UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
REDE NACIONAL - PROFMAT

MARCELO DE JESUS SANTOS

EXTENSÕES DO CONCEITO DE NÚMERO COM ÊNFASE NOS COMPLEXOS E QUATÉRNIOS

SÃO CRISTÓVÃO–SE
2015

MARCELO DE JESUS SANTOS

EXTENSÕES DO CONCEITO DE NÚMERO COM ÊNFASE NOS COMPLEXOS E QUATÉRNIOS

Dissertação apresentada ao Programa de Pós Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Zaqueu Alves Ramos

SÃO CRISTÓVÃO–SE
2015

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Santos, Marcelo de Jesus
S237e Extensões do conceito de número com ênfase nos complexos e quartérnios / Marcelo de Jesus Santos ; orientador Zaqueu Alves Ramos. – São Cristóvão, 2015.
68 f. : il.

Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Sergipe, 2015.

1. Teoria dos conjuntos. 2. Teoria dos números algébricos. 3. Quatérnios. l. Ramos, Zaqueu Alves, orient. II. Título.

CDU 511.11

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Extensões do Conceito de Número com ênfase nos Complexos e quatérnios.

por

Marcelo de Jesus Santos

Aprovada pela Banca Examinadora:

Prof. Dr. Zaqueu Alves Ramos- UFS
Orientador

Prof. Dr. Lucas Rezende Valeriano- UFS
Primeiro Examinador

Profª. Dra. Crislene Santos da Paixão - IFS
Segundo Examinador

São Cristóvão, 10 de Abril de 2015.

Agradecimentos

"Simplicidade é fruto de sabedoria".
Marcelo de Jesus Santos

A conclusão deste trabalho é um momento sublime, onde recordo o quão importantes foram os contribuintes deste feito. Dessa forma, os agradecimentos seguem humildemente, na confiança do não esquecimento.

Primeiramente agradeço a Deus, por toda força, direcionamento, sustentação e tudo o mais que me tem proporcionado.

À minha esposa Maria Helena, companheira e amiga, que partilhou comigo todas as alegrias e tristezas. Suportou todos os períodos em que ficamos distantes mesmo quando estávamos juntos. Obrigado pela paciência, apoio e carinho que me tem proporcionado. Por tudo que tem feito para fazer de nossos dias, os mais felizes de nossa história.

À minha filhinha Yanamara, que mesmo sem entender o que se passava durante esse período, sem saber o porquê da minha ausência, sorriu, brincou, me abraçou, me beijou, me puxou, deu seus primeiros passinhos distante de casa, riscou e rasgou meus livros, me chamou de papai pela primeira vez, enfim, me fez e me faz muito feliz. Te amo imensamente.

Ao meu orientador, Zaqueu Alves Ramos, mais que um orientador e professor, um amigo, uma referência profissional a todos os seus alunos. Obrigado por cada palavra de incentivo, pela atenção, por todos ensinamentos e contribuições dados no curso e a este trabalho.

Aos meus amigos Marcos, Roberto e Epifanio, que foram grandes amigos, companheiros, verdadeiros irmãos nos momentos felizes e difíceis em todo o curso.

Aos meus pais Joselito e Ana, grandiosos, gigantes, por todo o amor que me deram, por fazer de mim o que sou.

Aos meus irmãos André, Ana Paula, Maria Tereza e Maria Elizabete pelo carinho e apoio.

Aos meus vizinhos, que estiveram próximos a todo momento. Em especial ao meu amigo irmão Allan Rodrigues, pessoa simples, feliz, incomparável, culpado por eu ter ingressado nesse curso! Obrigado por tudo garoto.

Aos meus amigos irmãos Carlos Roberto e Carlos José, sempre presentes me incentivando, imensa é a participação de vocês em minha vida.

A todos os colegas que o mestrado me deu a honra de conhecer, pela amizade, troca de experiência e conhecimento, companheirismo, enfim, por tudo que passamos juntos.

Aos professores, Crislene Santos da Paixão e Lucas Rezende Valeriano por aceitarem o convite de participar da minha banca examinadora.

Aos professores Allyson, Almir Rogério, Danilo Dias, Danilo Felizardo, Débora Lopes, Evilson, Humberto Henrique, José Anderson, Kalasas, Leandro Favacho, Lucas Valeriano, Naldisson e Romero pela dedicação e empenho em compartilhar seus conhecimentos que contribuíram bastante para o nosso crescimento profissional.

À SBM (Sociedade Brasileira de Matemática), pela excelente iniciativa de promover um mestrado voltado para professores da educação básica.

À CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior), pela concessão da bolsa de estudos que foi de fundamental importância para o desenvolvimento deste mestrado profissionalizante.

A todos que direta ou indiretamente contribuíram para a elaboração deste trabalho e conclusão desse objetivo.

Resumo

A presente dissertação tem como objetivo mostrar a sistematização algébrica dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ como extensões que preservam propriedades aritméticas e algébricas. Apesar desse fato, veremos que esse campo de estudos não se limita por aí. Apresentaremos que após $\mathbb{C}$ existe a formalização dos quatérnios de Hamilton, também conhecidos como números hipercomplexos. Esses, assim como os demais conjuntos, são muito importantes para a matemática e o meio em que vivemos. Além disso buscamos abordar os números complexos em um dinâmica que possibilite observar sua importância de forma geral. Assim, este trabalho pretende aprofundar o estudo sobre o tema em questão, deixando margem para a necessidade do aperfeiçoamento profissional. Tornando perceptíveis formas diversificadas a serem desenvolvidadas no processo de ensino-aprendizagem que possibilitam um aprendizado diferenciado, que alicerçará o conhecimento discente para o futuro pessoal, social e acadêmico. No desenvolvimento desta dissertação iniciamos com o processo de sistematização dos números naturais aos reais. Consequentemente comentamos sobre o surgimento e formalização dos números complexos, onde em seguida expomos sua utilidade de forma global. Por fim, fechamos este trabalho com uma abordagem sobre os quatérnios de Hamilton, viajando em um campo matemático diferente, importante e que nos incentiva ir a fundo na pesquisa científica.

Palavras-chave: Conjuntos numéricos. Sistematização algébrica. Estrutura. Extensão.

Abstract

The present dissertation aims to show the algebraic systematization of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ as extensions that preserve arithmetic and algebraic properties. Despite this fact, we will see that this field studies is not limited there. We will present that after $\mathbb{C}$ there is a formalization of Hamilton's quaternions, also known as hypercomplex numbers. And these, like the other sets, are very important for mathematics and the environment we live in. Furthermore, we seek to approach the complex numbers in a dynamic that allows observe its importance in general. Therefore, this work intends to deepen the study on the subject in question leaving scope for the need for professional development. Making noticeable diversified forms to be developed in the teaching-learning process that enable a differentiated learning that will underpin the student knowledge for personal, social and academic future. In developing this dissertation, we started with the process of systematization of natural numbers to real. Consequently we commented on the emergence and formalization of complex numbers where then we exposed its usefulness in a global way. Lastly, we closed this work with an approach on Hamilton's quaternions, traveling in a different mathematical field, important and encouraging us go deep in scientific research.

Keywords: Numerical sets. Algebraic systematization. Structure. Extension.

Lista de Figuras

Sumário

Introdução

Profunda para quem se dedica a desenvolvê-la e estudá-la, a matemática oferece os mais diversos campos de estudos e aplicações. Em especial, a história dos números mostra-a claramente como uma ciência dinâmica, que foi sendo construída, transformada e aperfeiçoada pelo homem ao longo do tempo. Assim, na busca pela ampliação do conhecimento, ressaltamos a importância do constante aprimoramento profissional, uma vez que a pesquisa nos proporciona maiores condições de compreender e julgar as mais diversas relações que a matemática aborda.

É supreendente quando passamos a analizar a evolução de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ destacando a sistematização algébrica/axiomática. No tocante, percebemos a fragilidade nas abordagens que são dadas a esses conjuntos no ensino básico, já que quando são trabalhados, mencionam-se apenas as propriedades e suas operações em um conjunto numérico específico, em contexto meramente aritmético, sem a devida interligação sistemática de conjunto para conjunto. Nesse campo de estudo, é possível dar sentido ao processo, instigando o aluno a pesquisar e produzir um conhecimento formal que possibilite novas descobertas. Até onde essas estruturas ampliam suas partições mantendo as anteriores? Isso é contínuo ou não? Esses são alguns questionamentos que podem ser respondidos aprimorando o conhecimento e, entre outras coisas, minimizando a rejeição à disciplina.

O presente trabalho visa transmitir sutilmente que os conjuntos numéricos são sistemas que preservam axiomas e propriedades quando extendidos ($\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \supset \mathbb{Z} \supset \mathbb{N}$), o que estimulará a curiosidade de sabermos se esse processo de extensão sucessiva é continuado após $\mathbb{C}$. O que verificaremos é que em um certo sentido é possível, introduzindo os chamados números hipercomplexos. Mostraremos enfaticamente a importância dos números complexos para a matemática em consonância com o processo de ensino-aprendizagem e o mundo que nos cerca. Além disso buscaremos expor este trabalho apresentando alguns conflitos, divergências e discussões que proporcionaram a construção e reconstrução do conhecimento matemático sobre

os conjuntos numéricos historicamente. Vale salientar que não destacaremos aqui o conteúdo integral em questão, mas apontaremos situações relevantes que proporcionarão dar significados, numa nova perpectiva para o aprendizado.

Mediante o exposto, fracionamos o texto em três capítulos, os quais descreveremos brevemente a partir de então.

No capítulo 1 mostraremos a sistematização dos conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, os quais serão observados gradativamente no decorrer do trabalho a inclusão algébrica $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Faremos um ligeiro apanhado histórico desses conjuntos numéricos individualmente, mostrando pontos relevantes, além da estruturação algébrica. Verificaremos brevemente alguns fatos polêmicos, como o aperfeiçoamento e aceitação dos números negativos e irracionais.

No capítulo 2 daremos ênfase ao conjunto dos números complexos. Mostraremos como sua história nos reserva a beleza de um processo longo de discussões, divergências e tentativas na dinâmica de sistematização e aceitação desses números, até a formalização dada por Hamilton, onde veremos que $\mathbb{R}$ está imerso em $\mathbb{C}$. Apresentaremos a importância e utilidade dos números complexos para a ciência matemática, a sociedade em geral e o processo de ensino-aprendizagem numa abordagem de aplicações, expondo situações que almejam melhorar os conceitos sobre esse conjunto de números e aperfeiçoar o conhecimento. É natural imaginar o que levou o conjunto dos números complexos ter esta denominação. Mas concretizar o último termo desta designação como uma sobrecarga batismal do conteúdo em questão, é fruto de um contato não muito amistoso de um objeto em estudo que é abordado sem sentido, mal compreendido e/ou fora de contexto, uma vez que esses são trabalhados no ensino básico isoladamente, ou seja, sem nenhuma associabilidade com outros ramos da matemática, das ciências ou do meio ambiente. Essas situações podem ajudar o profissional na formalização de suas ideias, além de serem importantes nas abordagens de sala de aula pois proporcionam aos estudantes dinamização e sentido no que está sendo estudado, favorecendo uma melhor compreensão do conteúdo.

Finalmente, no Capítulo 3, chegaremos ao ponto que conheceremos todos os conjuntos de números que são abordados no ensino básico. A interrogação que convém no momento é: − Existe uma extensão de $\mathbb{C}$ que preserve suas propriedades aritméticas e algébricas? Responderemos esta pergunta e o direcionaremos à unicidade de $\mathbb{C}$ e os quatérnios de Hamilton (também conhecidos como números hipercomplexos), o qual faremos um apanhado histórico em consonância com sua formalização.

Capítulo 1

Dos Números Naturais aos Reais

"Deus criou os números naturais e o resto é obra da humanidade".
Leopold Kronecker

Neste capítulo abordaremos brevemente a evolução histórica do conceito de número na perspectiva de mostrar como o conhecimento matemático se desenvolveu ao longo dos tempos na construção dos conjuntos dos números naturais, inteiros, racionais e reais. Além disso observaremos a sistematização algébrica/axiomática desses conjuntos mediante as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Todavia, evitaremos demonstrações afim de evitarmos prolixidade.

1.1 Os números naturais

Os seres humanos, durante milhares de anos, viveram da caça, da obtenção de frutos e raízes. Eles não comerciavam, não plantavam, não criavam animais e nem construíam suas casas, sobreviviam do que a natureza lhes oferecia. Com o passar de milhões de anos, esse modo de vida foi se alterando e, deixando de ser apenas caçador e coletor de alimentos, o homem passou a ser agricultor, capturando animais para tê-los como reserva de alimento, aprendendo a domesticá-los e aproveitando-se do que ofereciam. Passaram então a viver em grupos, organizando-se e adequando-se às reais necessidades do seu povo que crescia, principalmente, reservar alimento para atender à população. "...afora os sistemas de contagem primitivos, tudo o mais teve de esperar o desenvolvimento da agricultura, intensiva e em grande escala, que requeria uma aritmética mais sofisticada" (EVES, 2004, P.23-24).

Inúmeras mudanças ocorreram na vida do homem, que de forma mais organizada desenvolveu o comércio rudimentar e o sistema de trocas. Sentindo a necessidade de contar e registrar essa contagem, o homem usava os dedos, marcas em madeira, pedras, folhas, nós em corda, marcas em ossos, etc. Na medida em que comparavam quantidades palpáveis com suas atividades cotidianas aprenderam a técnica, e se utilizavam da ideia de número inconscientemente. Através dessas comparações é que surgiu a ideia comum a esses dois grupos: o número.

Esta classe pioneira de números, utilizada principalmente para contagem, é chamada hoje em dia de *números naturais*. Utilizamos o símbolo $\mathbb{N}$ para representar o conjunto de todos os números naturais.

Do ponto de vista lógico/formal os números naturais podem ser apresentados através dos chamados *axiomas de Peano*.

No sistema axiomático desenvolvido por Peano para descrever os números naturais temos que os objetos não definidos são:

- Um conjunto $\mathbb{N}$, cujos elementos são chamados de *números naturais*.
- Uma função $s : \mathbb{N} \to \mathbb{N}$, tal que para cada $n \in \mathbb{N}$, $s(n)$ é chamado de *sucessor* de n.

Tais objetos não definidos satisfazem os seguintes axiomas:

P1. $s : \mathbb{N} \to \mathbb{N}$ é injetora.

P2. $\mathbb{N} - s(\mathbb{N})$ é um conjunto unitário. Ou seja, existe um número natural que não é sucessor de nenhum outro. Chamamos esse elemento de *zero* e o simbolizamos por 0.

P3. (Princípio da indução). Se $X \subset \mathbb{N}$ é um subconjunto tal que $0 \in X$ e, para todo $n \in X$ tem-se também $s(n) \in X$, então $X = \mathbb{N}$.

Às custas dos axiomas de Peano podemos definir as operações de adição e multiplicação de $\mathbb{N}$ e também derivar deles todas as propriedades aritméticas elementares, as quais listamos no teorema a seguir:

Teorema 1.1.1. *O conjunto dos números naturais* $\mathbb{N}$ *com as operações de adição e multiplicação satisfaz as seguintes propriedades:*

(a) *Quaisquer que sejam* $a, b, c \in \mathbb{N}$, $a + (b + c) = (a + b) + c$.

(b) *Quaisquer que sejam* $a, b \in \mathbb{N}$, $a + b = b + a$.

(c) *Se* $a, b, c \in \mathbb{N}$ *são tais que* $a + c = b + c$ *então* $a = b$.

(d) *Para qualquer* $a \in \mathbb{N}$, $a + 0 = a$.

(e) *Quaisquer que sejam* $a, b, c \in \mathbb{N}$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(f) *Quaisquer que sejam* $a, b \in \mathbb{N}$, $a \cdot b = b \cdot a$.

(g) *Se* $a, b, c \in \mathbb{N}$ *e* $c \neq 0$, *tais que* $a \cdot c = b \cdot c$ *então* $a = b$.

(h) *Quaisquer que seja* $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

(i) *Para qualquer* $a \in \mathbb{N}$, $a \cdot 1 = a$.

Assim, formalizamos este conjunto, o qual através dele podemos construir os números inteiros, racionais e reais.

1.2 Os números inteiros

Com o desenvolvimento da matemática, o conceito de número prosseguiu recriando-se, transformando-se e evoluindo naturalmente. O conjunto dos números naturais não mais contemplava a solução de todos os seus problemas.

Não se sabe ao certo quando se fez uso dos números negativos pela primeira vez. Mas é na China Antiga os relatos do surgimento do trabalho com números negativos. Segundo (NETO, 2010, p.11):

> Esse povo calculava usando coleções de barras vermelhas para os números positivos e barras pretas para os números negativos, contudo não aceitavam que um número negativo fosse solução de uma equação. Coube aos matemáticos indianos descobrirem os números negativos quando da tentativa de formular soluções de equações quadráticas.

As contribuições de Brahmagupta, teve impacto significativo nas construções matemáticas. Em sua obra há cerca de 628 d.C., sistematizou os números negativos e popularizou o conceito de zero, formalizando regras para esses. O matemático indiano "...não só utilizou os negativos em seus cálculos, como os considerou entidades

separadas e os dotou de uma aritmética concordante com a dos números naturais" (CARDOSO, 2013, p.17). Embora houvesse divergências, como a divisão por zero, que era considerada pelo matemático indiano ($\frac{0}{0} = 0$), e não definida na matemática moderna, mas muito se aproximava de nosso sistema atual.

