



UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA

CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS

PROGRAMA DE MESTRADO EM MATEMÁTICA EM REDE NACIONAL

DISSERTAÇÃO DE MESTRADO



PROFMAT

SOBRE ÁLGEBRAS DE DIVISÃO DE DIMENSÃO FINITA

JOSÉ CARLOS LEAL DO VALLE JÚNIOR

Cruz das Almas – Bahia

abril de 2017

SOBRE ÁLGEBRAS DE DIVISÃO DE DIMENSÃO FINITA

JOSÉ CARLOS LEAL DO VALLE JÚNIOR

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal do Recôncavo da Bahia como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 20 de abril de 2017.

Cruz das Almas – Bahia
abril de 2017

FICHA CATALOGRÁFICA

V181s	<p>Valle Júnior, José Carlos Leal do. Sobre álgebras de divisão de dimensão finita / José Carlos Leal do Valle Júnior. Cruz das Almas, BA, 2017. 108f.; il.</p> <p>Orientador: Antonio Andrade do Espírito Santo.</p> <p>Dissertação (Mestrado) – Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas.</p> <p>1. Matemática – Álgebra. 2. Matemática – Problemas, exercícios etc. I. Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas. II. Título.</p> <p>CDD: 512</p>
-------	---

SOBRE ÁLGEBRAS DE DIVISÃO DE DIMENSÃO FINITA

JOSÉ CARLOS LEAL DO VALLE JÚNIOR

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal do Recôncavo da Bahia como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 20 de abril de 2017.

Banca examinadora:

Antonio Andrade do Espírito Santo

Prof. Dr. Antonio Andrade do Espírito Santo (Orientador)

Universidade Federal do Recôncavo da Bahia (UFRB)

Maria Amélia de P. B. Hohlenweger

Profa. Dra. Maria Amélia Pinho Barbosa Hohlenweger

Universidade Federal do Recôncavo da Bahia (UFRB)

Joseph Nee Anyah Yartey

Prof. Dr. Joseph Nee Anyah Yartey

Universidade Federal da Bahia (UFBA)

Dedico este trabalho à minha avó, Odete Lourenço (*in memoriam*), e ao meu amado irmão, Carlos Eduardo (*in memoriam*). Sempre foi por mim, agora será por nós.

Agradecimentos

Foram muitas as dificuldades encontradas até a chegada deste momento. Após tantas noites de estudo, grupos de estudo, inúmeras viagens, disciplinas cursadas, exame nacional de qualificação, cursos de verão e perdas de pessoas queridas, ter armazenado na memória os nomes das pessoas e instituições que colaboraram e me apoiaram nestes anos de crescimento e maturação intelectual é angustiante e, ao mesmo tempo, alentador, principalmente por saber que estou encerrando este trabalho. Diante disto, recorro à memória para não esquecer de ninguém, porém, se isto acontecer, registro aqui o meu carinho e apreço por todos aqueles que de maneira direta ou indireta contribuíram para a construção deste trabalho. No entanto, gostaria de agradecer de maneira especial a,

DEUS, por tudo que tem me proporcionado durante toda essa caminhada e pela força que me faz seguir, apesar de todas as dificuldades.

Aos meus pais, José Carlos Leal do Valle e Sônia Regina Soares Lourenço pelo discernimento a mim transmitido, pelo positivismo e pela confiança em mim depositada. Sou eternamente grato por ter vocês ao meu lado sempre. Muito obrigado por acreditar em mim. Registro aqui o meu amor por vocês, meus exemplos de perseverança.

A minha noiva e futura esposa, Luane Moraes Paraíso. Foram muitas as dificuldades que superamos juntos durante a construção deste trabalho. Obrigado por se manter firme ao meu lado durante todo esse tempo. Você foi peça insubstituível nesta construção. Começamos juntos e sabemos que “juntos somos mais fortes”.

Ao meu orientador, o Professor Dr. Antonio Andrade do Espirito Santo. Agradeço-lhe pela disposição, competência, abertura e gentileza durante todo este percurso. Resalto que a construção deste trabalho não teria êxito sem a sua ajuda. Desempenhar esta parceria é a realização de um sonho de um ex-estudante de graduação que por coincidências do destino tem a oportunidade de reencontrar-se com o professor ao qual decidiu espelhar-se em toda sua carreira. Posso afirmar com plena convicção, eu tive “o orientador”.

Agradeço aos meus irmãos Leandro Lourenço e Carlos Eduardo pela amizade e incentivo durante a construção do presente trabalho. Tenho amigos, mas sem dúvida estes são os quais sempre irei contar. Hoje não estamos mais juntos, a vida nos proporciona

momentos de tristeza cuja explicação não existe. Ainda assim, sei que de onde Dudu estiver ele estará torcendo por nós. Este momento é uma realização nossa.

Não poderia deixar de agradecer à pessoa que me deu suporte para início de todo o processo que culminou na produção deste trabalho, a minha avó Odete Lourenço. Foi ao seu lado que vivi os tempos mais felizes de minha vida. A saudade é algo constante em mim. Seus conselhos se mantêm vivos em minha mente e coração, obrigado pela confiança.

Aos meus colegas de curso: Carlos, Benício, Bruno, Cléber, Jânio, Patrícia e Valdemir. Como sempre foi dito entre nós, “nunca deu errado”. Espero que nossos laços de amizade se mantenham eternamente. Nossa convivência sempre foi garantia de harmonia. Sentirei saudades de nossas “resenhas” e dos nossos estudos incessantes. Aprendi com cada um de vocês um pouco sobre a vida.

