b+y) \\ d+w & -(c+z) & b+y & a+x \end{pmatrix} = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} +$

$\begin{pmatrix} x & -y & -z & -w \\ y & x & -w & z \\ z & w & x & -y \\ w & -z & y & x \end{pmatrix} = \psi(a+bi+cj+dw)+\psi(x+yi+zj+wk).$

$\psi[(a+bi+cj+dk).(x+yi+zj+wk)]$

$= \psi[(ax-by-cz-dw)+(ay+bx+cw-dz)i+(az+cx+dy-bw)j$

$+(aw+dx+bz-cy)k]$

$= \begin{pmatrix} ax-by-cz-dw & -(ay+bx+cw-dz) & -(az+cx+dy-bw) & -(aw+dx+bz-cy) \\ ay+bx+cw-dz & ax-by-cz-dw & -(aw+dx+bz-cy) & az+cx+dy-bw \\ az+cx+dy-bw & aw+dx+bz-cy & ax-by-cz-dw & -(ay+bx+cw-dz) \\ aw+dx+bz-cy & -(az+cx+dy-bw) & ay+bx+cw-dz & ax-by-cz-dw \end{pmatrix}$

$= \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} . \begin{pmatrix} x & -y & -z & -w \\ y & x & -w & z \\ z & w & x & -y \\ w & -z & y & x \end{pmatrix} = \psi(a+bi+cj+dk).\psi(x+yi+zj+wk).$

Portanto ψ é um homomorfismo.

Vamos analisar agora se ψ é bijetora. Dado um elemento arbitrário de A $\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$, consideramos $z = a+bi+cj+dk \in \mathbb{H}$, que , por definição, satisfaz

$$\psi(z) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

sendo assim ψ sobrejetora.

Agora sejam $(a+bi+cj+dk) \neq (x+yi+zj+wk)$ em $\mathbb{H}$, temos que

$\begin{cases} a \neq x \\ b \neq y \\ c \neq z \\ d \neq w \end{cases} \Leftrightarrow \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \neq \begin{pmatrix} x & -y & -z & -w \\ y & x & -w & z \\ z & w & x & -y \\ w & -z & y & x \end{pmatrix} \Leftrightarrow f(a+bi+cj+dk) \neq$

$f(x+yi+zj+wk).$

Portanto, ψ é biejtora, logo, $\mathbb{H}$ e A são isomorfos.

6. Conclusão

Acreditamos que este trabalho tenha cumprido seu objetivo de introduzir o conjunto dos quatérnios como uma generalização do conjunto dos números complexos e, desta forma, contribuir para a formação do professor de matemática. Embora introdutório a teoria foi construída com o aparato estrutural algébrico necessário e de forma intuitiva e gradual, procurando seguir, inclusive, a sequencia de ideias provavelmente desenvolvida por William Rowan Hamilton, seu criador.

Os números complexos foram utilizados como base principal para o desenvolvimento deste trabalho, sendo explorados aspectos importantes deste conjunto, como as formas polares e as fórmulas de De Moivre. Apresentamos duas representações interessantes de C, uma delas possibilita a visualização de um número complexo como um matriz 2x2, de possível utilização no ensino básico. E uma segunda que foi construída a partir do estudo introdutório de noções sobre extensões de corpos, que julgamos atingir os objetivos de complementação na formação do professor de matemática.

A teoria dos quatérnios possibilitou o desenvolvimento de várias aplicações. Inclusive trabalhos recentes mostram os quatérnios como alternativa de representação para movimentos de rotação (orientação) e os movimentos de translação (posição) através da utilização de sua álgebra implementada computacionalmente.

7. Referências

[1] ANDRADE, Lenimar N. *Introdução à Álgebra: Questões Comentadas e Resolvidas.* 1ª Edição. João Pessoa: Edição do Autor, 2014.

[2] BIASI, Sergio C.; GATTASS, Marcelo. **Utilização dos quatérnios para representação de rotações em 3d**. Disponível em: <http://webserver2.tecgraf.puc-rio.br/~mgattass/Quaternios.pdf> Acesso em: 10 de outubro de 2018.

[3] CERRI, Cristina; MONTEIRO, Martha S. *História dos Números Complexos*. Disponível em <https://www.ime.usp.br/~martha/caem/complexos.pdf > Acesso em: 10 de outubro de 2018.

[4] GARCIA, A.; LEQUAIN, Y. Elementos de Álgebra. 6ª ed. Rio de Janeiro: IMPA, 2013. 363 p.

[5] MUÑOZ, José M. S. *Hamilton y el Descubrimiento de los Cuaterniones*. Disponível em <http://www2.caminos.upm.es/Departamentos/matematicas/revistapm/revista_impresa/numero_1/hamilton_y_el_descubrimiento_de_los_cuaterniones.pdf> Acesso em 15 de outubro de 2018.

[6] SILVA, Marco A. *Grupos Finitos*. 2002. 73. Trabalho de Conclusão de Curso – Universidade Federal de Santa Catarina, Florianópolis, 2002.

[7] SILVA, Lúcio H. O. *Transformações Lineares e Isomorfismos: Um Exemplo em Criptografia*. 2009. 40. Trabalho de Conclusão de Curso – Universidade Federal de Santa Catarina, Imperatriz, 2009.

[8] NEVES, Robson C. *Os quatérnios de Hamilton e o Espaço.* 2008. 112. Dissertação de Mestrado – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2008.

[9] POLCINO, Francisco C. *Anel de Grupo*. Disponível em <https://www.ime.usp.br/~polcino/aneis_grupo/> Acesso em 10 de outubro de 2018.