Outros matemáticos, embora não manipulassem os números nagativos, já tinham conhecimento de sua existência. Como é o caso de Diofanto, que realizou operações com os números negativos.

> Os números negativos aparecem constantemente na obra "Arithmetica" de Diofanto datada do século III. Em certos problemas para o qual as soluções eram valores inteiros negativos como por exemplo:
>
> $$4 = 4x + 20 \text{ ou } 3x - 18 = 5x^2$$
>
> Nestas situações Diofanto limitava-se a classificar o problema de absurdo (CARDOSO, 2013, p.17).

Muitas foram as discussões entre os matemáticos que ousaram usar e os que não gozaram da utilidade dos números negativos. Até meados século XVI muitos consideravam seus cálculos como falsos ou impossíveis quando esses números apareciam. A Exemplo desse fato podemos citar Michael Stifel, que teria se recusado a admitir números negativos como raízes de uma equação, denominando-os de números absurdos. Consta que Cardano também usou os números negativos, embora chamando-os, como podemos dizer atualmente, de números fictícios. Por outro lado,

> Em 1484 o matemático Francês Nicolas Chuquet começa a utilizar com destreza o zero e também os números negativos, e em 1489 o matemático alemão Johann Widmann de Eger introduz os sinais + e − em substituição as letras "p" inicial de piu (mais) e de "m" inicial de minus (menos). Mais adiante, ...em 1582 o matemático Belga Simon Stévin elaborou um sistema de notação unificando o domínio de aplicação das regras aritméticas, que é uma aproximação das regras que hoje são aplicadas aos números inteiros (IFRAN 1997, apud NETO, 2010, p.11).

Séculos se passaram para que se dispertasse o interesse e seu desenvolvimento fosse retomado. E, com a ascensão do comércio e das interrelações dos seres humanos, no século XVIII muitos problemas começaram a surgir e motivaram a sociedade a formular métodos que os ajudassem a resolvê-los.

Problemas com números negativos não eram tão frequentes como atualmente, porém, situações como a noção de perda, empréstimos e dívidas motivaram o surgimento de simbologias que os contemplassem, assim como as ciências precisavam de símbolos que representassem temperaturas acima e abaixo de 0 °C, procurar uma linguagem matemática que expressasse a atração entre dois corpos era necessidade dos físicos, por exemplo.

Nesse mesmo período é que os grandes pensadores matemáticos começam a formalizar a interpretação geométrica dos números positivos e negativos em uma reta (Figura 1.1).

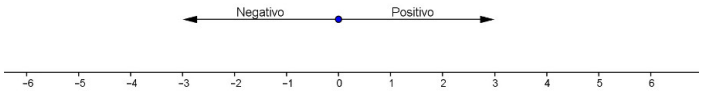


Figura 1.1: Reta de números inteiros
Fonte: Elaborado pelo Autor.

Nesse processo de formalização dos números inteiros, matemáticos como Hankel, buscaram realizar operações fundamentais, as quais geravam conflitos cognitivos, principalmente quando se multiplicava dois números negativos.

> A legitimidade dos números negativos deu-se definitivamente por Hermann Hankel $(1839 - 1873)$ publicada em 1867, "Teoria do Sistema dos números Complexos". Hankel formulou o *princípio de permanência e das leis formais* que estabelece um critério geral de algumas aplicações do conceito de número (NASCIMENTO, 2010, p.13).

Daí então muitos trabalhos foram desenvolvidos e concretizados ao longo dos tempos. A regra dos sinais foi estabelecida e as operações matemáticas organizadas e firmadas nos cálculos envolvendo números positivos e negativos que evoluíram ao que vemos na atualidade. Surgiu assim o novo conjunto numérico representado pela letra $\mathbb{Z}$ (que significa Zahl: número em alemão), sendo formado pelos números positivos (Naturais) e seus respectivos opostos, podendo ser escrito da forma: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.

Podemos construir formalmente os números inteiros a partir dos números naturais da seguinte maneira: dados $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ dizemos que $(a, b) \sim (c, d)$ se $a + d = c + b$. É de fácil verificação que $\sim$ assim definida é uma relação de equivalência.

Denotemos a classe de equivalência de um elemento $(a, b) \in \mathbb{N} \times \mathbb{N}$ módulo $\sim$ por $[(a, b)]$. Agora definimos operações de adição e multiplicação no espaço quociente $\dfrac{\mathbb{N} \times \mathbb{N}}{\sim}$ da seguinte maneira:

$$[(a, b)] + [(c, d)] := [(a + b, c + d)]$$

e

$$[(a, b)] \cdot [(c, d)] := [(ac + bd, bc + ad)].$$

Uma verificação de rotina permite concluir que estas duas operações estão bem definidas, ou seja, independem da escolha de representantes.

Observamos que para cada $[(a, a)]$ temos $[(a, a)] = [(0, 0)]$. Assim, para cada $[(a, 0)]$ temos a identidade:

$$[(a, 0)] + [(0, a)] = [(0, 0)]. \tag{1.1}$$

Outra observação é que se $(a, b) \in \mathbb{N} \times \mathbb{N}$ então existe $n \in \mathbb{N}$ tal que $a + n = b$ ou $a = b + n$; logo, $a + n = 0 + b$ ou $a + 0 = b + n$; logo $(a, b) \sim (0, n)$ ou $(a, b) \sim (n, 0)$; logo, $[(a, b)] = [(0, n)]$ ou $[(a, b)] = [(n, 0)]$. Portanto, temos

$$\frac{\mathbb{N} \times \mathbb{N}}{\sim} = \{[(a, 0)] \mid a \in \mathbb{N}\} \cup \{[(0, a)] \mid a \in \mathbb{N}\}$$

e

$$\{[(a, 0)] \mid a \in \mathbb{N}\} \cap \{[(0, a)] \mid a \in \mathbb{N}\} = \{[(0, 0)]\}.$$

Dessa maneira, todo elemento de $\dfrac{\mathbb{N} \times \mathbb{N}}{\sim}$ pode ser representado na forma $[(a, 0)]$ ou $[(0, a)]$.

O conjunto quociente $\dfrac{\mathbb{N} \times \mathbb{N}}{\sim}$ é de fato o que conhecemos como conjunto dos números inteiros e denotamos pelo símbolo $\mathbb{Z}$.

Teorema 1.2.1. *O espaço quociente $\mathbb{Z}$ com as operações acima definidas satisfaz as seguintes propriedades:*

(a) *Para cada $x, y, z \in \mathbb{Z}$, $x + (y + z) = (x + y) + z$.*

(b) *Para cada $x, y \in \mathbb{Z}$, $x + y = y + x$.*

(c) *Para cada $x \in \mathbb{Z}$, $x + [(0, 0)] = x$.*

(d) *Para cada* $x \in \mathbb{Z}$, *existe* $-x \in \mathbb{Z}$ *tal que* $x + (-x) = [(0,0)]$.

(e) *Para cada* $x, y, z \in \mathbb{Z}$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(f) *Para cada* $x, y \in \mathbb{Z}$, $x \cdot y = y \cdot x$.

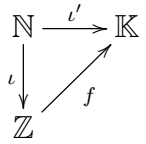
(g) *Para cada* $x \in \mathbb{Z}$, $x \cdot [(1,0)] = x$

(h) *Para cada* $x, y, z \in \mathbb{Z}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

(i) *Se* $x, y \in \mathbb{Z}$ *e* $x \cdot y = [(0,0)]$, *então* $x = [(0,0)]$ *ou* $y = [(0,0)]$.

(j) *A aplicação* $\iota : \mathbb{N} \to \mathbb{Z}$ *definida por* $\iota(a) = (a, 0)$ *para cada* $a \in \mathbb{N}$ *é um homomorfismo* (*ou seja,* (i) $\varphi(1) = (1,0)$; (ii) $\varphi(a+b) = \varphi(a) + \varphi(b)$; (iii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$) *injetor de* $\mathbb{N}$ *em* $\mathbb{Z}$.

(k) *Suponhamos que existe outra estrutura* $\mathbb{K}$ *equipada de operações* $+$ *e* $\cdot$ *e um homomorfismo* $\iota' : \mathbb{N} \to \mathbb{K}$ *satisfazendo as propriedades* (a)-(j). *Então existe um único homomorfismo injetor* $f : \mathbb{Z} \to \mathbb{K}$ *tal que o seguinte diagrama comuta*



Salientamos os fatos de que a demonstração da propriedade (d) é consequência da identidade (1.1) e que o item (k) nos diz que $\mathbb{Z}$ é único a menos de isomorfismos. Além disso, esta estrutura unicamente determinada pelas propriedades (a)-(j) do teorema acima, que chamamos de conjunto dos números inteiros, também possui todas as propriedades aritméticas de $\mathbb{N}$. Contudo, em $\mathbb{Z}$ existem propriedades não satisfeitas em $\mathbb{N}$, que ampliam possibilidades de estudo e desenvolvimento da matemática. Note também que a *lei do corte* da adição e multiplicação, definidas inicialmente em $\mathbb{N}$ nos itens (c) e (g), respectivamente, permanecem imersas em $\mathbb{Z}$, apresentadas sutilmente pelas propriedades (d) e (i), respectivamente, mencionadas acima.

1.3 Os números racionais

Os conjuntos de números não seguiram uma ordem cronológica, como muitos acreditam. A história nos mostra que os números naturais e racionais positivos antecedem os inteiros negativos.

Possivelmente as frações decimais surgiram como fruto da matemática moderna e não no período primitivo, uma vez que esses povos não tinham necessidade prática de usá-las.

Com o passar do tempo, a necessidade de expressar partes de um todo fez com que os racionais surgissem para representar situações em que os números inteiros positivos não eram suficientes.

> Os homens da Idade da Pedra não usavam frações, mas com o advento de culturas mais avançadas durante a Idade do Bronze parece ter surgido a necessidade do conceito de fração e de notação para frações (BOYER, 1974, P.9-10).

Assim como os inteiros são obtidos por uma construção formal a partir dos números naturais, também podemos obter os racionais a partir dos inteiros. Para isso, considere $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Diremos que $(a, b) \sim (c, d)$ se $a \cdot d = c \cdot b$. A relação $\sim$ assim definida é de equivalência e denotamos a classe de equivalência de um par $(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$ por $\frac{a}{b}$. Agora definimos operações $+$ e $\cdot$ em $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$ da seguinte maneira:

$$\frac{a}{b} + \frac{c}{d} := \frac{a \cdot d + b \cdot c}{b \cdot d}$$

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a \cdot c}{b \cdot d}$$

Observe que estas duas operações estão bem definidas, independentemente da escolha de seus representantes. O conjunto quociente $\mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim$ é, de fato, o conjunto dos números racionais, o qual denotamos por $\mathbb{Q}$.

Teorema 1.3.1. *O conjunto $\mathbb{Q}$ com as operações acima definidas satisfaz as seguintes propriedades:*

(a) *Para cada $x, y, z \in \mathbb{Q}$, $x + (y + z) = (x + y) + z$.*

(b) *Para cada $x, y \in \mathbb{Q}$, $x + y = y + x$.*

(c) *Para cada $x \in \mathbb{Q}$, $x + \frac{0}{1} = x$.*

(d) *Para cada $x \in \mathbb{Q}$, existe $-x \in \mathbb{Q}$ tal que $x + (-x) = \frac{0}{1}$.*

(e) *Para cada* $x, y, z \in \mathbb{Q}$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

(f) *Para cada* $x, y \in \mathbb{Q}$, $x \cdot y = y \cdot x$.

(g) *Para cada* $x \in \mathbb{Q}$, $x \cdot \frac{1}{1} = x$.

(h) *Para cada* $x, y, z \in \mathbb{Q}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

(i) *Para cada* $x \in \mathbb{Q}$, *não nulo, existe* $x^{-1} \in \mathbb{Q}$ *tal que* $x \cdot x^{-1} = \frac{1}{1}$.

(j) *A aplicação* $\iota : \mathbb{Z} \to \mathbb{Q}$ *definida por* $\iota(a) = \frac{a}{1}$ *para cada* $a \in \mathbb{Z}$ *é um homomorfismo* (*ou seja,* (i) $\varphi(1) = \frac{1}{1}$; (ii) $\varphi(a+b) = \varphi(a)+\varphi(b)$; (iii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$) *injetor de* $\mathbb{Z}$ *em* $\mathbb{Q}$.

(k) *Suponhamos que existe outra estrutura* $\mathbb{K}$ *equipada de operações* $+$ *e* $\cdot$ *e um homomorfismo* $\iota' : \mathbb{Z} \to \mathbb{K}$ *satisfazendo as propriedades* (a)-(j). *Então existe um único homomorfismo injetor* $f : \mathbb{Q} \to \mathbb{K}$ *tal que o seguinte diagrama comuta*

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\iota'} & \mathbb{K} \\ {\scriptstyle \iota}\downarrow & \nearrow_{f} & \\ \mathbb{Q} & & \end{array} .$$

Observe atentamente que $\mathbb{Z}$, pela aplicação (j) está imerso em $\mathbb{Q}$. Além disso, cabe perceber-mos que o conjunto dos números racionais preserva todas as propriedades do conjunto dos números inteiros e ainda estende-as.

1.4 Os números reais

Conta-se que Pitágoras[1] fundou a escola pitagórica em uma colônia grega ao sul da Itália, onde desenvolvia estudos filosóficos, de matemática e ciências naturais, além de ritos secretos e cerimônias, o que as heranças históricas nos reserva que era uma irmandade estreitamente unida. Com o tempo, forças democráticas do sul da Itália destruíram seus prédios e os pitagóricos se dispersaram, mas continuaram seus trabalhos secretamente por mais dois séculos. Um grande feito de Pitágoras é o teorema que leva seu nome - Teorema de Pitágoras, que lhe rendeu descobertas

[1]Pitágoras(c. 570-495 a.C.) - Foi um profeta, místico, nascido na Ilha Egéia de Samos, próxima a Mileto.

posteriores relacionando-o, entre outros, com o quadrado de lado unitário. "...esse teorema era conhecido pelos babilônios dos tempos de Hamurabi[2], mais de um milênio antes, mas sua primeira demonstração geral pode ter sido dada por Pitágoras" (EVES, 2004, p.103).

Os pitagóricos tinham uma filosofia de que tudo era explicado através dos números racionais. Representavam inteiros e racionais na reta numérica, de modo que o primeiro era representado em intervalos unitários igualmente espaçados, e o segundo representado também como subintervalos, o qual divide cada intervalo unitário em q subintervalos, que compõe as frações de denominador q.

> Deve ter sido um choque descobrir que há pontos na reta que não correspondem a nenhum número racional. Essa descoberta foi uma das grandes realizações dos pitagóricos. Em particular, os pitagóricos provaram que não há nenhum número racional ao qual corresponda o ponto P da reta no caso em que OP é igual à diagonal de um quadrado cujos lados medem uma unidade (Figura 1.2).
>
> A descoberta da existência de números irracionais foi surpreendente e perturbadora para os pitagóricos. Em primeiro lugar porque parecia desferir um golpe mortal na filosofia pitagórica segundo a qual tudo dependia dos números inteiros. Além disso parecia contrária ao senso comum, pois intuitivamente havia o sentimento de que toda grandeza podia ser expressa por *algum* número racional (EVES, 2004, p.105-106).

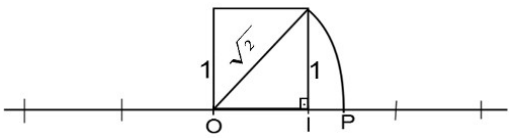


Figura 1.2: Representação geométrica de $\sqrt{2}$.
Fonte: Elaborado pelo autor.

Após essa descoberta, outros irracionais surgiram, embora ainda não houvesse uma definição precisa para tais números. Essa indefinição perdurou por séculos, sendo designados por palavras, ou valores aproximados aparentemente sem nenhuma relação uns com os outros. Como não foram definidos cientificamente, aceitou-se simplesmente a sua existência, mas sem generalizá-los.

[2]Hamurabi - foi um dos mais importantes reis da Babilônia. Viveu por volta de 1800 a.C. e 1750 a.C.

> Por volta de 370 a.C., o "escândalo" fora resolvido por Eudoxo, um brilhante discípulo de Platão e do pitagórico Arquitas, através de uma nova definição de proporção. O magistral tratamento dos incomensuráveis formulado por Eudoxo aparece no quinto livro dos *Elementos* de Eulides, e essencialmete coincide com a exposição moderna dos números irracionais dada por Dedekind em 1872 (EVES, 2004, p.107).

Tal exposição moderna dada por Dedekind evidencia esses números, também conhecidos como números incomensuráveis, que não são inteiros nem fracionários, como sendo aqueles que possuem parte decimal infinita e não periódica. Atualmente o denominamos de Conjunto dos Números Irracionais ($\mathbb{R} \setminus \mathbb{Q}$).

Para entender melhor o que fez Dedekind introduzimos a seguinte definição:

Definição 1.4.1. Dizemos que um subconjunto $\alpha \subset \mathbb{Q}$, de números racionais é um *corte de Dedekind*, se satisfaz as seguintes propriedades:

(a) $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$.

(b) Se $a \in \alpha$ então para todo racional b tal que $b \geq a$, devemos ter $b \in \alpha$.

(c) Para cada $a \in \alpha$ existe $c \in \alpha$ tal que $c < a$.

Para uma melhor compreensão do que seja um corte de Dedekind apresentamos o seguintes exemplos.