Aos professores do programa, cada um de vocês contribuiu de forma significativa na minha evolução e tem, ainda que de forma indireta, participação na construção deste trabalho.

Aos meus amigos de forma geral. Cada um de vocês teve enorme importância me mantendo de pé, nos momentos em que o cansaço e desgaste me inclinavam a desistir.

Agradeço ainda à CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pela concessão da bolsa durante todo o período de realização deste mestrado.

Resumo

Neste trabalho discutiremos sobre a não existência de uma \mathbb{R} -álgebra de divisão, associativa e de dimensão 3, usando o conceito de esferas paralelizáveis. Também é apresentada uma classificação das \mathbb{R} -álgebras de divisão associativas de dimensão finita (Teorema de Frobenius). Ademais, exploramos a construção formal dos naturais, inteiros, racionais, reais e complexos, mostrando, o significado preciso da sequência de inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Por outro lado, analisamos os resultados obtidos a partir da aplicação de questionários investigativos para estudantes egressos do ensino médio e para professores licenciados em matemática e, com base nesta análise, propomos uma atividade sobre o conteúdo de números complexos, pautada na aprendizagem significativa.

Palavras-chave: \mathbb{R} -álgebras, quatérnios e octônios, números complexos.

Abstract

In this work we will discuss about the non-existence of a R - associative and 3 division algebra, using the concept of parallelizable spheres. It is also presented a classification of the R - associative division algebras of finite dimension (Frobenius theorem). In addition, we explored the formal construction of the naturals, whole number, rational, reals, and complexes, showing the precise meaning of the inclusion sequence $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. On the other hand, we analyzed the results obtained from the application of investigative questionnaires for high school students and teachers licensed in mathematics and, based on this analysis, it was offered an activity on the content of complex numbers, based on meaningful learning.

Keywords: \mathbb{R} -álgebras, quaternions and octonions, complex numbers.

Sumário

Introdução	1
1 Os conjuntos numéricos na visão de estudantes e professores	5
1.1 Uma breve discussão sobre o ensino de conjuntos	5
1.2 Questionário dos estudantes	7
1.2.1 Questão 1 – Resultados e discussões	7
1.2.2 Questão 2 – Resultados e discussões	8
1.2.3 Questão 3 – Resultados e discussões	12
1.3 Questionário dos Professores	13
1.3.1 Questão 1 – Resultados e discussões	13
1.3.2 Questão 2 – Resultados e discussões	14
1.3.3 Questões 3, 4 e 5 – Resultados e discussões	14
2 Uma proposta de sequência didática	17
2.1 Fundamentação teórica	17
2.2 Conceitos básicos sobre números complexos	18
2.3 Sequência didática	24
2.3.1 Roteiro da sequência didática	24
2.3.2 Atividade 1 - Exercícios de iniciação aos números complexos	25
2.3.3 Atividade 2 - Análise investigativa da multiplicação de complexos não-nulos pelos complexo i e $-i$	26
2.3.4 Atividade 4 - Análise investigativa da multiplicação de complexos não-nulos por números reais	29
2.3.5 Atividade 4 - Situação Problema	31
2.4 Reflexões sobre a Sequência Didática	37
3 Conjuntos numéricos: dos naturais aos complexos	39
3.1 Os números naturais	40
3.1.1 Operações com naturais	41
3.2 Relação de equivalência	42

3.3	Os números inteiros	46
3.4	Os números racionais	46
3.5	Os números reais	46
3.6	Os números complexos	48
3.7	Relação de ordem	49
3.7.1	Relação de ordem em \mathbb{N}	50
3.7.2	Relação de ordem em \mathbb{Z}	51
3.7.3	Relação de ordem em \mathbb{Q}	54
3.7.4	Relação de ordem em \mathbb{R}	55
3.8	Cópias algébricas	56
4	Conjuntos numéricos: quatérnios e octônios	61
4.1	Os quatérnios	61
4.1.1	Um argumento para a regra da multiplicação dos quatérnios	65
4.2	Os octônios	65
4.2.1	Um argumento para a regra da multiplicação dos octônios	66
4.3	Aplicações	68
5	Estruturas Algébricas	71
5.1	Operações nos conjuntos numéricos	71
5.1.1	Operações com inteiros	71
5.1.2	Uma motivação para a definição das operações com inteiros	72
5.1.3	Operações com racionais	73
5.1.4	Operações com reais	73
5.2	Relações entre as estruturas algébricas e os conjuntos numéricos	74
5.2.1	Magma	74
5.2.2	Semigrupos	74
5.2.3	Monóides	77
5.2.4	Grupos	80
5.2.5	Grupos abelianos	84
5.2.6	Anéis	87
5.2.7	Domínios de Integridade	90
5.2.8	Corpos	90
5.2.9	Espaço vetorial	91
5.2.10	Álgebra	91
6	A questão proposta por Hamilton	95
6.1	A questão proposta por Hamilton: Quais esferas são paralelizáveis?	95

6.2	A questão proposta por Hamilton: Quais esferas são grupos?	98
6.3	O Teorema de Frobenius para \mathbb{R} -álgebras de divisão associativas de dimensão finita	99
Apêndice A		103
	Referências Bibliográficas	109