Exemplo 1.4.2. O subconjunto de números racionais $\alpha = \{r \in \mathbb{Q} \,|\, r > 0 \text{ e } r^2 > 2\}$ é um corte de Dedekind. Notemos que $0 \notin \alpha$ e $2 \in \alpha$, o que implica em α satisfazer a propriedade (a) da definição de corte de Dedekind. Para a propriedade (b), consideremos $a \in \alpha$ e $b \geq a$. Temos $b \geq a > 0$, o que nos dá $b^2 \geq a^2 > 2$. Logo, $b \in \alpha$, ou seja, α satisfaz a propriedade (b). Finalmente dado $a = \frac{p}{q} \in \alpha$ temos $\frac{p^2}{q^2} > 2$. Fazendo $n = 8q$, temos facilmente que $c = \frac{np}{nq+1}$ é tal que $c < a$. E ainda, de $a^2 = \frac{p^2}{q^2} > 2$ que

$$q^2 \geq 1 \tag{1.2}$$

e

$$p^2 \geq 2q^2 + 1, \tag{1.3}$$

pois p, $q \in \mathbb{Z}$. Assim, temos que

$$c^2 = \left(\frac{8qp}{8q^2+1}\right)^2 = \frac{64q^2p^2}{(8q^2+1)^2} \overset{(1.3)}{\geq} \frac{64q^2\cdot(2q^2+1)}{(8q^2+1)^2} = \frac{2\cdot 64q^4+64q^2}{(8q^2+1)^2}. \tag{1.4}$$

Afirmamos que

$$2\cdot 64q^4+64q^2 > 2\cdot(8q^2+1)^2. \tag{1.5}$$

De fato,

$$2\cdot 64q^4+64q^2-2\cdot(8q^2+1)^2 = 32q^2-2 \overset{(1.2)}{>} 0. \tag{1.6}$$

Logo, $2\cdot 64q^4+64q^2 > 2\cdot(8q^2+1)^2$ e, substituindo a desigualdade (1.5) em (1.4) segue que

$$c^2 = \left(\frac{8qp}{8q^2+1}\right)^2 > \frac{2\cdot(8q^2+1)^2}{(8q^2+1)^2} = 2 \tag{1.7}$$

e $c \in \alpha$. Portanto, α também satisfaz a propriedade (c) e temos, assim, a afirmação de que α é um corte de Dedekind verificada.

Exemplo 1.4.3. Para cada $r \in \mathbb{Q}$, denotaremos o conjunto $\{a \in \mathbb{Q} \mid a > r\}$ por $\overline{r}$. É imediata a verificação que $\overline{r}$ é um corte de Dedekind.

Consideremos agora o conjunto

$$\mathcal{R} = \{\alpha \subset \mathbb{Q} \mid \alpha \text{ é um corte de Dedekind}\}.$$

Definição 1.4.4. Sejam $\alpha, \beta \in \mathcal{R}$. Dizemos que α é *menor ou igual* a β, e denotamos por $\alpha \leq \beta$, se $\alpha \subset \beta$. Quando α está contido propriamente em β dizemos que α é *estritamente menor* que β e denotamos essa situação por $\alpha < \beta$.

Temos as seguintes propriedades para a relação $\leq$ em $\mathcal{R}$.

Proposição 1.4.5. *Sejam $\alpha, \beta \in \mathcal{R}$. Então apenas uma das três possibilidades pode ocorrer:*

(a) $\alpha < \beta$.

(b) $\alpha = \beta$.

(c) $\beta < \alpha$.

Destacamos os seguintes subconjuntos de $\mathcal{R}$:

$$\mathcal{R}_+ = \{\alpha \in \mathcal{R} \mid \overline{0} < \alpha\} \qquad \text{e} \qquad \mathcal{R}_- = \{\alpha \in \mathcal{R} \mid \alpha < \overline{0}\}.$$

Temos da Proposição 1.4.5 que $\mathcal{R}$ se escreve como a seguinte união disjunta

$$\mathcal{R} = \mathcal{R}_+ \cup \{\overline{0}\} \cup \mathcal{R}_-..$$

Dado $\alpha \in \mathcal{R} - \{\overline{0}\}$, temos que α é da forma $\overline{r}$, com $r \in \mathbb{Q} - \{0\}$, ou não. No primeiro caso definimos $-\alpha := \overline{-r}$ e no segundo $-\alpha := \{a \in \mathbb{Q} \mid \ -a \notin \alpha\}$.

Proposição 1.4.6. *Seja $\alpha \in \mathcal{R} - \{\overline{0}\}$. Então $-\alpha$ pertence a $\mathcal{R}$ e $-\alpha \neq \overline{0}$. Além disso,*

(a) $-(-\alpha) = \alpha$.

(b) $\alpha \in \mathcal{R}_+$ *se, e somente se,* $-\alpha \in \mathcal{R}_-$.

Definimos uma operação de adição no conjunto $\mathcal{R}$ da seguinte maneira: para cada $\alpha, \beta \in \mathcal{R}$,

$$\alpha + \beta = \{a + b \,|\, a \in \alpha \,\text{e}\, b \in \beta\}.$$

Também definimos uma multiplicação em $\mathcal{R}$. Nesse caso, definimos primeiramente para $\alpha, \beta \in \mathcal{R}_+$:

$$\alpha \cdot \beta = \{a \cdot b \,|\, a \in \alpha \,\text{e}\, b \in \beta\}.$$

Em seguida, definimos a multiplicação para quaisquer dois elementos de $\mathcal{R}$ da forma:

$$\alpha \cdot \overline{0} = \overline{0},$$

$$\alpha \cdot \beta = -((-\alpha) \cdot (\beta)), \quad \text{se} \quad \alpha < \overline{0} \quad \text{e} \quad \overline{0} < \beta;$$

$$\alpha \cdot \beta = -(\alpha \cdot (-\beta)), \quad \text{se} \quad \overline{0} < \alpha \quad \text{e} \quad \beta < \overline{0};$$

e

$$\alpha \cdot \beta = (-\alpha) \cdot (-\beta), \quad \text{se} \quad \alpha < \overline{0} \quad \text{e} \quad \beta < \overline{0}.$$

Temos então o seguinte teorema:

Teorema 1.4.7. *O conjunto $\mathcal{R}$ com a relação $\leq$ e as operações de adição e multiplicação acima definidas satisfaz as seguintes propriedades:*

(a) *Para cada* $\alpha, \beta \in \mathcal{R}$, $\alpha + \beta, \alpha \cdot \beta \in \mathcal{R}$ (*ou seja, as operações de adição e multiplicação são internas em* $\mathcal{R}$).

(b) *Para cada* $\alpha, \beta, \gamma \in \mathcal{R}$, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

(c) *Para cada* $\alpha, \beta \in \mathcal{R}$, $\alpha + \beta = \beta + \alpha$.

(d) *Para cada* $\alpha \in \mathcal{R}$, $\alpha + \overline{0} = \alpha$.

(e) *Para cada* $\alpha \in \mathcal{R}$, *existe* $-\alpha \in \mathcal{R}$ *tal que* $\alpha + (-\alpha) = \overline{0}$.

(f) *Para cada* $\alpha, \beta, \gamma \in \mathcal{R}$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

(g) *Para cada* $\alpha, \beta \in \mathcal{R}$, $\alpha \cdot \beta = \beta \cdot \alpha$.

(h) *Para cada* $\alpha \in \mathcal{R}$, $\alpha \cdot \overline{1} = \alpha$.

(i) *Para cada* $\alpha \in \mathcal{R}$ *com* $\alpha \neq \overline{0}$, *existe* $\alpha^{-1} \in \mathcal{R}$ *tal que* $\alpha \cdot \alpha^{-1} = \overline{1}$.

(j) *Para cada* $\alpha, \beta, \gamma \in \mathcal{R}$, $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

(k) *Se* $\alpha, \beta, \gamma \in \mathcal{R}$ *e* $\alpha \leq \beta$ *então* $\alpha + \gamma \leq \beta + \gamma$.

(l) *Se* $\alpha, \beta \in \mathcal{R}_+$, *então* $\alpha \cdot \beta \in \mathcal{R}_+$.

(m) *A aplicação* $\iota : \mathbb{Q} \to \mathcal{R}$ *definida por* $\iota(r) = \overline{r}$ *é um homomorfismo injetor de* $\mathbb{Q}$ *em* $\mathcal{R}$.

A aplicação $\iota : \mathbb{Q} \to \mathcal{R}$ permite identificarmos $\mathbb{Q}$ como subconjunto de $\mathcal{R}$.

Definição 1.4.8. Um subconjunto S de $\mathcal{R}$ é dito *limitado superiormente* se existe $\alpha \in \mathcal{R}$ tal que $\beta \leq \alpha$ para todo $\beta \in S$.

De maneira análoga definimos conjunto *limitado inferiormente*.

Definição 1.4.9. Seja S um subconjunto de $\mathcal{R}$ limitado superiormente. Um elemento α de $\mathcal{R}$ é chamado de *supremo* de S se satisfaz as seguintes condições:

(i) $\beta \leq \alpha$ para cada $\beta \in S$.

(ii) Se $\beta \leq \alpha'$ para cada $\beta \in S$ então $\alpha \leq \alpha'$.

Teorema 1.4.10. *Todo subconjunto de* $\mathcal{R}$ *limitado superiormente possui um supremo.*

Finalmente, temos:

Teorema 1.4.11. *Suponhamos que exista uma estrutura $\mathcal{R}'$ equipada com operações de adição e multiplicação e uma relação de ordem $\leq$ satisfazendo as propriedades dos teoremas* 1.4.7 *e* 1.4.10. *Então, $\mathcal{R}'$ é isomorfa a $\mathcal{R}$.*

De fato, esta estrutura unicamente determinada, a menos de isomorfismo, pelos teoremas 1.4.7 e 1.4.10 é o que conhecemos como conjunto de números reais e denotamos por $\mathbb{R}$.

Capítulo 2

Os Números Complexos

O capítulo em questão aborda a história dos números complexos mostrando como surgiram, sua problematização, formalização e aceitação no decorrer da história. Além disso apresentaremos situações que exibem sua utilidade tanto na matemática em si, como no meio social e no processo de ensino-aprendizagem.

2.1 Sobre o surgimento

Várias foram as civilizações que historicamente buscaram representações que possibilitassem a construção de um sistema matemático organizado para o desenvolvimento do cálculo. A evolução desse fenômeno gerou vários conjuntos, os quais até então abordamos os naturais, inteiros, racionais e reais.

Paralelamente às demais situações e problemáticas que geraram os conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, operações que envolveram radicais causaram muita discussão, imparcialidade e desprezo. Atualmente muitos enganam-se por associar o surgimento da raiz quadrada de números negativos com o estudo das equações do segundo grau.

Nas proximidades do ano 2000 a.C. os matemáticos antigos da Babilônia "...resolviam equações quadráticas, seja pelo método equivalente ao de substituição numa fórmula geral, seja pelo método de completar quadrados, como também se discutiam algumas cúbicas (grau três) e algumas biquadradas (grau quatro)" (EVES, 2004, P.61-62). Esses apenas consideravam resultados positivos, descartando os casos em que apareciam as raízes quadradas de números negativos, ou apenas julgavam não haver solução, já que associavam os problemas a situações concretas. Nesse período, não há registros das raízes quadradas de números negativos, nem tampouco, a sugestão do

uso de números complexos.

Centenas de anos se passaram, havendo uma lacuna no que se refere a esse fenômeno. Todavia, a partir do século I d.C., matemáticos deixaram indícios de um conhecimento em processo de sistematização.

> O primeiro registro de um radical de um número negativo ...aparece na *Estereometria* de Heron, matemático grego do período Alexandrino, publicada aproximadamente em 75 d.C.. Num cálculo sobre o desenho de uma pirâmide surge a necessidade de avaliar $\sqrt{81-144}$. A questão parece não causar nenhum problema simplesmente porque logo em seguida os números apresentam-se trocados: $\sqrt{144-81}$, resultando $\sqrt{63}$, que é calculado como aproximadamente igual a $7\frac{15}{16}$ (SBM, 2013, p.143).

Em aproximadamente 275 d.C., na *Arithmetica* de Diofanto, é abordado o problema: *"Um triângulo retângulo tem área igual a* 7 *e seu perímetro é de* 12 *unidades. Encontre o comprimento dos seus lados"*(SBM, 2013, p.143). Nesse, ao algebrizar as informações, denominando de x e y o comprimento dos catetos desse triângulo temos que $\frac{1}{2}xy = 7$; e $x^2+y^2 = (12-x-y)^2$, as quais geram a equação $24x^2-172x+336 = 0$. "Nesse ponto Diophanto observa que só poderia haver solução se $\left(\frac{172}{2}\right)^2 \geq 24 \cdot 336$. Nesse contexto, é claro que não há necessidade alguma de introduzir um sentido para a expressão $\sqrt{-167}$, sendo -167 o discriminante da equação"(SBM, 2013, p.143).

> Encontram-se novas referências à questão na matemática indiana. Aproximadamente no ano de 850 d.C, o matemático indiano Mahavira afirma: *...como na natureza das coisas um negativo não é um quadrado, ele não tem, portanto, raiz quadrada.*
>
> Já no século XII, o famoso matemático Bhaskara ($1114-1185$ aprox.) escreve: *O quadrado de um afirmativo é afirmativo; e a raiz quadrada de um afirmativo é dupla: positiva e negativa. Não há raiz quadrada de um negativo; pois ele não é um quadrado.*
>
> Também na matemática européia aparecem observações dessa natureza; Luca Pacioli, na sua *Summa de arithmetica, geométrica, proportioni et proportionalita*, publicada em 1494, escreve que a equação $x^2 + c = bx$ é solúvel somente se $\frac{1}{4}b^2 \geq c$, e o matemático francês Nicolas Chuquet ($1445-1500$ aproximadamente) faz observações semelhantes sobre "soluções impossíveis" num manuscrito, não publicado, de 1484 (SBM, 2013, p.144).

Assim, é conciso o fato de os matemáticos já terem conhecido a problemática das raízes de números negativos há muito tempo. A rejeição com essa nova noção de número se concretizava principalmente pela crença de que se tratava de mera abstração, isto é, não tinha utilidade prática. Noção que foi sendo extinta com desenvolvimentos posteriores. Cardano e Bombelli em meados do século XVI também desenvolveram trabalhos que contribuíram significativamente na transição, aperfeiçoamento e aceitação desses números.

Cardano, apesar de não ser o precursor, em sua obra *Ars Magna*, tornou pública a resolução das equações cúbicas e quárticas, fato que ocorreu no ano de 1545 da era cristã.

> A sugestão para resolver a cúbica, ele afirma, lhe tinha sido dada por Niccolo Tartaglia (cerca de $1500 - 1557$); a solução da quártica tinha sido descoberta primeiramente pelo antigo amanuense de Cardano, Ludovico Ferrari ($1522 - 1565$). É possível que o próprio Tartaglia tenha recebido uma sugestão quanto à resolução da cúbica de uma fonte mais antiga (Boyer, 1974, p.206).

Nem Cardano nem Tartaglia foram pioneiros na resolução dessas equações cúbicas, que conduziram fortemente as raízes quadradas de números negativos a serem reconhecidas como números no sentido próprio.

> O herói no caso foi evidentemente alguém cujo nome mal é lembrado hoje − Scipione Del Ferro (cerca de $1465-1526$), professor de matemática em Bolonha, uma das mais antigas universidades medievais e uma escola com forte tradição matemática. Como ou quando Ferro fez sua maravilhosa descoberta não se sabe. Não publicou a solução, mas antes de sua morte ele a revelou a um estudante, Antônio Maria Fior (ou Floridus em latim), um medíocre matemático.
>
> Na época, porém, quando coeficientes negativos praticamente não eram usados, havia tantos tipos de cúbicas quantas são as possibilidades de coeficientes positivos e negativos. Fior só sabia resolver equações do tipo em que cubos e raízes estão igualados a um número – isto é, as do tipo $x^3 + px = q$, embora na época só fossem usados coeficientes numéricos (positivos) específicos. Mas enquanto isso Tartaglia tinha aprendido também a resolver equações em que cubos e quadrados são igualados a um número. É provável que Tartaglia soubesse reduzir esse caso ao de Fior por remoção

> do termo quadrático, pois por essa época tornou-se conhecido que se o primeiro coeficiente é a unidade, então o coeficiente do termo quadrático, quando aparece do outro lado do sinal de igual, é a soma das raízes (Boyer, 1974, p.207).

Mas, é fato que *Ars Magna* significou uma nova etapa para o pensamento matemático quando Cardano publicou métodos algébricos para a resolução da equação cúbica $x^3 + px = q$, cuja solução é dada por $x = \sqrt[3]{\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} + \frac{q}{2}} - \sqrt[3]{\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} - \frac{q}{2}}$. E ainda, após demonstrar que "a fórmula que recebeu de Del Ferro e Tartaglia estava correta,..., encontrou um método para reduzir as formas mais complexas das cúbicas" (JÚNIOR, 2009, p.15) reduzindo uma equação de terceiro grau completa à sua forma mais simples (Equação (2.4)).

Os trabalhos de Cardano, assim como de muitos matemáticos que nos antecederam tinham uma linguagem específica do período e da região em questão. Atualmente, no que se refere à fórmula resolutiva de equações cúbicas, podemos demonstrá-la como segue.

Na equação completa de grau três

$$x^3 + bx^2 + cx + d = 0 \tag{2.1}$$

Substituindo $x = y + t$ na equação (2.1) temos

$$(y+t)^3+b(y+t)^2+c(y+t)+d = y^3+(3t+b)y^2+(3t^2+2tb+c)y+(t^3+t^2b+tc+d) = 0. \tag{2.2}$$

Fazendo $t = -\frac{b}{3}$ na expressão (2.2) temos que

$$x^3 + bx^2 + cx + d = y^3 + py + q,$$

onde

$$x = y - \frac{b}{3}, \quad p = c - \frac{b^2}{3} \quad \text{e} \quad q = \frac{2b^3}{27} - \frac{bc}{3} + d \tag{2.3}$$

Portanto, para encontrar as raízes da equação (2.1) basta achar as raízes de

$$y^3 + py + q = 0 \tag{2.4}$$

com p e q como em (2.3) subtraído de $\frac{b}{3}$.

Prosseguindo a demonstração, fazendo $y = u + v$ e substituindo em (2.4):

$$(u+v)^3 + p(u+v) + q = (u^3 + v^3 + q) + (u+v)\cdot(p + 3uv) = 0. \tag{2.5}$$

Daí, cada solução (u, v) do sistema

$$\begin{cases} u^3 + v^3 &= -q \\ u \cdot v &= -\frac{p}{3} \end{cases}$$

fornece uma solução (u, v) de (2.5) da forma $y = u + v$ da equação (2.4).
Assim,

$$u^3 + v^3 = -q \Rightarrow u^3 = -v^3 - q. \tag{2.6}$$

Como

$$u \cdot v = -\frac{p}{3} \Leftrightarrow u^3 \cdot v^3 = -\frac{p^3}{27}, \tag{2.7}$$

então, substituindo (2.6) em (2.7), segue que

$$(-v^3 - q)v^3 = -\tfrac{p^3}{27} \Leftrightarrow v^6 + v^3 q - \tfrac{p^3}{27} = 0.$$

Fazendo $v^3 = z$ temos a equação quadrática

$$z^2 + qz - \frac{p^3}{27} = 0. \tag{2.8}$$

cujas raízes são

$$z_1 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad \text{e} \quad z_2 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}. \tag{2.9}$$

Portanto, pela simetria em que u e v desempenham, segue a famosa fórmula de *Cardano*, *Tartaglia* ou de *Tartaglia-Cardano* (Raízes da equação (2.1)).

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{2.10}$$

Não motivadas por situações práticas, a resolução de equações cúbicas foi considerada por muitos, uma das maiores contribuições à álgebra desde que os babilônios no segundo milênio antes de Cristo aprenderam a completar quadrados para resolução de equações quadráticas.

Todavia, Cardano tinha problemas em resolver equações do tipo $x^3 = 15x + 4$, por exemplo, cujo resultado é $x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$. Sabia da não existência de raiz quadrada de número negativo, mas percebeu que $x = 4$ é uma raiz, sendo embaraçoso a sua compreensão. "Cardano se referia a essas raízes quadradas de números negativos como *sofísticas* e concluía que o resultado nesse caso era *tão sutil quanto inútil*" (BOYER, 1974, p.209).

Trabalhar com raiz quadrada de números negativos originou muitas dificuldades, pois não podiam ser tratados como os irracionais, que eram manipulados com aproximações de números racionais, por exemplo. Consta que Cardano usou-os embora chamando-os números fictícios, pois não conseguiu decifrar o enigma da generalização do conceito que conhecemos hoje, os números complexos.

Foi preciso pouco mais de duas décadas para Bombelli dar mais sentido à raiz da equação $x^3 = 15x + 4$ que, apesar da existência da raiz quadrada de número negativo, apresentava uma solução para o problema ($x = 4$). Fato que impulsionou o matemático a tentar compreender o sentido de seu acontecimento.

Em seu estudo, publicado em *l'Augebra* - 1572, Bombelli observou que radicais como $\sqrt{-1}$ não tinham signicado, mas era possível realizar operações quando se cancelavam. Assim, admitindo a possibilidade de que a raiz cúbica de $2 + \sqrt{-121}$ seja $a + \sqrt{-b}$, isto é, que $(a + \sqrt{-b})^3 = 2 + \sqrt{-121}$, supôs que

$$\begin{cases} \sqrt[3]{2+\sqrt{-121}} &= a + \sqrt{-b} \\ \sqrt[3]{2-\sqrt{-121}} &= a - \sqrt{-b}. \end{cases} \tag{2.11}$$

> Como ele sabe que 4 deve ser raiz da equação, necessariamente $a + \sqrt{-b} + a - \sqrt{-b} = 4$. Nesse ponto, felizmente, as quantidades não existentes se cancelam e obtemos $a = 2$. Com esse resultado, é muito fácil voltar à equação $(a + \sqrt{-b})^3 = 2 + \sqrt{-121}$ e deduzir que $b = 1$. Assim, ele obtém que $\sqrt[3]{2+\sqrt{-121}} = 2 + \sqrt{-1}$ e que $x = 2+\sqrt{-1}+2-\sqrt{-1} = 4$ é uma solução da equação (SBM, 2013, p.145).

Inseguro, com suspeitas, ou não, Bombelli acabara de dar um grande passo para o aperfeiçoamento das operações com esse tipo de número. E, a partir de então esses começam a ser utilizados para resolver equações de terceiro grau, ao mesmo tempo que era cogitado que tais números não poderiam existir.

Talvez, uma grande deficiência em se trabalhar com esses números seria a ausência de uma associação a algo físico ou de uma representação geométrica. Essa útima percorreu um longo caminho até a sua formalização.

O primeiro a se ater a uma interpretação geométrica foi o inglês J. Wallis. No entanto suas idéias foram confusas e não exerceram influência sobre seus contemporâneos.

Entre outros que se dispuseram a buscar uma representação geométrica para esse conjunto de números podemos citar:

• A. De Moivre que deixou a importante fórmula que conhecemos atualmente por

$$(\cos\alpha + i\ \operatorname{sen}\beta)^n = \cos n\alpha + i\ \operatorname{sen} n\beta.$$

• O inglês R. Cotes que em 1714 obteve um importante resultado, associado a obtenção de raizes n-ésimas da unidade que, em notação atual, pode-se escrever como

$$log_e(\cos\varphi + i\ \operatorname{sen}\varphi) = i\varphi;$$

• O matemático Albert Girard, enuncia claramente as relações entre raízes e coeficientes, admitindo raizes negativas e imaginárias, nas quais fez uso do símbolo $\sqrt{-1}$.

> Caspar Wessel, Jean Robert Argand e Gauss foram os primeiros autores a notar a associação, agora familiar, entre números complexos e pontos reais do plano.
>
> Parece não haver dúvida de que a prioridade da idéia cabe a Wessel, com um artigo apresentado à Real Academia Dinamarquesa de Ciências em 1797 e publicado nas atas dessa academia em 1799. A contribuição de Argand figura num artigo publicado em 1806 e mais tarde, em 1814 apresentado nos *Annales de Mathématiques* de Gergonne (EVES, 2004, p. 522).

Todavia, os registros do artigo de Wessel permaneceram inacessíveis durante cerca de noventa e oito anos após ter sido escrito, o que justifica a denominação do plano complexo ser chamado de *plano de Argand* em vez de *plano de Wessel*.

Muitos matemáticos, foram tão sutís quanto grandiosos na construção do conhecimento matemático. Dentre eles, a priori, expor completamente as contribuições de

Euler seria um tanto demasiado. Mas, dentre suas numerosas heranças ficou registrado algumas elementares notações, tais como "$f(x)$" para funções, "e" para base dos logaritmos naturais, "$\sum$" para somatórios, e a nobre utilização de "i" para representar a unidade imaginária, $\sqrt{-1}$. Este último símbolo "apareceu impresso pela primeira vez em 1794 e se tornou amplamente aceito após seu uso por Gauss em 1801. Os termos real e imaginário foram empregados pela primeira vez por René Descartes em 1637" (SBM, 2013, p.147).

Matemático, entre outros, que não se pode passar despercebido, Gauss foi quem "deu a primeira demonstração plenamente satisfatória do *teorema fundamental da álgebra* (que uma equação polinomial, com coeficientes complexos e de grau $n > 0$, tem pelo menos uma raiz complexa)" (EVES, 2004, p.520). Além disso, em 1832 foi quem introduziu a expressão a qual ficou conhecida e é utilizada até os dias de hoje: *Número Complexo*.

Conceber um número complexo $a+bi$ de forma que as partes real (a) e imaginária (b) sejam as coordenadas retangulares de um ponto do plano proporcionou aos matemáticos visualização e um conforto no trabalho com os números imaginários, pois cada número complexo correspondia a um único ponto do plano e vice-versa (figura 2.1).

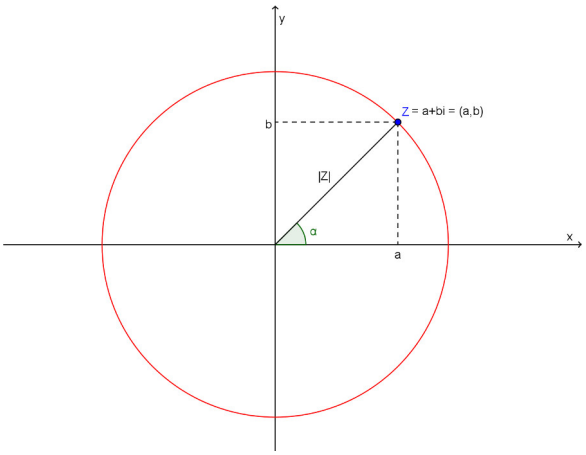


Figura 2.1: Plano de Argand-Gauss
Fonte: Elaborada palo autor.

A formalização completa dos números complexos deve-se a Hamilton[1]. Assim como muitos atualmente, matemáticos da época consideravam um número complexo

[1]William Rowan Hamilton (1805 – 1865) - Foi matemático, físico e astrônomo irlandês.

como simplesmente $z = a + bi$, onde a e b são números reais e i um número tal que $i^2 = -1$. Além disso eram satisfeitas:

a) a adição

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

b) e a multiplicação

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$

normalmente, substituindo i^2 por -1, como se fossem polinômios lineares em i.

Hamilton concebeu os números complexos como pares de números. Assim, o número complexo $a + bi$ foi representado por ele simplesmente pelo par ordenado de números reais (a, b), de modo que a igualdade de dois pares $(a, b) = (c, d)$ fosse satisfeita se, e somente se, $a = c$ e $b = d$. E ainda,

$$(a, b) + (c, d) \quad = \quad (a + c, b + d) \tag{2.12}$$

e

$$(a, b) \cdot (c, d) \quad = \quad (ac - bd, ad + bc). \tag{2.13}$$

Definidas dessa forma, é facilmente demonstrável que a comutatividade, a associatividade e a distibutividade da multiplicação com relação à adição, são válidas para pares ordenados de números reais.

> Deve-se notar que assim o sistema de números reais está *imerso* no sistema dos números complexos. Isso significa que, identificando-se cada número real r com o par correspondente $(r, 0)$, essa correspondência preserva a adição e a multiplicação, pois temos
>
> $$(a, 0) + (b, 0) = (a + b, 0)$$
>
> e
>
> $$(a, 0) \cdot (b, 0) = (ab, 0).$$
>
> Na prática, um número complexo da forma $(r, 0)$ pode ser substituído pelo número real r associado a ele. Para obter a forma antiga

> de um número complexo, a partir da forma de Hamilton, notemos que todo número complexo (a, b) pode ser escrito como
>
> $$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi,$$
>
> onde se representa $(0, 1)$ pelo símbolo i e se identificam $(a, 0)$ e $(b, 0)$ com os números reais a e b. Finalmente, observemos que
>
> $$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1.$$
>
> Dessa forma eliminou-se a aura mística que cercava os números complexos, pois não há nada místico num par ordenado de números reais. Esse foi um grande feito de Hamilton (EVES, 2004, p.549).

Durante séculos o desenvolvimento da matemática percorreu maneiras originais, sutís e rigorosas. Não obstante, é Hamilton que concretiza e garante a estruturação e existência matemática dos números complexos, que ganharam espaço e a natureza que conhecemos atualmente.

2.2 Uma defesa concretizada no decorrer da história

O conhecimento dos números complexos foi construído em um processo de evolução muito longo. Para muitos matemáticos ficava claro que um número negativo não era um quadrado, o que conduzia a conclusão de que tais raízes quadradas não tinham nenhum significado. De fato, esse pensamento prevaleceu por muito tempo, e a rejeição era clara, uma vez que acreditava-se que sua utilidade prática era inexistente.

Muitas foram as denominações que receberam durante décadas, mas, o uso desses termos refletiu nada a mais que a natureza enganadora do conceito de matemáticos que viveram séculos atrás, os quais muitos não presenciaram o momento em que o paradigma foi quebrado.

Desenvolvimentos posteriores a Bombelli mostraram que muitos matemáticos estavam equivocados. Os números complexos ascenderam e contribuíram para o desenvolvimento das ciências, além de desempenhar um papel sumamente importante nos mais diversos ramos da matemática, em consonância com o meio social. A seguir apresentamos alguns fatos e acontecimentos que corroboram esta defesa dos números complexos.

2.2.1 Uma defesa do ponto de vista algébrico

Um marco crucial para a redenção dos números complexos foi sem dúvida o celebrado teorema fundamental da álgebra o qual enunciamos a seguir.

Teorema 2.2.1. *Todo polinômio não constante em uma variável com coeficientes em* $\mathbb{C}$ *contém ao menos uma raiz em* $\mathbb{C}$.

A primeira tentativa séria de demonstrar este teorema foi feita pelo matemático francês Jean Le Rond D'Alember em 1746,

> ...cuja prova foi considerada falha, sendo melhorada e simplificada por Argand em 1806 e posteriormente em 1814. Naquela época, com o conhecimento que se tinha dos números reais, não era possível provar tal teorema de existência. A prova desse fato teve que esperar que os números reais fossem construídos por Richard Dedekind, por volta de 1870, para ser realizada em 1874 pelo matemático alemão Karl Weierstrass (HEFEZ; VILLELA, 2012, p. $142 - 143$).

Uma outra prova foi dada em 1772 pelo matemático francês Lagrange, a qual é considerada a mais algébrica de todas. Essa prova foi contestada por Gauss, "por não aceitar que se recorresse a nenhum corpo estranho aos complexos para garantir a existência das raízes de uma equação algébrica com coeficientes reais" (HEFEZ; VILLELA, 2012, p. 143). Apesar que em 1887, Kronecker garante a existência de um corpo onde um determinado polinômio tem sempre raízes, completando a prova de Lagrange.

Em sua tese de doutorado de 1797, publicada em 1799, Gauss fez críticas às demonstrações anteriores, as quais segundo tinha falhas. "Ao longo de sua vida, Gauss, deu quatro provas do Teorema Fundamental da Álgebra, todas com alguma falha, dado o grau insuficiente do desenvolvimento da matemática da época" (HEFEZ; VILLELA, 2012, p. 143).

Uma consequência imediata do teorema fundamental da álgebra é:

Corolário 2.2.2. *Seja* $f(X) = a_nX^n + \ldots + a_1X + a_0$ *um polinômio com coeficientes complexos, então* $f(X)$ *se fatora completamente na forma*

$$f(X) = a_n(X - z_1)\cdots(X - z_n)$$

onde $z_1, \ldots, z_n$ *são as raízes complexas de* f.

Para falar um pouco mais sobre a utilidade desse teorema introduzimos mais uma importante definição associada aos números complexos.

Definição 2.2.3. A função $- : \mathbb{C} \to \mathbb{C}$ definida pela regra

$$\overline{a + bi} = a - bi$$

é chamada de *conjugação complexa*. Para cada $z \in \mathbb{C}$ chamamos $\overline{z}$ de *conjugado* de z.

Propriedades fundamentais da conjugação complexa são listadas na seguinte proposição.

Proposição 2.2.4. *A conjugação complexa é uma bijeção e além disso temos:*

(a) *Para cada* $z_1, z_2 \in \mathbb{C}$, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.

(b) *Para cada* $z_1, z_2 \in \mathbb{C}$, $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

(c) *Para* $z \in \mathbb{C}$ *tem-se* $\overline{z} = z$ *se, e somente se,* $z \in \mathbb{R}$. *Em particular, a conjugação complexa quando restrita a* $\mathbb{R}$ *nos dá a aplicação identidade de* $\mathbb{R}$.

Prova. Para ver que é uma bijeção notemos que

$$\overline{\overline{a + bi}} = \overline{a - bi} = a - (-b)i = a + bi.$$

Logo, compor a conjugação com ela própria resulta na aplicação identidade de $\mathbb{C}$. Assim, a conjugação complexa é inversa dela própria. Portanto, a conjugação complexa é uma bijeção.

Agora suponhamos $z_1 = a_1 + b_1 i$ e $z_2 = a_2 + b_2 i$. Temos:

$$\begin{aligned}
\overline{z_1 + z_2} &= \overline{(a_1 + a_2) + (b_1 + b_2)i} \\
&= (a_1 + a_2) - (b_1 + b_2)i \\
&= (a_1 - b_1 i) + (a_2 - b_2 i) \\
&= \overline{z_1} + \overline{z_2}
\end{aligned}$$

e

$$\begin{aligned}\overline{z_1 \cdot z_2} &= \overline{(a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i} \\ &= (a_1a_2 - b_1b_2) - (a_1b_2 + a_2b_1)i \\ &= (a_1 - b_1i) \cdot (a_2 - b_2i) \\ &= \overline{z_1} \cdot \overline{z_2}.\end{aligned}$$

Portanto, os itens (a) e (b) seguem. O item (c) segue imediatamente da definição da conjugação complexa. □

Combinando o teorema fundamental da álgebra com as propriedades da conjugação complexas podemos obter o seguinte resultado.