Lista de Figuras

1.1	Questão 1 – Questionário dos estudantes	7
1.2	Resultados da questão 1 – Questionário dos estudantes	8
1.3	Questão 2 – Questionário dos estudantes	8
1.4	Resolução da questão 2 (Estudante 1)	9
1.5	Resolução da questão 2 (Estudante 2)	9
1.6	Resolução da questão 2 (Estudante 8)	10
1.7	Resolução da questão 2 (Estudante 9)	10
1.8	Resolução da questão 2 (Estudante 15)	11
1.9	Resolução da questão 2 (Estudante 26)	11
1.10	Questão 3 – Questionário dos estudantes	12
1.11	Resultados da questão 3 – Questionário dos estudantes	12
1.12	Questão 1 – Questionário dos professores	13
1.13	Resultados da questão 1 – Questionário dos professores	13
1.14	Questão 2 – Questionário dos professores	14
1.15	Resultados da questão 2 – Questionário dos professores	14
1.16	Questão 3 – Questionário dos professores	14
1.17	Questão 4 – Questionário dos professores	15
1.18	Questão 5 – Questionário dos professores	15
1.19	Resultados das questões 3 e 4 – Questionário dos professores	15
1.20	Resultados da questão 5 – Questionário dos professores	15
2.1	Representação geométrica de complexos	21
2.2	Interpretação geométrica da adição de complexos	21
2.3	Interpretação geométrica da subtração de complexos	21
2.4	Interpretação geométrica do conjugado de um complexo	22
2.5	Complexo e coordenadas trigonométricas	22
2.6	Multiplicação de complexos unitários	23
2.7	Operações com complexos	26
2.8	Operações com complexos	27
2.9	Operações com complexos	28

2.10	Operações com complexos	28
2.11	Operações com complexos - item <i>a</i>)	30
2.12	Operações com complexos - item <i>b</i>)	30
2.13	Operações com complexos - item <i>b</i>)	31
2.14	Ilustração do rio	32
2.15	Ilustração da primeira etapa do problema	33
2.16	Ilustração da segunda etapa do problema	34
2.17	Ilustração da terceira etapa do problema	35
2.18	Figura conclusiva do problema	36
4.1	Diagrama multiplicativo dos quatérnios	64
4.2	Diagrama multiplicativo dos octônios	67
5.1	Exemplos de monóides	80
6.1	Questionário aplicado aos alunos - p.1	103
6.2	Questionário aplicado aos alunos - p.2	104
6.3	Questionário aplicado aos professores - p.1	105
6.4	Questionário aplicado aos professores - p.2	106

Introdução

A partir de um sistema de coordenadas, concebido por *Gerolamo Cardano*, hoje conhecido como sistema de coordenadas cartesianas, sabemos que é possível estabelecer uma identificação dos números reais com os pontos de uma reta. Do mesmo modo, sabemos que os números complexos podem ser identificados com os pontos de um plano. De modo natural, surge a seguinte questão: é possível definir uma estrutura algébrica, similar a apresentada para os números complexos, que permita operar com vetores no espaço? Esta questão foi formulada, no século *XIX*, pelo matemático, físico e astrônomo irlandês William Rowan Hamilton¹, a qual, em linguagem atual, pode ser descrita como abaixo:

Questão 1. *Existe uma \mathbb{R} -álgebra de divisão, associativa e de dimensão 3?*

É possível formular a questão proposta por Hamilton em um contexto mais geral, da seguinte forma:

Teorema. Não existe uma \mathbb{R} -álgebra de divisão associativa de dimensão ímpar maior do que 1. Em particular, não existe uma \mathbb{R} -álgebra de divisão associativa de dimensão 3.

Uma vez obtida resposta para a questão proposta por Hamilton, uma outra discussão surge naturalmente, a saber:

Questão 2. *Existe uma classificação para as \mathbb{R} -álgebras de divisão, associativas e de dimensão finita?*

No presente trabalho, apresentamos o Teorema de Frobenius², o qual caracteriza as \mathbb{R} -álgebras de divisão, associativas e de dimensão finita. Explicitamente,

¹William Rowan Hamilton (1805 – 1865) foi uma criança prodígio; aos três anos de idade lia perfeitamente inglês e aprendeu os rudimentos da aritmética. Aos quatro aprendeu geografia, aos cinco sabia latim e hebraico e até os dez anos de idade aprendeu italiano, francês, árabe, sânscrito, persa, caldeu e várias línguas orientais. Aos doze interessou-se por matemática. Estudou então a Álgebra *Universalis* de Newton e, antes dos dezessete, estudou a monumental *Mecanique Céleste* de Laplace na qual descobriu um erro e publicou a correção correspondente. ([22], p. 31, 2004).

²Ferdinand Georg Frobenius (Berlim, 26 de outubro de 1849 - Berlim, 3 de agosto de 1917)

Teorema de Frobenius. Se A é uma \mathbb{R} -álgebra de divisão associativa, com dimensão finita, então A é isomorfa ao conjunto dos números reais, ou ao conjunto dos números complexos, ou ao conjunto de dimensão 4, denominado de quatérnios. Isto é, A tem dimensão 1, 2 ou 4.