Proposição 2.2.5. *Seja f um polinômio não constante em uma variável com coeficientes reais. Se $z \in \mathbb{C}$ é raiz de f então $\overline{z}$ também é raiz de f. Em particular, as raízes complexas de f que não são reais acontecem aos pares, uma conjugada da outra.*

Prova. Digamos que

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots a_1X + a_0,$$

com $a_0, \ldots, a_n \in \mathbb{R}$. Como z é raiz de f temos:

$$a_nz^n + a_{n-1}z^{n-1} + \ldots a_1z + a_0 = 0.$$

Aplicando a conjugação complexa nos dois lados dessa igualdade segue que

$$\overline{a_nz^n + a_{n-1}z^{n-1} + \ldots a_1z + a_0} = 0.$$

Aplicando os itens (a), (b) e (c) no lado esquerdo dessa igualdade tem-se que

$$a_n\overline{z}^n + a_{n-1}\overline{z}^{n-1} + \ldots a_1\overline{z} + a_0 = 0,$$

ou seja, $f(\overline{z}) = 0$. Portanto, temos o desejado. □

Passamos agora a colher os frutos das observações acima.

Corolário 2.2.6. *Seja f um polinômio não constante em uma variável com coeficientes em $\mathbb{R}$. Se f tem grau ímpar então f contém uma raiz real.*

Prova. Se todas as raízes de f não pertencessem a $\mathbb{R}$ então pela Proposição 2.2.5 f teria uma quantidade par de raízes. Logo, f seria um produto par de fatores de grau 1. Logo, f teria grau par. □

Para o próximo corolário necessitamos introduzir a seguinte definição.

Definição 2.2.7. *Seja f um polinômio não constante em uma variável, com coeficientes em $\mathbb{R}$. Dizemos que f é irredutível sobre $\mathbb{R}$ se não existe polinômios não constantes g e h, com coeficientes em $\mathbb{R}$, tais que $f = g \cdot h$.*

No corolário abaixo detalhamos como deve ser o formato de um polinômio irredutível sobre $\mathbb{R}$.

Corolário 2.2.8. *Se f é um polinômio irredutível sobre $\mathbb{R}$ então o grau de f é 1 ou 2.*

Prova. Provaremos o resultado utilizando a contrapositiva. Para isso, estabeleceremos inicialmente a seguinte afirmação:

Afirmação: *Seja p um polinômio não constante com coeficientes em $\mathbb{R}$. Suponhamos q e s polinômios com coeficientes complexos tais que $p = q \cdot s$. Então q tem coeficientes reais se, e somente se, s tem coeficientes reais.*

Digamos que $p = a_n X^n + \ldots + a_0$, $q = b_m X^m + \ldots + b_0$ e $s = c_{n-m} X^{n-m} + \ldots + c_0$ (com a_n, b_m, c_{n-m} não nulos). Primeiro suponhamos q com coeficientes reais. Temos que $a_n = b_m \cdot c_{n-m}$; logo $c_{n-m} = a_n \cdot b_m^{-1} \in \mathbb{R}$. Para o coeficiente a_{n-1} temos $a_{n-1} = b_m \cdot c_{n-m-1} + b_{m-1} \cdot c_{n-m}$; logo, $c_{n-m-1} = b_m^{-1}(a_{n-1} - b_{m-1} \cdot c_{n-m}) \in \mathbb{R}$. Procedendo dessa maneira sucessivamente mostramos que todos o coeficientes c_i de s estão em $\mathbb{R}$ e obtemos o desejado. A recíproca é análoga.

Agora suponhamos o grau de f maior que 2. Se f tem uma raiz real α então sabemos que $f(X) = (X - \alpha)g(X)$ para algum $g(X)$ com coeficientes, *a priori* em $\mathbb{C}$. Note que o grau de $g(X)$ é maior que 1 pois o grau de $f(X)$ é maior que 2. Logo, $g(X)$ não é constante. Como $X - \alpha$ tem coeficientes reais segue pela afirmação que g também tem coeficientes reais. Logo f não é irredutível.

Por outro lado, se f não contém raiz real então pelo teorema fundamental da álgebra ele deverá conter uma raiz complexa $z = a + bi$ que não pertence a $\mathbb{R}$. Mas, pela Proposição 2.2.5 devemos ter $\overline{z} = a - bi$ como raiz de f. Assim

$$f(X) = (X - z)(X - \overline{z})g(x)$$

onde $g(X)$ é um polinômio com coeficientes complexos e seu grau é maior ou igual a 1 pois o grau de f é maior que 2. Notemos que

$$(X - z)(X - \overline{z}) = X^2 + 2aX + (a^2 + b^2)$$

é um polinômio com coeficientes reais. Logo, pela afirmação segue que $g(X)$ também é um polinômio com coeficientes reais. Logo, f não é irredutível.

Portanto, temos o resultado desejado. □

Observação 2.2.9. Note que as hipóteses e teses dos dois corolários acima são informações no âmbito do conjunto dos números reais. Contudo, para ligar os pontos hipótese e tese, nos dois casos, tivemos que sair do universo dos números reais, explorando uma maior liberdade proporcionada pelo conjunto dos números complexos. Essa é uma estratégia belíssima que põe em relevo a importância dos números complexos do ponto vista algébrico.

2.2.2 Uma defesa do ponto de vista geométrico

Nas discussões anteriores vimos que cada número complexo $a + bi$ é naturalmente identificado com o vetor (a, b) do plano. A porta de entrada para usufruir a estrutura multiplicativa de $\mathbb{C}$ do ponto de vista geométrico é dada pela função conjugação como nos mostra a seguinte proposição:

Proposição 2.2.10. *Se z um número complexo, então $|z|^2 = z \cdot \overline{z}$.*

Prova. Digamos que $z = a + bi$. Então:

$$\begin{aligned} z \cdot \overline{z} &= (a + bi)(a - bi) \\ &= (a^2 + b^2) + (ab - ab)i \\ &= a^2 + b^2 \\ &= |z|^2. \end{aligned}$$

Assim, temos o desejado. □

Temos então por essa proposição que o comprimento de um vetor, que é um ente de natureza geométrico, pode ser traduzido em termos de multiplicação de números complexos. Uma primeira consequência dessa simples proposição é a compatibilidade da norma com o produto, como nos mostra o seguinte corolário.

Corolário 2.2.11. *Sejam z_1 e z_2 números complexos. Então $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.*

Prova. Pelo teorema acima temos

$$|z_1 \cdot z_2|^2 = (z_1 \cdot z_2)(\overline{z_1 \cdot z_2})$$

Usando a Proposição 2.2.4, tem-se

$$|z_1 \cdot z_2|^2 = (z_1 \cdot z_2) \cdot (\overline{z_1} \cdot \overline{z_2}) = (z_1 \cdot \overline{z_1})(z_2 \cdot \overline{z_2}) = |z_1|^2 \cdot |z_2|^2.$$

Assim,

$$\sqrt{|z_1 \cdot z_2|^2} = \sqrt{|z_1|^2 \cdot |z_2|^2},$$

ou seja,

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|.$$

□

Observação 2.2.12. O leitor conhecedor na noção de grupos facilmente observará que o corolário acima nos diz que a aplicação norma $|\quad| : \mathbb{C} - \{0\} \to \mathbb{R}_+$ é um homomorfismo do grupo multiplicativo dos complexos não nulos no grupo multiplicativo dos reais positivos. Perceberá também que o núcleo desse homomorfismo é a circunferência unitária centrada na origem.

Fixemos um número complexo unitário $u = \cos\theta + \operatorname{sen}\theta i$. Consideremos agora a aplicação

$$\begin{array}{rccc} \psi_u : & \mathbb{C} & \to & \mathbb{C} \\ & z & \mapsto & uz \end{array}$$

Notemos que

$$|\psi_u(z)| = |uz| = |u| \cdot |z| = |z|,$$

ou seja, ψ_u é uma aplicação que preserva norma. Dessa maneira, podemos dizer que ψ_u é uma *isometria planar*. Resta saber que tipo de isometria ψ_u é, ou seja, saber se ela é uma translação, reflexão ou rotação. No teorema a seguir detalhamos essa informação.

Teorema 2.2.13. *Seja $u = \cos\theta + \operatorname{sen}\theta i$ um número complexo. Então a aplicação ψ_u é a rotação de ângulo θ.*

Prova. Notemos que u pode ser escrito na forma

$$u = \cos\theta + \operatorname{sen}\theta i.$$

Dado $z \in \mathbb{C}$ também podemos escrevê-lo na forma

$$z = |z|(\cos\theta_z + \operatorname{sen}\theta_z i)$$

onde θ_z é o argumento de z. Desse modo, temos:

$$\begin{aligned}\psi_u(z) &= uz \\ &= |z|[(\cos\theta\cos\theta_z - \operatorname{sen}\theta\operatorname{sen}\theta_z) + (\cos\theta\operatorname{sen}\theta_z + \operatorname{sen}\theta\cos\theta_z)i] \\ &= |z|(\cos(\theta_z + \theta) + \operatorname{sen}(\theta_z + \theta)i).\end{aligned}$$

Esta última igualdade nos dá o resultado desejado. □

Observação 2.2.14. Notemos com este teorema que a multiplicação por complexo permite uma expressão compacta e simples para as rotações planares. Essa característica é fundamental na simplificação de várias equações vetoriais onde figure rotações planares.

A seguir mostramos um problema lúdico onde na solução levamos em consideração essa interpretação geométrica da multiplicação dos números complexos como rotações.

Exemplo 2.2.15 (**O Problema do Tesouro Perdido**)**.** No mapa do pirata constava que a ilha onde escondeu o tesouro era a única de um arquipélago, onde se encontravam *duas rochas e uma palmeira*. O proprietário do mapa, após encontrar a ilha, a palmeira e as duas rochas, deveria proceder da seguinte maneira:

(i) Contar os passos a partir da palmeira até a rocha que se encontra do seu lado esquerdo e, em seguida efetuar uma rotação de 90º à direita, contar novamente os mesmos passos e no final marcar o ponto x;

(ii) Retornar para a palmeira e caminhar contando os passos até a rocha que se encontra a sua direita e, em seguida efetuar uma rotação de 90º à esquerda e contar o mesmo número de passos, marcando no final o ponto y.

(iii) Por fim, o tesouro irá encontrar-se no ponto médio entre X e Y, que estará à direita das rochas.

O problema é que o proprietário do mapa, após encontrar a ilha verificou que não mais existia a palmeira. E então, como solucionar o problema e encontrar o tesouro?

Solução: Sejam R e Q as duas rochas existentes na ilha. Como o tesouro está à direita das rochas, suponhamos uma palmeira P num ponto aleatório do plano, à esquerda das rochas, como figura 2.2.

Figura 2.2: R - Rocha 1; Q - Rocha 2; P - Palmeira.
Fonte: Elaborada pelo autor.

Seguindo as orientações do mapa e realizando (i) e (ii) o portador do mapa deverá ter as coordenadas como na Figura 2.3.

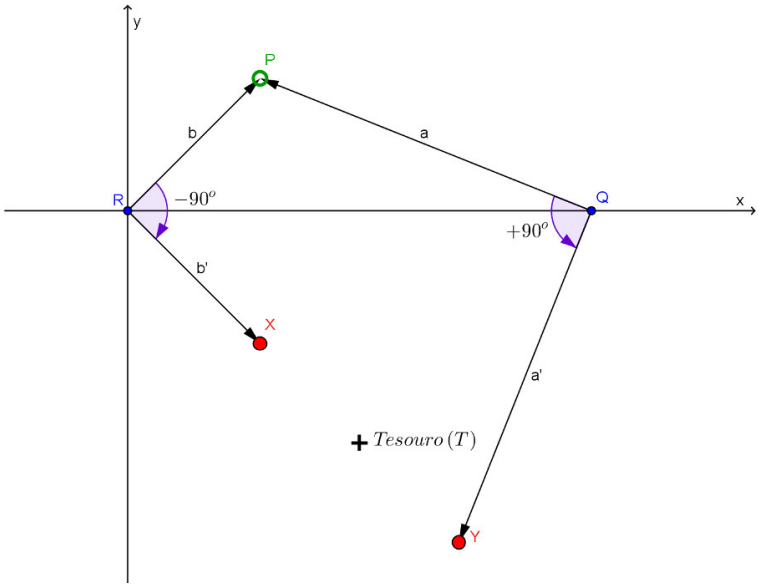


Figura 2.3: Mapa do Tesouro 1.
Fonte: Elaborada pelo autor.

Assim, o tesouro estará no ponto médio entre X e Y, como indica (iii) (Figura 2.4).

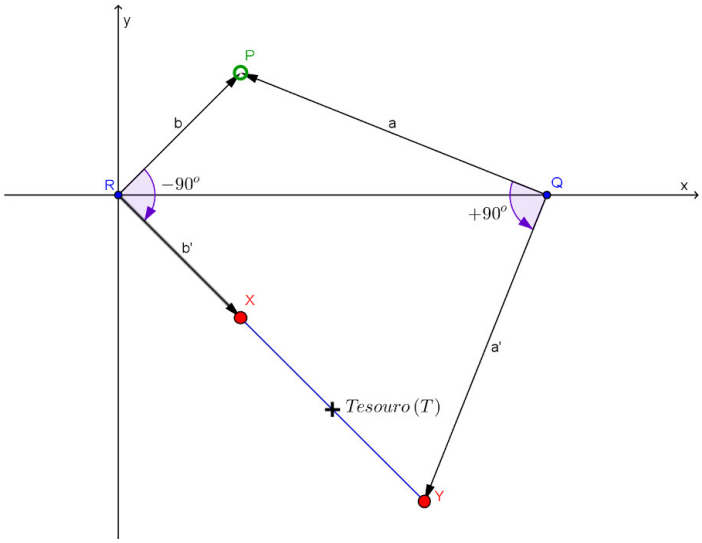


Figura 2.4: Mapa do Tesouro 2.
Fonte: Elaborada pelo autor.

As figuras ilustram facilmente o que o proprietário do mapa deveria fazer para ter posse do tesouro. Mas devido a palmeira ser inexistente torna-se complexa a missão de encontrá-lo. A não ser que o pirata fosse inteligente ao ponto de prever a extinção da planta! E ainda, encontrar o tesouro não dependia da posição ao qual a palmeira se encontrava.

De fato, se o pirata teve essa brilhante ideia estava correto. Da Figura 2.4 tem-se:

$$\begin{cases} \overrightarrow{RX} &= \overrightarrow{RP} \cdot (\cos(-90)^{\text{o}} + i \text{ sen}(-90)^{\text{o}}) \\ \overrightarrow{QY} &= \overrightarrow{QP} \cdot (\cos(90^{\text{o}}) + i \text{ sen}(90^{\text{o}})) \\ T &= \frac{X+Y}{2}. \end{cases}$$

Note que pelo Teorema 2.2.13, $\overrightarrow{RX}$ equivale a $\overrightarrow{RP}$ rotacionado de -90^{o} e $\overrightarrow{QY}$ equivale a $\overrightarrow{QP}$ rotacionado de 90^{o}.

Das relações acima obtemos:

$$(X - R) = (P - R) \cdot (-i); \tag{2.14}$$
$$(Y - Q) = (P - Q)i; \tag{2.15}$$
$$T = \frac{X + Y}{2}. \tag{2.16}$$

Daí, adicionando (2.14) e (2.15) membro a membro temos

$$X + Y - R - Q = (R - Q)i \tag{2.17}$$
$$X + Y = R + Q + \overrightarrow{QR}i. \tag{2.18}$$

De (2.16), segue

$$T = \frac{R + Q}{2} + \frac{\overrightarrow{QR}}{2}i \tag{2.19}$$

Portanto, o tesouro pode ser encontrado de modo independente da existência da palmeira, de acordo com a fórmula 2.19, como mostra a Figura 2.5.

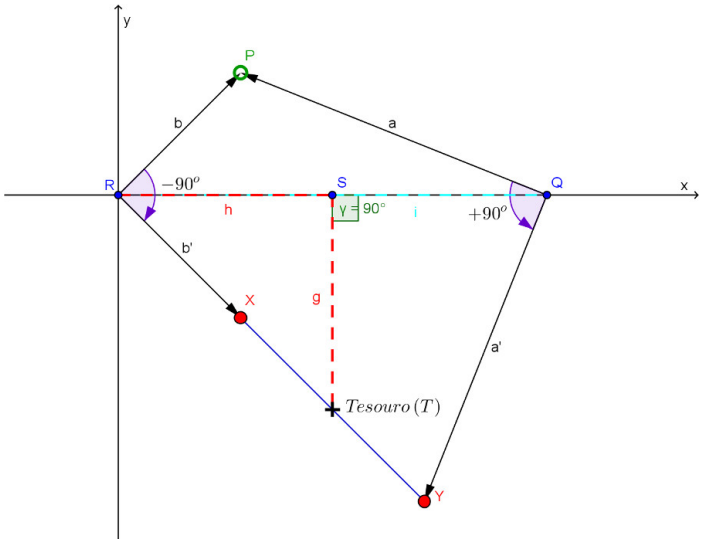


Figura 2.5: Mapa do Tesouro 3.
Fonte: Elaborada pelo autor.

Note ainda que para chegar ao tesouro basta o herdeiro do mapa seguir o caminho destacado em vermelho na figura 2.5, explícito na fórmula (2.19). □

Capítulo 3

Os quatérnios de Hamilton

Acompanhamos nas páginas anteriores a evolução da noção de número. A síntese dessa evolução é dada pela cadeia de inclusões abaixo:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Vimos que em cada nova classe de números que surgia, esta estendia a anterior e todas as propriedades aritméticas e algébricas eram preservadas. Por exemplo, ao estendermos $\mathbb{N}$ para $\mathbb{Z}$, propriedades como associatividade, comutatividade, existência de elemento neutro, etc, antes válidas para $\mathbb{N}$ também continuam válidas para $\mathbb{Z}$. Nesse processo sucessivo, cada novo objeto também passa a ter propriedades extras e que suprem deficiências da classe anterior (e.g, em $\mathbb{R}$ nem toda equação polinomial, em uma variável, contém solução, mas em $\mathbb{C}$ sim).

Uma vantagem desse processo é que em cada passo, a nova classe obtida também permite um melhor entendimento da classe anterior (e.g., vide Observação 2.2.9).

A pergunta natural é se esse processo de extensão sucessiva pode ser continuado depois de $\mathbb{C}$, ou seja, existe uma nova classe de números contendo $\mathbb{C}$ de tal modo que todas as suas propriedades aritméticas sejam válidas? O objetivo deste capítulo é responder a esta questão e introduzir os chamados números de Hamilton, também conhecidos como números hipercomplexos.

3.1 Unicidade de $\mathbb{C}$

A fim de tornar mais preciso o que discutiremos na sequência, fazemos algumas definições prévias.

Definição 3.1.1. Chamaremos de *extensão* de $\mathbb{R}$ a um conjunto $\mathbb{K}$ contendo $\mathbb{R}$, equipado com operações $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ e $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$, satisfazendo às seguintes propriedades:

(a) As operações $+$ e $\cdot$ de $\mathbb{K}$ quando restritas a $\mathbb{R}$ coincidem com a adição e multiplicação usual de $\mathbb{R}$.

(b) Quaisquer que sejam $a, b, c \in \mathbb{K}$ tem-se $(a + b) + c = a + (b + c)$.

(c) Quaisquer que sejam $a,\ b \in \mathbb{K}$, $a + b = b + a$.

(d) $0 \in \mathbb{R}$ é tal que para qualquer $a \in \mathbb{K}$, $0 + a = a$.

(e) Para cada $a \in \mathbb{K}$ existe $-a \in \mathbb{K}$ tal que $a + (-a) = 0$.

(f) Quaisquer que sejam $a, b, c \in \mathbb{K}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(g) $1 \in \mathbb{R}$ é tal que $a \cdot 1 = 1 \cdot a = a$ para qualquer $a \in \mathbb{K}$.

(h) Quaisquer que sejam $a, b, c \in \mathbb{K}$, $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(b+c) \cdot a = b \cdot a + c \cdot a$.

Dizemos que $\mathbb{K}$ é uma extensão *comutativa* se a multiplicação de $\mathbb{K}$ é comutativa, ou seja, $a \cdot b = b \cdot a$ para qualquer $a, b \in \mathbb{K}$.

Exemplo 3.1.2. O exemplo canônico de extensão de $\mathbb{R}$ é obviamente o corpo dos complexos $\mathbb{C}$.

Na sequência, apresentamos outros exemplos de extensões de $\mathbb{R}$ que são de certa forma inspirados na construção de Hamilton para os números complexos, na qual cada número complexo é pensado como um vetor do plano. Analogamente, nos exemplos abaixo veremos que cada elemento da extensão considerada será visto como vetor de um espaço vetorial apropriado.

Exemplo 3.1.3. Considere o conjunto

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

ou seja, $\mathbb{K}$ é o conjunto das matrizes quadradas de ordem 2 com entradas em $\mathbb{R}$. Se pensarmos $\mathbb{K}$ com suas operações usuais de adição e multiplicação de matrizes e identificarmos cada número real a com a matriz $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ temos que $\mathbb{K}$ é uma extensão de $\mathbb{R}$. Como é bem sabido, $\mathbb{K}$ assim definida não é uma extensão comutativa.

Exemplo 3.1.4. Considere o conjunto $\mathbb{K} = \{(a, b) \mid a, b \in \mathbb{R}\}$ equipado com operações $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ e $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ definidas pelas seguintes igualdades:

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

$$(a, b) \cdot (c, d) = (a \cdot c, a \cdot d + b \cdot c).$$

Verificamos que para elementos $(a, 0), (c, 0) \in \mathbb{K}$ temos

$$(a, 0) + (c, 0) = (a + c, 0)$$

e

$$(a, 0) \cdot (c, 0) = (a \cdot c, 0).$$

Essas igualdades permitem que possamos identificar o número real a com o par $(a, 0)$. Como podemos notar, $\mathbb{K}$ satisfaz o item (a) da definição de extensão. Uma verificação direta nos mostra que $\mathbb{K}$ com as operações acima definidas também satisfaz as propriedades (b)-(h) elencadas na definição acima bem como a comutatividade da multiplicação. Portanto, $\mathbb{K}$ é uma extensão comutativa de $\mathbb{R}$.

Observamos que a extensão exibida no exemplo acima apresenta muitas semelhanças com a extensão $\mathbb{C}$. Contudo, uma diferença fundamental ocorre no que diz respeito aos chamados *divisores de zero*.

Definição 3.1.5. Seja $\mathbb{K}$ uma extensão de $\mathbb{R}$. Um elemento $a \in \mathbb{K}$, diferente de zero, é dito um *divisor de zero à direita* (resp. à esquerda) se existe um elemento $b \in \mathbb{K}$ não nulo tal que $b \cdot a = 0$ (resp. $a \cdot b = 0$). Se $a \in \mathbb{K}$ é divisor de zero à direita e à esquerda dizemos simplesmente que a é *divisor de zero*.

Observe que em $\mathbb{C}$, se $a, b \in \mathbb{C}$ são não nulos então $a \cdot b \neq 0$. Contudo, no exemplo 3.1.4 temos $(0, 1) \in \mathbb{K}$ diferente de zero e $(0, 1) \cdot (0, 1) = (0, 0)$. Ou seja, $\mathbb{C}$ não admite divisores de zero não nulos, enquanto $\mathbb{K}$ sim. Essa é a diferença fundamental citada acima.

Obviamente, a distinção em divisor de zero à direita ou à esquerda só faz sentido para extensões de $\mathbb{R}$ não comutativas, uma vez que no caso comutativo as duas noções coincidem.

Observação 3.1.6. O leitor experiente com a noção de espaço vetorial deve notar facilmente que uma extensão $\mathbb{K}$ de $\mathbb{R}$ tem naturalmente estrutura de espaço vetorial

sobre $\mathbb{R}$. Existe um resultado geral que diz que se $\mathbb{K}$ tem dimensão finita como espaço vetorial sobre $\mathbb{R}$ então todo divisor de zero à direita é também divisor de zero à esquerda. Assim, nos exemplos 3.1.3 e 3.1.4 acima não temos a distinção entre divisor de zero à esquerda ou à direita, sendo que o primeiro justifica-se por esse resultado e o segundo pelo fato da extensão ser comutativa. Doravante estaremos interessados apenas em extensões que sejam de dimensão finita sobre $\mathbb{R}$, por isso, em virtude do resultado supracitado utilizaremos apenas o adjetivo divisor de zero.

Do ponto de vista algébrico, duas estruturas algébricas são a "mesma" quando existe uma correspondência bijetora entre elas e que preserva suas operações. No contexto das extensões de $\mathbb{R}$, tais correspondências são definidas como abaixo.

Definição 3.1.7. Sejam $\mathbb{K}$ e $\mathbb{K}'$ extensões de $\mathbb{R}$. Uma aplicação $\varphi : \mathbb{K} \to \mathbb{K}'$ é dita um *isomorfismo* de $\mathbb{K}$ em $\mathbb{K}'$ se:

(a) φ é bijetora.

(b) φ restrita a $\mathbb{R}$ é a aplicação identidade de $\mathbb{R}$.

(c) $\varphi(a+b) = \varphi(a) + \varphi(b)$.

(d) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Duas extensões de $\mathbb{R}$ são ditas *isomorfas* quando existe um isomorfismo entre elas.

Notação: Se $\mathbb{K}$ e $\mathbb{K}'$ são extensões de $\mathbb{R}$ isomorfas então simbolizamos este fato escrevendo $\mathbb{K} \simeq \mathbb{K}'$.

Observação 3.1.8. Notemos que se $\varphi : \mathbb{K} \to \mathbb{K}'$ é um isomorfismo entre duas extensões de $\mathbb{R}$ então esta φ é, em particular, um isomorfismo de espaços vetoriais sobre $\mathbb{R}$. Assim, $\mathbb{K}$ e $\mathbb{K}'$ serem isomorfos como espaços vetoriais é condição necessária para serem isomorfos como extensões de $\mathbb{R}$. Todavia, não é condição suficiente. Por exemplo, $\mathbb{C}$ e a extensão $\mathbb{K}$ do Exemplo 3.1.4 são isomorfas como espaços vetoriais mas não o são como extensão de $\mathbb{R}$.

Definição 3.1.9. Seja $\mathbb{K}$ um extensão de $\mathbb{R}$. Um elemento α de $\mathbb{K}$ é dito *algébrico* sobre $\mathbb{R}$ se existe um polinômio não-nulo em uma variável com coeficientes em $\mathbb{R}$ que é anulado quando avaliado em α. Se todo elemento de $\mathbb{K}$ é algébrico sobre $\mathbb{R}$ então dizemos que a extensão $\mathbb{K}$ é *algébrica* sobre $\mathbb{R}$.

Exemplo 3.1.10. Afirmamos que $\mathbb{C}$ é uma extensão algébrica de $\mathbb{R}$. Para verificar essa afirmação consideremos $\alpha \in \mathbb{C}$. Temos que o polinômio $f(x) = (x - \overline{\alpha}) \cdot (x - \alpha)$ é anulado por α. Por outro lado, ao efetuarmos o produto tem-se $f(x) = x^2 + 2\mathrm{Re}(\alpha) + |\alpha|^2$, ou seja, os coeficientes de f são reais. Portanto, α é algébrico sobre $\mathbb{C}$ e a afirmação segue.

Exemplo 3.1.11. Mais geralmente, se $\mathbb{K}$ é uma extensão de $\mathbb{R}$ que, pensada como espaço vetorial sobre $\mathbb{R}$, tem dimensão finita, então $\mathbb{K}$ é algébrica sobre $\mathbb{R}$. Para ver essa afirmação, considere $\alpha \in \mathbb{K}$. Seja n a dimensão vetorial de $\mathbb{K}$ como espaço vetorial sobre $\mathbb{R}$. O conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ possui $n + 1$ elementos, logo, é um conjunto linearmente dependente. Assim, deve existir uma combinação $a_0 \cdot 1 + a_1 \cdot \alpha + \ldots + a_n \cdot \alpha^n = 0$, com $a_0, \ldots, a_n \in \mathbb{R}$ não todos nulos. Assim, $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ é um polinômio não nulo com coeficientes reais que é anulado quando avaliado em α. Portanto, α é algébrico sobre $\mathbb{R}$.

Temos agora o principal resultado dessa seção.

Teorema 3.1.12. *Seja $\mathbb{K}$ uma extensão de $\mathbb{R}$ comutativa e sem divisores de zero. Suponhamos que cada elemento de $\mathbb{K}$ é algébrico sobre $\mathbb{R}$. Então $\mathbb{K}$ é isomorfo a $\mathbb{C}$.*

Prova. Primeiro provaremos a seguinte afirmação:

Afirmação 1: *Para cada $u \in \mathbb{K} - \mathbb{R}$, existe um polinômio f de grau 2 com coeficientes em $\mathbb{R}$ tal que $f(u) = 0$.*

Para provar essa afirmação usaremos o fato de que se um polinômio com coeficientes reais é irredutível então ele tem que ter grau 1 ou 2.

Considere f o polinômio com coeficientes reais de menor grau possível tal que $f(u) = 0$. Este polinômio existe por conta da extensão $\mathbb{K}$ ser algébrica e pelo princípio da boa ordenação. Afirmamos que f é irredutível. Para verificar isso, suponhamos o contrário. Então isso significaria que

$$f(X) = g(X) \cdot h(X)$$

com $g(X)$ e $h(X)$ sendo polinômios não constantes e com grau menor que o de f. Assim,

$$0 = f(u) = g(u) \cdot h(u).$$

Como $\mathbb{K}$ não tem divisores de zero, então $g(u) = 0$ ou $h(u) = 0$. Mas $g(u) = 0$ ou $h(u) = 0$ nos leva a contradição, pois f é o polinômio com coeficientes reais de

grau mínimo com a propriedade de ter u como raiz. Assim, segue que realmente f é irredutível. Pelo comentário feito no início da prova da afirmação segue que f tem grau 1 ou 2. De fato, f não pode ter grau 1 pois caso contrário u pertenceria a $\mathbb{R}$. Logo, f é um polinômio de grau 2.

Agora fixemos um $u \in \mathbb{K} - \mathbb{R}$. Pela Afirmação 1 temos um polinômio com coeficientes reais $f(X) = ax^2 + bx + d$ $(a \neq 0)$ tal que $f(u) = au^2 + bu + d = 0$. Logo, temos a igualdade

$$u^2 = \alpha u + \beta \tag{3.1}$$

onde $\alpha = -\frac{b}{a}$ e $\beta = -\frac{d}{a}$.

Consideremos agora o elemento $v = u - \frac{\alpha}{2}$ (note que v também não pertence a $\mathbb{R}$, pois caso contrário u também pertenceria $\mathbb{R}$). Temos:

$$\begin{aligned} v^2 &= (u - \frac{\alpha}{2})^2 && (3.2)\\ &= u^2 - \alpha u + \frac{\alpha^2}{4} && (3.3)\\ &= \alpha u + \beta - \alpha u + \frac{\alpha^2}{4} && (3.4)\\ &= \beta + \frac{\alpha^2}{4} && (3.5) \end{aligned}$$

o que implica que v^2 pertence a $\mathbb{R}$ (notemos que da igualdade (3.2) para a igualdade (3.3) foi utilizado a comutatividade de $\mathbb{K}$). Como v não pertence a $\mathbb{R}$ então devemos ter $r := \beta + \frac{\alpha^2}{4}$ negativo. Assim, existe um número real s tal que $s^2 = -\frac{1}{r}$. Definindo $w = sv$ temos $w^2 = -1$ e $w \in \mathbb{K} - \mathbb{R}$.

Considere agora o espaço vetorial V sobre $\mathbb{R}$ gerado por 1 e w. Este é um espaço vetorial de dimensão 2. Além disso, dados $\gamma + \theta w, \gamma' + \theta' w \in V$ temos

$$(\gamma + \theta w)(\gamma' + \theta' w) = (\gamma\gamma' - \theta\theta') + (\gamma\theta' + \gamma'\theta)w \tag{3.6}$$

ou seja, o produto de dois elementos de V é também um elemento de V. Com isso segue que as operações de $\mathbb{K}$ quando restritas a V fazem de V uma extensão de $\mathbb{R}$.

Afirmação 2: *A aplicação $\varphi : \mathbb{C} \to V$ definida por $\varphi(\gamma + \theta i) = \gamma + \theta w$ é um isomorfismo de $\mathbb{C}$ em V.*

De fato temos:

$$\varphi(1) = \varphi(1 + 0i) = 1 + 0w = 1,$$

$$\begin{aligned}\varphi((\gamma + \theta i) + (\gamma' + \theta' i)) &= \varphi((\gamma + \gamma') + (\theta + \theta')i) \\ &= (\gamma + \gamma') + (\theta + \theta')w \\ &= (\gamma + \theta w) + (\gamma' + \theta')w \\ &= \varphi(\gamma + \theta i) + \varphi(\gamma' + \theta' i)\end{aligned}$$

e

$$\begin{aligned}\varphi((\gamma + \theta i) \cdot (\gamma' + \theta' i)) &= \varphi((\gamma\gamma' - \theta \cdot \theta') + (\gamma\theta' + \gamma'\theta)i) \\ &= (\gamma\gamma' - \theta \cdot \theta') + (\gamma\theta' + \gamma'\theta)w \\ &= (\gamma + \theta w) \cdot (\gamma' + \theta' w) \\ &= \varphi(\gamma + \theta i) \cdot \varphi(\gamma' + \theta' i).\end{aligned}$$

Logo, para mostrar que é isomorfismo resta provar que φ é bijetora. Para isso, considere a aplicação $\psi : V \to \mathbb{C}$ definida por $\psi(\gamma + \theta w) = \gamma + \theta i$. Temos

$$\varphi \circ \psi(\gamma + \theta w) = \varphi(\psi(\gamma + \theta w)) = \varphi(\gamma + \theta i) = \gamma + \theta w$$

e

$$\psi \circ \varphi(\gamma + \theta i) = \psi(\varphi(\gamma + \theta i)) = \psi(\gamma + \theta w) = \gamma + \theta i.$$

Segue dessas igualdades que ψ é uma inversa a direita e a esquerda de φ. Logo, φ é bijetora. Portanto, φ é um isomorfismo.

Até agora temos $V \simeq \mathbb{C}$. Mas desejamos mostrar que $\mathbb{K} \simeq \mathbb{C}$. Para isso deduziremos que $V = \mathbb{K}$.