Uma outra abordagem que também nos remete ao Teorema de Frobenius e que também será explorada no presente trabalho é a seguinte:

Dados os conjuntos numéricos: naturais (\mathbb{N}), inteiros (\mathbb{Z}), racionais (\mathbb{Q}), reais (\mathbb{R}) e complexos (\mathbb{C}). Sabe-se, dos conhecimentos advindos do ensino médio, que vale a seguinte cadeia de inclusões: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. A partir daí, é natural os seguintes questionamentos:

Questão 3. *Existe algum conjunto numérico, digamos X , tal que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset X$?*

Questão 4. *Caso exista um conjunto X , tal como referido na questão anterior, questione-se: a sucessão de inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset X$ chegou ao “fim”?*

Neste ponto, ressaltamos que para além de desenvolver uma discussão sobre tais conjuntos numéricos, fornecendo aporte teórico para a compreensão do presente trabalho, também buscaremos discutir alguns elementos associados aos processos de ensino e aprendizagem destes conjuntos numéricos, de tal sorte que alguns obstáculos que o professor de matemática possa encontrar ao ensinar tais conteúdos possam ser minimizados, conforme destaca Cezar, ao falar sobre o ensino desses conceitos:

“muitos desses obstáculos surgiram na formulação de conceitos matemáticos, ou surgem até hoje durante o processo de ensino e aprendizagem, que acabam por dificultar a compreensão do conceito de números reais” ([4],2011, p.22).

Na direção de compreender alguns destes obstáculos inerentes aos processos de ensino e aprendizagem, notadamente, no que tange ao ensino dos conjuntos numéricos, é realizada uma pesquisa e, a partir dos resultados oriundos desta investigação, é construída uma atividade acerca dos números complexos, baseada na (re)significação de conceitos, com o aporte de um *software* de geometria dinâmica, a saber: o Geogebra.

Objetivando cumprir os objetivos propostos, o presente trabalho foi dividido nos capítulos descritos abaixo.

No capítulo 1 fomentamos a discussão sobre os processos de ensino e aprendizagem dos conjuntos numéricos, apresentando, inicialmente, a análise realizada em [18], de livros

didáticos, amplamente utilizados nas escolas brasileiras. E, em seguida, faremos algumas reflexões de dados obtidos de questionários investigativos aplicados para professores da rede básica de ensino e para estudantes concluintes do ensino médio.

No capítulo 2, inspirados nos resultados do capítulo 1, são apresentados alguns conceitos básicos sobre os números complexos e, em seguida, é proposta uma sequência didática, acerca dos números complexos. Esta sequência didática culmina com a resolução de um determinado problema, utilizando o *software* livre de geometria dinâmica: Geogebra.

Ainda inspirados nos resultados do capítulo 1, mais especificamente, nos dados dos questionários aplicados para os professores, apresentamos, no capítulo 3, uma construção dos conjuntos \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} . Em seguida, na direção de responder a questão 3, no capítulo 4 é apresentada a construção de dois outros conjuntos numéricos, a saber: quatérnios e octônios.

Face ao objetivo de classificar \mathbb{R} -álgebras, no capítulo 5 são apresentadas algumas estruturas algébricas, permitindo, oportunamente, classificar os conjuntos apresentados no capítulo 3, com respeito a estas estruturas.

No capítulo 6 é apresentada, inicialmente, uma resposta à questão 1, usando o conceito de esferas paralelizáveis. Em seguida, é discutida uma outra solução para esta questão, a partir do questionamento de quais esferas são grupos. Finalmente, é discutido o Teorema de Frobenius, respondendo as questões 2 e 4.

Capítulo 1

Os conjuntos numéricos na visão de estudantes e professores

Neste capítulo faremos uma reflexão sobre o ensino dos conjuntos numéricos. Inicialmente faremos uma reflexão sobre a abordagem dos conjuntos numéricos no ensino básico, a partir da referência [18]. Em seguida, apresentaremos os principais resultados de uma pesquisa realizada, através da aplicação de questionários, com estudantes e professores do ensino básico.

1.1 Uma breve discussão sobre o ensino de conjuntos

Em [18], Lima faz a seguinte reflexão ao analisar um livro didático, acerca dos conteúdos sobre conjuntos numéricos.

O capítulo sobre conjuntos é pequeno e pobre. Como não cita a relação de inclusão entre conjuntos, perde a oportunidade de fazer a conexão com a Lógica e, em particular, deixa de explicar o significado da implicação e da equivalência. ([18], 2008, p.230).

Buscando orientações nos referenciais oficiais, a saber: “Parâmetros Curriculares Nacionais (PCNs)” e “Orientações Curriculares para o Ensino Médio”, de como ensinar os conjuntos numéricos, identificamos, no primeiro, apenas trechos com comentários gerais sobre a utilização da noção de conjuntos. Do segundo, destacamos o trecho a seguir:

Os números complexos devem ser apresentados como uma histórica necessidade de ampliação do conjunto de soluções de uma equação, tomando-se, para isso, uma equação bem simples, a saber, $x^2 + 1 = 0$. ([19], 2006, p.71)

Visando aprofundar uma aprendizagem ampla e significativa dos conjuntos numéricos, o professor de matemática não pode prescindir de apresentar ao estudante, em formação, elementos do formalismo matemático, sem exageros. Nesta direção, em [18], os autores

sugerem que os conteúdos matemáticos sejam tratados, considerando sua conceituação¹, a manipulação² e a aplicação³, permitindo, deste modo a ampliação dos saberes. Para exemplificar esta abordagem metodológica que busca a ampliação de saberes, destacamos o trecho abaixo:

Os alunos que ingressam no ensino médio certamente já tiveram um longo contato anterior com números naturais, inteiros, racionais e até mesmo certos números irracionais, como o número π e algumas raízes quadradas não-exatas. Reapresentar-lhes esses números só tem sentido se o objetivo for o de ganhar mais consistência teórica, explicando-lhes de forma mais convincente fatos que foram impostos peremptoriamente antes e, ao mesmo tempo, mostrar, mediante exemplos, problemas e outras aplicações, que essas sucessivas ampliações do conceito de número têm alguma utilidade, na matemática ou fora dela. ([18], 2001, p. 7)

Motivados pelas discussões apresentadas pelos autores em [18] e objetivando apresentar uma contribuição com a discussão sobre o ensino dos conjuntos numéricos, apresentamos nas seções 1.2 e 1.3, os resultados da análise investigativa, realizada com estudantes de um curso pré-vestibular, situado em uma cidade no interior do estado da Bahia e com professores licenciados em matemática e, em pleno exercício da docência (no ato da realização da pesquisa), em municípios do estado da Bahia. A pesquisa foi dividida em duas etapas. A primeira etapa consistiu da aplicação dos questionários para alunos egressos do ensino médio. Nesta etapa participaram 34 estudantes. A segunda etapa consistiu da aplicação dos questionários aos professores. Participaram 5 professores nesta etapa da pesquisa. Aqui ressaltou-se a representatividade da amostra, tanto no caso dos estudantes quanto no caso dos professores, haja vista que os primeiros, por se tratar de uma classe de pré-vestibular, apresentam formação heterogênea, corroborando para a diversidade. Quanto aos professores, destaca-se, o fato do nível de qualificação: todos possuíam especialização *latu sensu* e atuavam em diversas séries do ciclo básico e em diversos municípios, no ato da pesquisa.

Para uma melhor compreensão dos resultados obtidos, discutiremos os resultados dos questionários em duas seções, apresentando, sempre que possível, um comentário dos resultados esperados para cada item analisado. Uma cópia completa dos questionários

¹A conceituação compreende a formulação de definições, o enunciado de proposições, o estabelecimento de conexões entre os diversos conceitos, bem como a interpretação e a reformulação dos mesmos sob diferentes aspectos.

²a manipulação de caráter essencialmente (mas não exclusivamente) algébrico, está para o ensino e o aprendizado da matemática assim como a prática dos exercícios e escalas musicais está para a Música.

³aplicação é o emprego de noções e teorias da matemática em situações que vão de problemas triviais do dia-a-dia a questões mais sutis provenientes de outras áreas, quer científicas, quer tecnológicas. Ela é a principal razão pela qual o ensino da matemática é tão difundido e tão necessário.

encontrar-se-á no Apêndice A.

1.2 Questionário dos estudantes

Nesta seção apresentaremos a análise detalhada do questionário aplicado para os estudantes. Destaca-se que tal questionário tem por objetivo estabelecer o nível de formação dos estudantes apenas no que tange a classificação dos conjuntos numéricos, os quais denominamos por conjuntos numéricos clássicos, a saber: naturais, inteiros, racionais, reais e complexos. Os conhecimentos avaliados estão em consonância com o disposto nas orientações curriculares para o ensino médio. Ademais, buscamos introduzir os conteúdos através de uma linguagem simplificada de modo a permitir a melhor compreensão por todos os estudantes alvos da pesquisa. Com o intuito de garantir o sigilo e a confidencialidade desta pesquisa, ao mencionar algumas das respostas apresentadas, utilizaremos a denominação “estudante” 1, 2, 8, 9, 15 e 26.

1.2.1 Questão 1 – Resultados e discussões

A primeira questão do questionário

- 1) Sendo \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} e \mathbb{C} os conjuntos dos naturais, inteiros, racionais, reais e complexos, respectivamente. Supondo que as caixas abaixo representam tais conjuntos e que os seus elementos devem estar inseridos nas mesmas, direcione os elementos abaixo, posicionando-os na(s) caixa(s) corretas.

0	1	$1 + i$	$\frac{2}{1}$	$\frac{3}{4}$	i	1000	0,353535...	π	-2
---	---	---------	---------------	---------------	-----	------	-------------	-------	----

N	Z	Q	R	C
---	---	---	---	---

Figura 1.1: Questão 1 – Questionário dos estudantes

Análise dos resultados

Nesta questão o desempenho dos alunos foi analisado quanto ao posicionamento correto dos elementos de cada conjunto numérico nas caixas correspondentes, sendo computado como acerto, a situação em que o aluno posicionou corretamente **todos** os elementos de uma determinada caixa. A partir da análise do gráfico abaixo é possível notar que os alunos, em sua maioria, não compreendem de forma clara as relações de pertinência e de inclusão.