Considere $v \in \mathbb{K}$. Seja f um polinômio não constante com coeficientes reais que tem v como raiz. Note que o fato de V ser isomorfo a $\mathbb{C}$, implica pelo teorema fundamental da álgebra, que f se fatora na forma

$$f(X) = a(X - r_1) \cdot \ldots \cdot (X - r_n),$$

onde n é o grau de f, a o coeficiente líder de f e $r_1, \ldots, r_n \in V$. Temos assim que

$$a(v - r_1) \cdot \ldots \cdot (v - r_n) = 0.$$

Como $\mathbb{K}$ não tem divisores de zero segue que $v - r_i = 0$ para algum $1 \leq i \leq n$. Logo, $v = r_i \in V$. Portanto, temos a igualdade desejada. □

3.2 O surgimento dos Quatérnios

Em meados do século XIX surgiram descobertas que revolucionaram a álgebra. Durante séculos esta era vista apenas como aritmética simbólica, ou seja, utilizava-se letras ao invés de números específicos, como em aritmética.

Vimos anteriormente que o matemático William Rowan Hamilton $(1805 - 1865)$ foi o precursor na representação dos números complexos por pontos no plano, isto é, por pares ordenados (x, y) de números reais. Essa generalização deu um grande impulso às pesquisas e a busca por novas descobertas, mas não o quanto estava por vir através de sua pessoa.

Ao considerar a tripla ordenada (x, y, z), Hamilton tentou generalizar sua ideia para o sistema de três dimensões. Assim, buscou definir a adição e a multiplicação, como nos pares ordenados já mencionados em (2.12) e (2.13). Nessa analogia, interpretando (a, b, c) como sendo $a + bi + cj$ com $i^2 = j^2 = -1$, efetuar a soma de duas ou mais triplas seria tarefa fácil. De fato, se $z = a + bi + cj$ e $z' = a' + b'i + c'j$, então

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

O problema residia em multiplicar triplas como números complexos, pois produz o termo ij. De fato,

$$\begin{aligned} z \cdot z' &= (a + bi + cj) \cdot (a' + b'i + c'j) && (3.7)\\ &= aa' + ab'i + ac'j + ba'i + bb'i^2 + bc'ij + ca'j + cb'ji + cc'j^2 && (3.8)\\ &= (aa' - bb' - cc') + (ab' + ba')i + (ac' + a'c)j + (bc' + b'c)ij. && (3.9) \end{aligned}$$

Mas o que poderiam ser os termos ij? Por muitos anos Hamilton procurou essa resposta sem lograr êxito.

Notemos que, em virtude do Teorema 3.1.12 (ver também Observação 3.1.8 e Exemplo 3.1.11), nenhuma multiplicação poderia ser conferida a $\mathbb{R}^3$ de modo a fazê-lo uma extensão de $\mathbb{R}$ comutativa e sem divisores de zero.

Consta nos relatos históricos que em 1843, num momento de inspiração, ao invés de aceitar apenas ternos ordenados, Hamilton considerou quádruplos ordenados, isto

é, usando i e j, e mais um terceiro número imaginário k, com $i^2 = j^2 = k^2 = -1$, criou

$$a + bi + cj + dk, \tag{3.10}$$

com a, b, c e $d \in \mathbb{R}$. A estes elementos, Hamilton denominou de *quatérnios*.

Nesta representação

$$1 := (1, 0, 0, 0),\ i := (0, 1, 0, 0),\ j := (0, 0, 1, 0) \text{ e } k := (0, 0, 0, 1). \tag{3.11}$$

Além das relações $i^2 = j^2 = k^2 = -1$, Hamilton também estipulou que

$$ij = k = -ji,\ jk = i = -kj,\ ki = j = -ik, \tag{3.12}$$

A Figura 3.1 nos dá uma boa associação com as relações (3.12)

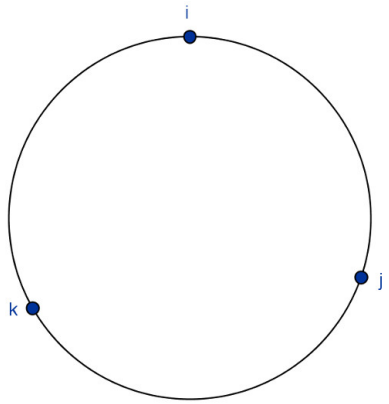


Figura 3.1: Círculo de Relações Imaginárias.
Fonte: Elaborada pelo autor.

Seguindo o círculo no sentido horário, o produto de dois é sempre o terceiro. Seguindo o círculo no sentido anti-horário o produto de dois é menos o terceiro.

Mediante as relações acima citadas, para $z = a+bi+cj+dk$ e $z' = a'+b'i+c'j+d'k$, temos

$$z \cdot z' = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' + a'c - bd' db')j + (ad' + da' + bc' - cb')k \tag{3.13}$$

É de fácil verificação que $\mathbb{R}^4$ com a operação de adição natural e com a multiplicação dada em (3.13) é uma extensão de $\mathbb{R}$. Esta extensão de $\mathbb{R}$ é chamada de *álgebra de quatérnios* e é denotada por $\mathbb{H}$.

Pelas relações (3.12) segue imediatamente que $\mathbb{H}$ não é comutativa.

> Hamilton contava que a história de abandonar a lei comutativa da multiplicação ocorreu-lhe num átimo, após quinze anos de cogitações infrutíferas, enquanto caminhava com a esposa ao longo do Royal Canal perto de Dublin, pouco antes do escurecer. Essa idéia tão pouco ortodoxa impressionou-o tanto que pegou de seu canivete e com ele gravou a parte fundamental da tábua de multiplicação dos quatérnios numa das pedras da Ponte de Broughm (EVES, 2004, p.551).

Como podemos facilmente observar, temos a seguinte decomposição para $\mathbb{H}$

$$\mathbb{H} = \mathbb{R} \oplus \mathrm{Im}(\mathbb{H})$$

onde

$$\mathrm{Im}(\mathbb{H}) := \{bi + cj + dk \mid b, c, d \in \mathbb{R}\}$$

Em analogia com os complexos, os elementos de $\mathrm{Im}(\mathbb{H})$ são chamados *imaginários puros*. Naturalmente, também temos $\mathbb{C} \subset \mathbb{H}$.

3.3 A geometria dos Quatérnios

Como visto anteriormente, Hamilton conseguiu estatelecer uma multiplicação em $\mathbb{R}^4$ que imitava a multiplicação de números complexos. Uma "deficiência" dessa multiplicação era a não comutatividade. Todavia, uma boa propriedade de $\mathbb{H}$ é que podemos definir uma conjugação que possui propriedades semelhantes a conjugação em $\mathbb{C}$. De fato, dado um quatérnio

$$z = a + bi + cj + dk$$

definimos seu *conjugado*, denotato $\overline{z}$, por

$$\overline{z} = a - bi - cj - dk.$$

Temos então o seguinte resultado contendo propriedades da conjugação em $\mathbb{H}$

Teorema 3.3.1. *Sejam $z, z' \in \mathbb{H}$. A conjugação de $\mathbb{H}$ satisfaz as seguintes condições:*

(a) $z = \overline{z}$ *se, e somente se,* $z \in \mathbb{R}$.

(b) $\overline{\overline{z}} = z$

(c) $z\overline{z} = a^2 + b^2 + c^2 + d^2 = |z|^2$.

(d) $\overline{z \cdot z'} = \overline{z'} \cdot \overline{z}$ (*note aqui a ordem dos fatores do lado direito da igualdade*).

(e) $|z \cdot z'| = |z| \cdot |z'|$

Prova. Digamos que $z = a + bi + cj + dk$ e que $z' = a' + b'i + c'j + d'k$.

(a) $z = \overline{z} \Leftrightarrow a + bi + cj + dk = a - bi - cj - dk \Leftrightarrow a = a,\ b = -b,\ c = -c,\ d = -d \Leftrightarrow a = a,\ b = c = d = 0 \Leftrightarrow z = a \Leftrightarrow z \in \mathbb{R}$. Portanto, temos a equivalência desejada.

(b) Segue das seguintes igualdades

$$\begin{aligned} \overline{\overline{z}} &= \overline{\overline{a - bi - cj - dk}} && (3.14)\\ &= a - (-b)i - (-c)j - (-d)k && (3.15)\\ &= a + bi + cj + dk = z. && (3.16) \end{aligned}$$

(c) e (d) seguem imediatamente utilizando-se a fórmula do produto (3.13).

(e) Temos,

$$\begin{aligned} |z \cdot z'|^2 &= (z \cdot z')(\overline{z \cdot z'}) && (3.17)\\ &= (z \cdot z')(\overline{z'} \cdot \overline{z}) && (3.18)\\ &= z(z' \cdot \overline{z'})\overline{z} && (3.19)\\ &= |z'|^2 z \cdot \overline{z} && (3.20)\\ &= |z|^2 |z'|^2 && (3.21) \end{aligned}$$

Portanto, $|z \cdot z'| = |z| \cdot |z'|$ como desejávamos. □

Embora $\mathbb{H}$ seja não comutativa, uma outra propriedade aritmética bastante importante ocorre, como nos revela o seguinte teorema.

Teorema 3.3.2. *Todo elemento não nulo de $\mathbb{H}$ possui inverso multiplicativo. Em particular, $\mathbb{H}$ não contém divisor de zero não nulo.*

Prova. Seja $z \in \mathbb{H}$ não nulo. Temos que $|z| \neq 0$. Como $z \cdot \overline{z} = |z|^2$ segue que $z \cdot (|z|^{-2}\overline{z}) = 1$. Portanto, z é invertível. □

Para cada $u \in \mathbb{H}$ unitário, considere a aplicação

$$\begin{array}{rccc} \psi_u : & \mathbb{H} & \to & \mathbb{H} \\ & z & \mapsto & u \cdot z \cdot u^{-1} \end{array}$$

(observemos pela prova do teorema 3.3.2 que u^{-1} é também unitário).

Notemos que, em virtude do Teorema 3.3.1 (e), a aplicação ψ_u é uma isometria.

No teorema a seguir veremos como utilizar as aplicações ψ_u para representar as rotações de $\mathbb{R}^3$ de forma compacta e elegante. Para isso, identificaremos $\mathbb{R}^3$ com $\mathrm{Im}(\mathbb{H})$. Outro fato que utilizaremos é que dado um quatérnio unitário $u = a + bi + cj + dk$ temos

$$a^2 + (b^2 + c^2 + d^2) = 1;$$

assim, existe $\theta \in \mathbb{R}$ tal que $\cos\theta = a$ e $\operatorname{sen}\theta = |v|$ (onde $v = (b, c, d)$); logo,

$$u = \cos\theta + \operatorname{sen}\theta u'$$

como $u' = \frac{v}{|v|} \in \mathrm{Im}(\mathbb{H})$ é unitário.

Teorema 3.3.3. *Seja $u = \cos\theta + \operatorname{sen}\theta u' \in \mathbb{H}$ um quatérnio unitário escrito como na representação acima. Então, a aplicação ψ_u restrita a $\mathrm{Im}(\mathbb{H})$ corresponde a rotação de um ângulo θ em torno do eixo gerado pelo vetor u'.*

Prova. Ver [3, Capítulo 7]. □

3.3.1 Campos de Vetores na esfera de $\mathbb{R}^4$

A *esfera* em $\mathbb{R}^n$ é o conjunto de todos os vetores que possuem norma 1, o qual denotamos por $\mathbb{S}^{n-1}$. Um vetor v é tangente a $\mathbb{S}^n$ em um ponto $p \in \mathbb{S}^{n-1}$ se $\langle v, p\rangle = 0$, onde $\langle\ ,\ \rangle$ é o produto interno canônico de $\mathbb{R}^n$. Um *campo de vetores* sobre $\mathbb{S}^{n-1}$ é uma função f que associa a cada ponto p de $\mathbb{S}^{n-1}$ um vetor tangente $f(p)$ a $\mathbb{S}^{n-1}$ em p. Quando a função f é contínua, dizemos que f é um campo de vetores contínuo sobre $\mathbb{S}^{n-1}$.

Exemplo 3.3.4. Para cada ponto $(u_1, u_2) \in \mathbb{S}^1$, defina $f(u_1, u_2) = (u_2, -u_1)$. Temos que esta aplicação f é um campo de vetores contínuo sobre a esfera $\mathbb{S}^1$.

Definição 3.3.5. Seja f um campo de vetores sobre a esfera $\mathbb{S}^{n-1}$. Um ponto $p \in \mathbb{S}^{n-1}$ é chamado *ponto de singularidade* de f se $f(p) = 0$.

O campo de vetores do Exemplo 3.3.4 não possui singularidades. Um famoso resultado da topologia afirma que tal fenômeno não ocorre para esferas de $\mathbb{R}^3$. Precisamente

Teorema 3.3.6 (Teorema da esfera cabeluda). *Todo campo de vetores contínuo sobre a esfera $\mathbb{S}^2$ possui um ponto de singularidade.*

O que podemos dizer então da esfera de $\mathbb{R}^4$? No teorema a seguir nos apropriamos da multiplicação de $\mathbb{H}$ para responder essa questão.

Teorema 3.3.7. *A esfera $\mathbb{S}^3$ admite três campos de vetores f_1, f_2, f_3 tal que em cada ponto $p \in \mathbb{S}^3$ tem-se $\{f_1(p), f_2(p), f_3(p)\}$ formando um conjunto linearmente independente.*

Prova. Para cada $p = (x, y, z, w) = x + yi + zj + wk \in \mathbb{S}^3$ afirmamos que p, pi, pj, pk formam um conjunto linearmente independente. Essa afirmação é consequência do fato que a aplicação $\psi_p : \mathbb{H} \to \mathbb{H}$ definida por $\psi_p(z) = p \cdot z$ é um isomorfismo de espaços vetoriais. Ortogonalizando a base $\{p, pi, pj, pk\}$ vem a base ortogonal

$$\mathcal{B} = \{p, pi - \langle pi, p\rangle p, pj - \langle pj, p\rangle p - \langle pj, pi\rangle pi, pk - \langle pk, p\rangle p - \langle pk, pi\rangle pi - \langle pk, pj\rangle pj\}$$

Defina agora f_1, f_2, f_3 pelas seguintes regras

$$f_1(p) = pi - \langle pi, p\rangle p,$$

$$f_2(p) = pj - \langle pj, p\rangle p - \langle pj, pi\rangle pi,$$

e

$$f_3(p) = pk - \langle pk, p\rangle p - \langle pk, pi\rangle pi - \langle pk, pj\rangle pj,$$

ou seja $\{p, f_1(p), f_2(p), f_3(p)\}$ é justamente a base ortogonal $\mathcal{B}$. Segue dessa maneira que f_1, f_2, f_3 são campos de vetores sobre $\mathbb{S}^3$ satisfazendo a propriedade de

que $\{f_1(p), f_2(p), f_3(p)\}$ forma um conjunto linearmente independente. Resta mostrar que estes campos são contínuos. Mas isso é imediato pois f_1, f_2, f_3 são somas e produtos de funções contínuas. □

Observe que esse teorema é bem mais forte do que afirmar a existência de um campo contínuo sem singularidades. De fato ele fornece 3 campos com a propriedade de serem linearmente independentes em cada ponto. Além disso, se desenvolvermos as expressões dos f_i obtidas na demonstração do teorema, podemos observar que os campos são mais que contínuos, são de fato campos polinomiais, ou seja, campos em que as funções coordenadas são polinômios.

3.4 Unicidade de $\mathbb{H}$

Definição 3.4.1. Seja $\mathbb{K}$ uma extensão de $\mathbb{R}$. Três elementos $u, v, w \in \mathbb{K}$ formam um *tripla Hamiltoniana* se satisfazem as nove condições de Hamilton, i.e., a tabela de multiplicação para estes elementos é:

$\cdot$	u	v	w
u	-1	w	$-v$
v	$-w$	-1	u
w	v	$-u$	-1

Dada uma extensão $\mathbb{K}$ de $\mathbb{R}$, considere

$$\mathrm{Im}(\mathbb{K}) = \{v \in \mathbb{K} \mid v^2 \in \mathbb{R} \text{ e } v \notin \mathbb{R} \setminus 0\}. \tag{3.22}$$

O conjunto $\mathrm{Im}(\mathbb{K})$ se diz *parte imaginária de* $\mathbb{K}$. Claramente

$$\mathbb{R} \cap \mathrm{Im}(\mathbb{K}) = \{0\}$$

e se $v \in \mathrm{Im}(\mathbb{K})$, então $\alpha v \in \mathrm{Im}(\mathbb{K})$ para cada $\alpha \in \mathbb{R}$. A terminologia é baseada na observação que no caso $\mathbb{K} = \mathbb{C}$ ou $\mathbb{H}$, existe um espaço de vetores *imaginários*, no sentido que se $v \notin \mathbb{R}$, então $v^2 \in \mathbb{R}$.

Proposição 3.4.2. *Seja $\mathbb{K}$ uma extensão de $\mathbb{R}$.*

(a) *Se $u, v \in \mathrm{Im}(\mathbb{K})$ são linearmente independentes, então $1, u$ e v são linearmente independentes.*

(b) *Se* $u, v, u+v \in \mathrm{Im}(\mathbb{K})$*, então*

$$u \cdot v + v \cdot u \in \mathbb{R}; \tag{3.23}$$

(c) *Se* $\mathbb{K}$ *não tem divisores de zero, então para cada elemento* $v \in \mathrm{Im}(\mathbb{K})$ *temos* $v^2 = -\omega$ *com* $\omega > 0$*. Em particular, se* $\mathrm{Im}(\mathbb{K}) \neq \emptyset$ *então existe* $u \in \mathrm{Im}(\mathbb{K})$ *tal que* $u^2 = -1$*.*

(d) *Se* $u, v, w \in \mathbb{K}$ *é uma tripla Hamiltoniana, então a transformação linear de*

$$\varphi : \mathbb{H} \to \mathbb{K}$$

definido por $\varphi(1) = 1$*,* $\varphi(i) = u$*,* $\varphi(j) = v$*,* $\varphi(k) = w$ *é injetora e o subespaço* $\langle u, v, w\rangle$ *está contido em* $\mathrm{Im}(\mathbb{K})$*.*

Prova. (a) Suponhamos que $v = \alpha + \beta u$, com $\alpha, \beta \in \mathbb{R}$. Teremos

$$2\alpha\beta u = v^2 - \alpha^2 - \beta^2 u^2 \in \mathbb{R}.$$

Portanto, $\alpha\beta = 0$, pela definição de elemento puramente imaginário. Pela hipótese, $\alpha \neq 0$ porque u e v são linearmente independentes. Assim, $\beta = 0$. Isso por sua vez implica que $v \notin \mathrm{Im}(\mathbb{K})$. Mas isso é um absurdo. Portanto (a) está provada.