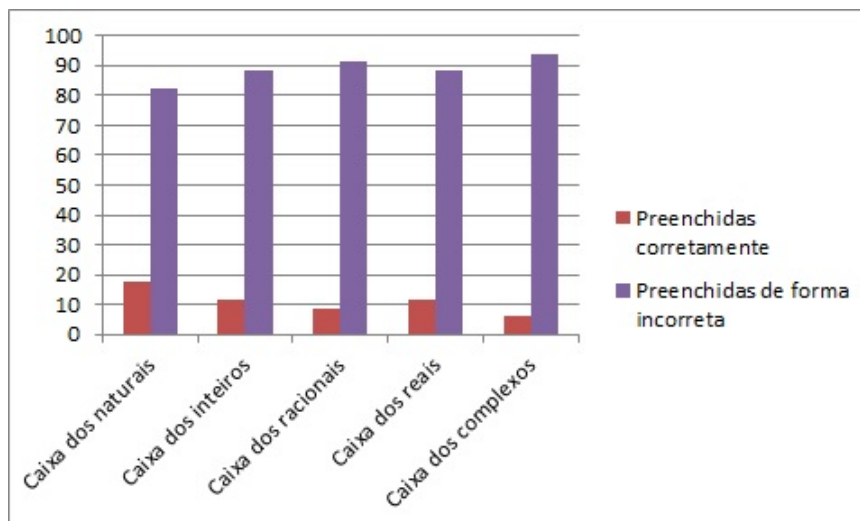


Figura 1.2: Resultados da questão 1 – Questionário dos estudantes

1.2.2 Questão 2 – Resultados e discussões

A segunda questão do questionário

- 2) Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

- a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

- b) Assinale abaixo as caixas que contém a solução da equação acima.

N	Z	Q	R	C
---	---	---	---	---

Figura 1.3: Questão 2 – Questionário dos estudantes

Nesta questão os estudantes deveriam resolver a equação $x^2 + 1 = 0$. Na próxima seção discutiremos de maneira detalhada e qualitativa os resultados apresentados na Questão 2. Para tanto, destacamos abaixo as respostas dos estudantes 1, 2, 8, 9, 15 e 26. Destacamos que estes exemplos, tomados como modelo, tem representatividade no conjunto de estudantes analisados, com respeito aos erros cometidos.

Análise dos resultados

Estudante 1

Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

$x' = \frac{-0 \pm \sqrt{(0)^2 - 4 \cdot 1 \cdot 1}}{2 \cdot 1}$ ou $x(x+1) = 0$ uso Bhaskara ou $x = 0$ como $b = 0$, a respa-
 $x' = \frac{0 \pm \sqrt{-4}}{2} = \frac{0 \pm 2i}{2} = -1$ ou $x+1 = 0$ rações de x^2
 $x = -1$

b) Assinale abaixo as caixas que contém a solução da equação acima.

N	Z	Q	ℝ	ℂ
---	---	---	--------------	---

Figura 1.4: Resolução da questão 2 (Estudante 1)

Este estudante demonstra conhecer métodos variados para a resolução de equações. No entanto, o mesmo não desenvolve tais métodos de forma correta. Chama a atenção a forma como este estudante tenta utilizar a propriedade distributiva.

Estudante 2

Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

$x^2 = -1$
 $x = \pm \sqrt{-1}$

b) Assinale abaixo as caixas que contém a solução da equação acima.

N	Z	Q	ℝ	ℂ
---	---	---	---	--------------

Figura 1.5: Resolução da questão 2 (Estudante 2)

A resolução deste estudante chama atenção pois o mesmo demonstra confusão, quanto ao significado da unidade imaginária i . Em princípio, considera $i = -1$. No entanto, enquadra a solução da equação no conjunto dos números complexos.

Estudante 8

Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

$$\begin{aligned} x^2 + 1 &= 0 \\ x^2 &= -1 \\ x &= \pm 1 \end{aligned}$$

b) Assinale abaixo as caixas que contém a solução da equação acima.

N $\begin{matrix} 0 \\ 1 \end{matrix}$	Z \pm	Q $\frac{\pm}{x}$	R \pm	C x^{\pm}
--	---------	-------------------	---------	-------------

Figura 1.6: Resolução da questão 2 (Estudante 8)

Chama a atenção a dificuldade do estudante em detectar qual o simétrico do elemento 1, o que contribui para a resolução incorreta da equação $x^2 + 1 = 0$.

Estudante 9

Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

$$\begin{aligned} x^2 + 1 &= 0 \\ x^2 &= -1 \\ x &= \sqrt{-1} \end{aligned}$$

b) Assinale abaixo as caixas que contém a solução da equação acima.

N	Z	Q	R	C
---	---	---	---	---

Figura 1.7: Resolução da questão 2 (Estudante 9)

Neste questionário o estudante embora demonstre um certo conhecimento nos processos resolutivos de equações, ele não identifica em qual conjunto numérico deve estar posicionada esta solução.

Estudante 15

Assim como o estudante 8, este estudante apresenta dificuldades na determinação do elemento simétrico, conseqüentemente afirma que 1 é solução da equação $x^2 + 1 = 0$. No entanto, a sua resposta para o item b) deixa evidente a deficiência quanto as noções de inclusão de conjuntos e/ou o entendimento da sucessão de inclusões dos conjuntos numéricos, uma vez que o mesmo afirma que o elemento 1 pertence aos conjuntos dos naturais, reais e complexos e não pertence ao conjunto dos inteiros e racionais.

Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

- a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

$$\begin{aligned} x^2 + 1 &= 0 \\ x^2 &= -1 \end{aligned}$$

- b) Assinale abaixo as caixas que contém a solução da equação acima.

N	Z	Q	R	C
---	---	---	---	---

Figura 1.8: Resolução da questão 2 (Estudante 15)

Estudante 26

Este estudante resolve a equação $x^2 + 1 = 0$ de maneira análoga ao estudante 9, porém chama atenção o fato deste estudante caracterizar $\sqrt{-1}$, simultaneamente, como elemento do conjunto dos números reais e do conjunto dos números complexos.

Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:

$$x^2 + 1 = 0$$

a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

$$\begin{aligned} x^2 &= 0 - 1 \\ x^2 &= -1 \end{aligned}$$

$$x = \sqrt{-1}$$

NÃO HÁ RAIZ PARA NÚMERO NEGATIVO

b) Assinale abaixo as caixas que contém a solução da equação acima.

N	Z	Q	R	C
---	---	---	---	---

Figura 1.9: Resolução da questão 2 (Estudante 26)

Ainda sobre a questão 2, de maneira geral, apenas 10% dos estudantes participantes da pesquisa conseguiram resolver a equação $x^2 + 1 = 0$ de maneira satisfatória. Este fato, evidencia uma possível deficiência no que diz respeito ao ensino de números complexos e dos conjuntos numéricos de forma geral.

1.2.3 Questão 3 – Resultados e discussões

Nesta questão, objetiva-se investigar se os estudantes compreendem a sucessão de inclusões dos conjuntos numéricos.

A terceira questão do questionário

- 3) Quando um conjunto A possui todos os elementos de outro conjunto, por exemplo, B , dizemos que o conjunto A contém o conjunto B ; ou que o conjunto B está contido no conjunto A . Denota-se este fato como $A \supset B$ (A contém B) ou $B \subset A$ (B está contido em A). Tomando como base a notação apresentada acima, complete os espaços vazios com as respectivas inclusões entre os conjuntos numéricos.

N ___ Z	Q ___ Z	Z ___ Q	R ___ Q	R ___ C
---------	---------	---------	---------	---------

Figura 1.10: Questão 3 – Questionário dos estudantes

Análise dos resultados

Nesta questão foi computado como acerto as situações em que o aluno inseriu corretamente, no espaço indicado, os símbolos \subset e \supset .

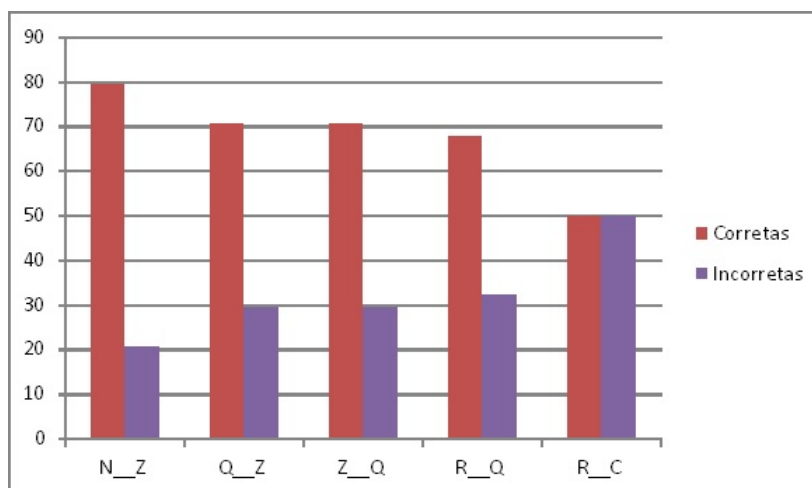


Figura 1.11: Resultados da questão 3 – Questionário dos estudantes

O gráfico acima mostra que 50% dos estudantes identificam o conjunto dos números complexos como um subconjunto dos números reais.

Uma conclusão para os resultados e discussões apresentadas acima é a existência de uma defasagem, com respeito aos conhecimentos sobre os conjuntos numéricos, de forma geral.

1.3 Questionário dos Professores

Nesta seção apresentamos os resultados dos questionários aplicados a professores do ensino básico, em efetiva docência no estado da Bahia, buscando compreender alguns aspectos das relações de ensino, concernentes aos conjuntos numéricos, bem como a compreensão dos docentes com respeito a questão, a saber: se a sequência de inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, apresentada no ensino médio, chegou ao fim?

Os professores participantes desta pesquisa possuem especializações em ensino de matemática e lecionam em escolas e institutos no estado da Bahia.

1.3.1 Questão 1 – Resultados e discussões

Nesta questão busca-se compreender os aspectos relacionados a motivação dos estudantes para aprender sobre o conjunto dos números complexos, na visão dos docentes. Ressaltamos que a motivação dos estudantes é uma questão basilar no âmbito das relações de ensino-aprendizagem no ciclo básico de ensino.

- 1) Nas suas experiências como docente de matemática, os alunos apresentam motivação para o estudo dos números complexos?
- a) Sim
 - b) Não
 - c) Raramente

Figura 1.12: Questão 1 – Questionário dos professores

O gráfico abaixo mostra que apenas 20% dos professores acredita que seus estudantes se sentem motivados ao trabalhar com estes números. Apresentaremos no capítulo 2 uma proposta de sequência didática, a qual busca tratar a questão da motivação dos estudantes, através da inserção de um *software* de geometria dinâmica.