(b) Segue observando-se que

$$u \cdot v + v \cdot u = (u+v)^2 - u^2 - v^2 \in \mathbb{R}.$$

(c) Seja $v \in \mathrm{Im}(\mathbb{K})$. Por definição $v^2 = \alpha$ com $\alpha \in \mathbb{R}$. Se $\alpha \geq 0$, então $\alpha = \beta^2$, para um $\beta \in \mathbb{R}$. Assim,

$$(v - \beta) \cdot (v + \beta) = v^2 - \alpha = 0.$$

Disso segue $v = \beta$ ou $v = -\beta$ e v não pertenceria a $\mathrm{Im}(\mathbb{K})$ o que é um absurdo. Logo, $\alpha = -\omega$ com $\omega > 0$ e $\omega = \gamma^2$. O elemento $u = \gamma^{-1} v$ é tal que $u^2 = -1$.

(d) A injetividade de φ é equivalente a mostrar que $1, u, v$ e w são linearmente independentes em $\mathbb{K}$. Os vetores u e v são linearmente independentes porque se v fosse múltiplo escalar de u, teríamos $w = u \cdot v = v \cdot u = -w$ e portanto $w = 0$, contradizendo $w^2 = -1 \neq 0$. O item (a) mostra que $1, u$ e v são linearmente independentes. Se $w \in \langle 1, u, v\rangle$, existiriam únicos $\alpha, \beta, \gamma \in \mathbb{R}$ tais que

$$w = \alpha u + \beta v + \gamma. \tag{3.24}$$

Multiplicando essa relação por u, teremos

$$-v = -\alpha + \beta w + \gamma u \Rightarrow w = -\frac{\gamma}{\beta}u - \frac{1}{\beta}v + \frac{\alpha}{\beta}. \tag{3.25}$$

De (3.24) e (3.25) implicaria, pela unicidade das constantes, que $\beta^2 = -1$. Essa contradição prova a asserção, enquanto uma conta direta prova que $(\alpha u+\beta v+\gamma w)^2 \in \mathbb{R}$. □

A noção de tripla de Hamilton deve sua importância ao seguinte resultado de existência.

Proposição 3.4.3. *Seja $\mathbb{K}$ uma extensão de $\mathbb{R}$ sem divisores de zero. Seja $U \subseteq \mathrm{Im}(\mathbb{K})$ um subespaço de dimensão dois de $\mathbb{K}$. Para cada elemento $u \in U$ tal que $u^2 = -1$, existe $v \in U$ tal que u, v e $u \cdot v$ formam uma tripla Hamiltoniana em $\mathbb{K}$.*

Prova. Pela Proposição 3.4.2 (b), existe $v' \in U$ tal que $u \cdot v' + v' \cdot u = \beta \in \mathbb{R}$. Definamos agora $v'' = v' + \frac{\beta}{2}u$. Obviamente, $v'' \in U \subset \mathrm{Im}(\mathbb{K})$. Além disso,

$$\begin{aligned} u \cdot v'' + v'' \cdot u &= u \cdot (v' + \frac{\beta}{2}u) + (v' + \frac{\beta}{2}u) \cdot u \\ &= \frac{\beta}{2}u^2 + u \cdot v' + \frac{\beta}{2}u^2 + v' \cdot u \\ &= \beta u^2 + u \cdot v' + v' \cdot u \\ &= -\beta + \beta \\ &= 0 \end{aligned}$$

Pela prova da Proposição 3.4.2 (c), existe um múltiplo $v = \gamma v''$, com $\gamma \in \mathbb{R}$, tal que $v^2 = -1$. Uma conta direta nos mostra que v também satisfaz a relação $u \cdot v + v \cdot u = 0$. Assim, temos

$$u^2 = v^2 = -1 \quad \text{e} \quad u \cdot v = -v \cdot u.$$

Para concluirmos o desejado resta provarmos que para $w = u \cdot v$ temos

$$w^2 = -1 \quad \text{e}$$

(as demais identidades seguem de $u^2 = v^2 = 1,\ w = u \cdot v,$ e $u \cdot v = -v \cdot u$). Ora,

$$v \cdot w^2 = (v \cdot w) \cdot w = u \cdot w = -v.$$

Assim, deduzimos

$$v(w^2 + 1) = 0.$$

Portanto, $w^2 = -1$, já que $\mathbb{K}$ não tem divisores de zero. □

Necessitaremos mais adiante da seguinte definição:

Definição 3.4.4. Uma extensão $\mathbb{K}$ de $\mathbb{R}$ é dita *quadrática* se para cada $z \in \mathbb{K}$, existem $\alpha, \beta \in \mathbb{R}$ tais que $z^2 = \alpha z + \beta$.

Exemplo 3.4.5. A extensão $\mathbb{H}$ é quadrática. De fato, para cada $z = a + bi + cj + dk$, temos $z^2 = 2az + (a^2 + b^2 + c^2 + d^2)$. Em particular, como $\mathbb{C} \subset \mathbb{H}$, também temos que $\mathbb{C}$ é quadrática.

O seguinte resultado de Frobenius mostra a importância da noção de elemento imaginário.

Teorema 3.4.6. (**Lema de Frobenius**) *Seja* $\mathbb{K}$ *uma extensão de* $\mathbb{R}$ *quadrática. Então* $\mathrm{Im}(\mathbb{K})$ *é um subespaço vetorial de* $\mathbb{K}$ *e*

$$\mathbb{K} = \mathbb{R} \oplus \mathrm{Im}(\mathbb{K}).$$

Prova. Sejam $u, v \in \mathrm{Im}(\mathbb{K})$. É suficiente mostrar que $u+v \in \mathrm{Im}(\mathbb{K})$, pois $\alpha u \in \mathrm{Im}(\mathbb{K})$ para cada $u \in \mathrm{Im}(\mathbb{K})$ e para cada $\alpha \in \mathbb{R}$ como já observado acima. Se u e v são linearmente dependentes, teremos $v = \alpha u$ e $u + v = (1 + \alpha)u \in \mathrm{Im}(\mathbb{K})$. Assim, suponhamos u e v linearmente independentes. Como $\mathbb{K}$ é quadrática,

$$(u + v)^2 = \alpha_1 + \beta_1(u + v),\ \ (u - v)^2 = \alpha_2 + \beta_2(u - v),$$

para certos $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{R}$. Isso implica que

$$(\beta_1 + \beta_2)u + (\beta_1 - \beta_2)v = 2u^2 + 2v^2 - (\alpha_1 + \alpha_2) \in \mathbb{R}.$$

A Proposição 3.4.2 garante que $\beta_1 + \beta_2 = \beta_1 - \beta_2 = 0$, i.e. $\beta_1 = \beta_2 = 0$ e $(u+v)^2 = \alpha_1$. Novamente pela Proposição 3.4.2 $u + v \notin \mathbb{R}$ e portanto $u + v \in \mathrm{Im}(\mathbb{K})$.

Seja $v \in \mathbb{K} \setminus \mathrm{Im}(\mathbb{K})$. Por hipótese $v^2 = \alpha + \beta v$ e portanto $(v - \beta/2)^2 = (\alpha + \beta^2/4)$. Como $v - \beta/2 \notin \mathbb{R}$ então $v - \beta/2 \in \mathrm{Im}(\mathbb{K})$, i.e., $\mathbb{K} = \mathbb{R} + \mathrm{Im}(\mathbb{K})$ e portanto $\mathbb{K} = \mathbb{R} \oplus \mathrm{Im}(\mathbb{K})$. □

Podemos finalmente provar o resultado principal dessa seção.

Teorema 3.4.7. (**Frobenius, 1877**) *Seja $\mathbb{K}$ uma extensão de $\mathbb{R}$ quadrática e sem divisores de zero. Então, a menos de isomorfismos, $\mathbb{K}$ é uma das seguintes extensões: $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. Em particular, uma extensão quadrátiva sem divisores de zero e não comutativa deve ser isomorfa a $\mathbb{H}$.*

Prova. Seja $n \geq 1$ a dimensão vetorial de $\mathbb{K}$. Se $n = 1$, é imediato deduzir que o homomorfismo $\varphi : \mathbb{K} \to \mathbb{R}$ definido por $\varphi(1) = 1$ é um isomorfismo de $\mathbb{K}$ em $\mathbb{R}$.

Seja $n = 2$. Pelo Lema de Frobenius temos $\mathrm{Im}(\mathbb{K}) \neq \emptyset$ e portanto existe $u \in \mathbb{K}$ tal que $u^2 = -1$. Seja $\varphi : \mathbb{C} \to \mathbb{K}$ a transformação linear definida por $\varphi(1) = 1$ e $\varphi(i) = u$. Esta transformação é injetora pois 1 e u são linearmente independentes. Sendo $n = 2$, φ é um isomorfismo e linear. Para mostrar que é isomorfismo de extensões de $\mathbb{R}$ basta mostrar que $\varphi(z \cdot z') = \varphi(z) \cdot \varphi(z')$ o que é imediato.

Seja $n \geq 3$. Como $\dim(\mathrm{Im}(\mathbb{K})) \geq 2$, $\mathbb{K}$ contém uma tripla Hamiltoniana $u, v, w \in \mathrm{Im}(\mathbb{K})$ é uma sub-álgebra isomorfa a $\mathbb{H}$, vide Proposição 3.4.2. Seja $x \in \mathrm{Im}(\mathbb{K})$ qualquer. Pela Proposição 3.4.2 existem $\alpha, \beta, \gamma \in \mathbb{R}$ tais que

$$x \cdot u + u \cdot x = \alpha, \quad x \cdot v + v \cdot x = \beta, \quad x \cdot w + w \cdot x = \gamma. \tag{3.26}$$

Multiplicando à direita a primeira equação por v e multiplicando à esquerda a segunda equação por u, deduzimos

$$x \cdot w + (u \cdot x) \cdot v = \alpha v, \quad u \cdot (x \cdot v) + w \cdot x = \beta u$$

e portanto

$$x \cdot w - w \cdot x = \alpha v - \beta u.$$

A última equação combinada com a terceira em (3.26) fornece

$$2x \cdot w \in \langle u, v, w \rangle$$

e enfim $-2x = x \cdot w^2 \in \langle u, v, w \rangle$, i.e. $\mathrm{Im}(\mathbb{K}) = \langle u, v, w \rangle$ e $\mathbb{K} \simeq \mathbb{H}$. □

3.5 Os quatérnios e a Libertação da Álgebra

Com o surgimento dos quatérnios chegamos a seguinte cadeia

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$$

Notemos que na evolução dessa cadeia, até chegar aos números complexos, levava-se em consideração a preservação das propriedades aritméticas elementares. A contribuição fundamental de Hamilton foi quebrar esse paradigma dando maior liberdade ao pensamento. Esse feito de Hamilton é considerado como o primeiro passo para o fenômeno da história da matemática conhecido como *Libertação da Álgebra*.

Depois do surgimento dos quatérnios, vários outros matemáticos aventuraram-se em construir estruturas que não se restringissem às regras da aritmética usual. Entre esses, podemos citar os trabalhos de Boole, Grassmann e Cayley, em que, não só a comutatividade deixava de ser válida, mas também outras propriedades, como exemplo, a associatividade.

Toda essa manifestação de idéias inspiradas no trabalho pioneiro de Hamilton acabou influenciando na concepção atual da área da matemática conhecida como álgebra, onde o foco principal deixou de ser manipulações para resolução de equações polinomiais e passou a ser as chamadas *estruturas algébricas*.

Considerações Finais

Neste trabalho foi realizado um estudo com o objetivo de mostrar os conjuntos numéricos numa nova perspectiva, não restritamente como inclusões triviais, mas como sistemas vistos através de estruturas algébricas que preservam axiomas e propriedades quando estendidos. No tocante, foi dado destaque aos números complexos, onde apresentamos aplicações e que nesse processo de extensão a estrutura agébrica de $\mathbb{C}$ é única. Porém, ressaltamos que o seguimento de estudos e pesquisa na construção do conhecimento sistematizado não cessou, os números hipercomplexos ganharam espaço, dando novos direcionamentos aos rumos da matemática, em especial, da álgebra.

Através desse processo de extensão $\mathbb{N} - \mathbb{C}$ até os hipercomplexos, percebemos o quanto é importante as propriedades aritméticas e algébricas dos conjuntos numéricos, uma vez que quanto mais propriedades um campo de estudo possui, maior são as possibilidades para o matemático desenvolver o conhecimento científico. Além disso, mostramos que os números complexos são aplicáveis tanto na matemática em si, como no meio social e no processo de ensino-aprendizagem, na perpectiva de articular o ensino de matemática no ensino básico com a ciência e a tecnologia. Essas aplicações, inclusive a sistematização dos conjuntos numéricos assim apresentados, proporcionam ao processo de ensino da matemática a oportunidade de torná-lo mais dinâmico e experimental, no qual o aluno deixa de ser coadjuvante, passando a participar e viajar no mundo da matemática ativamente na construção do conhecimento sistematizado.

Note que ao trabalhar as aplicações de números complexos, assim como as extensões do conceito de números dessa forma, proporcionamos ao aluno não ter uma postura errônea de encarar os problemas apenas como manipulação de símbolos algébricos mecanicamente, sem se preocupar com seus significados. Mas propomos perceptivelmente dar acesso significativo ao que está sendo estudado, contribuindo consideravelmente à formação discente na projeção de um novo horizonte. Pois, é objetivo do ensino torná-lo cada vez mais diferenciado, para que conquiste e aumente

sua autonomia e liberdade na sociedade que o cerca. É claro que o profissional detentor desse conhecimento, além de ter domínio e transmitir segurança, deve adequar da melhor maneira possível essas abordagens, para que o sujeito envolvido tenha um aprendizado agradável e em alto nível.

Assim, é sublime neste trabalho o quanto a matemática é surpreendente, onde podemos ampliar nosso conhecimento e aprimorar nossas práticas para o processo de ensino. Uma vez que ensino de qualidade requer aperfeiçoamento profissional, então este deve estar sempre em contínua preparação, buscando conhecimento científico e alternativas pedagógicas que propiciem uma maior proximidade com as exigências do mundo contemporâneo.

Portanto, na certeza de que o processo de ensino-aprendizagem de matemática é desafiador, e ao mesmo tempo buscamos uma educação de qualidade para todos, então devemos estar envolvidos e motivados no processo, a dispor de energia suficiente para enfrentar todos os estímulos negativos impostos pelo mundo cotidiano.

Referências Bibliográficas

[1] EVES, Howard. *Introdução à história da Matemática*; Tradução: Higino H. Domingues. Campinas, SP: Editora da Unicamp, 2004.

[2] BOYER, Carl Benjamin. *História da matemática*; Tradução: Elza F. Gomide. São Paulo: Edgard Blucher, Ed. Da Universidade de São Paulo, 1974.

[3] EBBINGHAUS, Heinz-Dieter; HERMES, Hans; KOEKER, Max; REMMENT, Reinhold; NEUKIRCH, Jürgen; HIRZEBRUCH, Friedrich; MAINZER, Klaus; PRESTEL, Alexander. *Numbers*. Traduzido para o inglês, tendo como editor John H. Ewing. New York: Springer-Verlag, 1991.

[4] NETO, Francisco Tavares da Rocha. *Dificuldades na Aprendizagem Operatória de Números Inteiros no Ensino Fundamental*. Fortaleza: UFC, 2010.

[5] CARDOSO, Andréa. *Apostila de Matemática Elementar I*. Minas Gerais: UNIFAL, 2013.

[6] FONSECA, Rubens Vilhena. *Teoria dos Números*. Belém: UEPA, 2011.

[7] NASCIMENTO, Alane Gomes de Albuquerque Nascimento. *As Dificuldades de Aprendizagem das Operações Aritméticas Básicas no 7º Ano do Ensino Fundamental: Números Inteiros Relativos*. Campina Grande: UEPA, 2010.

[8] Sociedade Brasileira de Matemática (SBM). *RPM - Revista do Professor de Matemática*. São Paulo: SBM, 2013.

[9] JÚNIOR, Ulício Pinto. *A História dos Números Complexos: "das quantidades sofisticadas de Cardano às linhas orientadas de Argand"*. Rio de Janeiro: UFRJ/ Programa de Pós-Graduação em Ensino de Matemática, 2009.

[10] HEFEZ, Abramo; VILLELA, Maria Lúcia Torres. *Polinômios e Equações Algébricas*. Coleção PROFMAT. Rio de Janeiro: SBM, 2012.

[11] CARMO, Marfredo Perdigão do; MORGADO, Augusto César; WAGNER, Eduardo. *Trigonometria e Números Complexos*. 3ª ed. Rio de Janeiro: SBM, 2005.