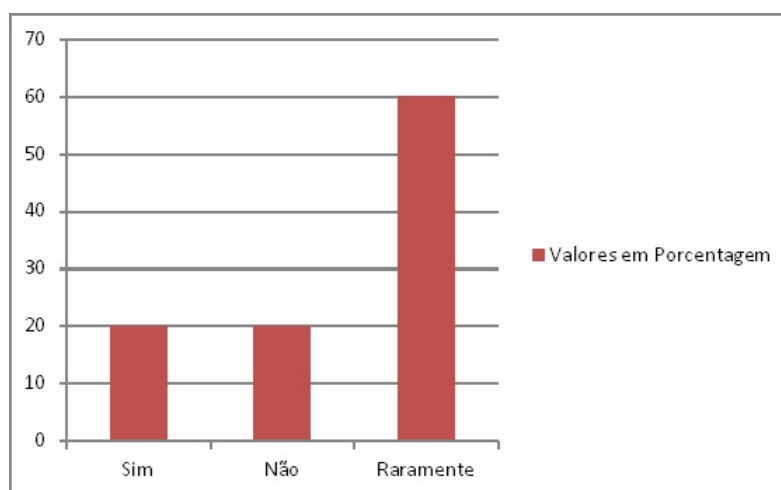


Figura 1.13: Resultados da questão 1 – Questionário dos professores

1.3.2 Questão 2 – Resultados e discussões

- 2) Os alunos conseguem identificar alguma aplicação dos números complexos associada à realidade?
 a) Sim
 b) Não
 c) Raramente
 Se sim, qual (is)?

Figura 1.14: Questão 2 – Questionário dos professores

O gráfico abaixo demonstra que 100% dos professores atestam que os seus alunos não identificam aplicações dos complexos associados à realidade.

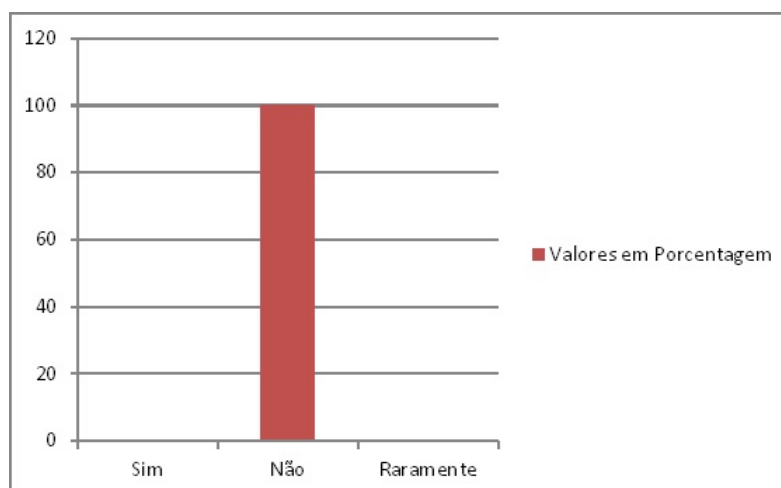


Figura 1.15: Resultados da questão 2 – Questionário dos professores

1.3.3 Questões 3, 4 e 5 – Resultados e discussões

As questões 3, 4 e 5 do questionário aplicado para os docentes estão inter-relacionadas, por este motivo apresentaremos tais questões, bem como a análise destas de forma concomitantemente.

- 3) Sendo $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e \mathbb{C} os conjuntos dos naturais, inteiros, racionais, reais e complexos, respectivamente e motivado pela sucessão de inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, você acredita que existe um conjunto X tal que $\mathbb{C} \subset X$?
 a) Sim
 b) Não

Figura 1.16: Questão 3 – Questionário dos professores

As questões induzem a discussão, de forma paulatina, sobre a finitude ou não da sequência de inclusões: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Aqui, destaca-se, que, de forma

- 4) Caso tenha respondido sim na questão anterior, você acredita que existe um conjunto Y tal que $X \subset Y$?
- Sim
 - Não

Figura 1.17: Questão 4 – Questionário dos professores

- 5) Caso tenha respondido sim na questão anterior, você julga a sucessão $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset X \subset Y$ é:
- finita
 - infinita

Figura 1.18: Questão 5 – Questionário dos professores

subliminar, indaga-se sobre o conhecimento do docente sobre a existência dos quatérnios e octônios. Além disso, a questão 5 questiona sobre o conhecimento específico do docente com respeito a um teorema do tipo do que apresentaremos na seção 6.3.

Abaixo apresentamos as respostas dos docentes às questões 3, 4 e 5.

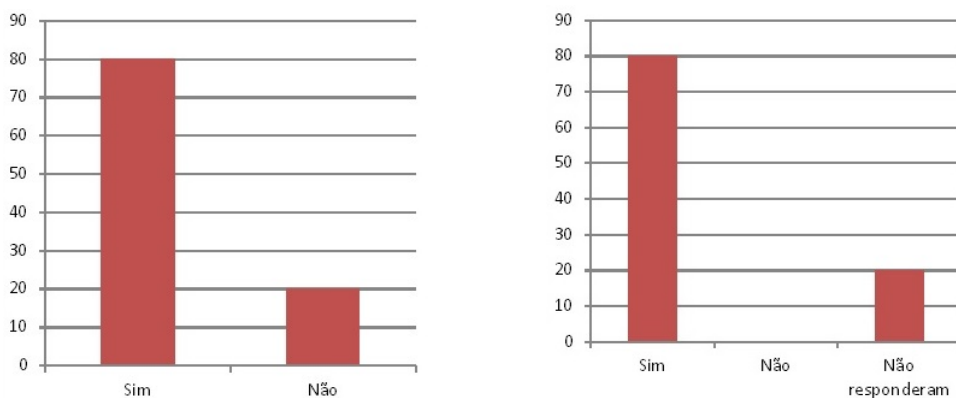


Figura 1.19: Resultados das questões 3 e 4 – Questionário dos professores

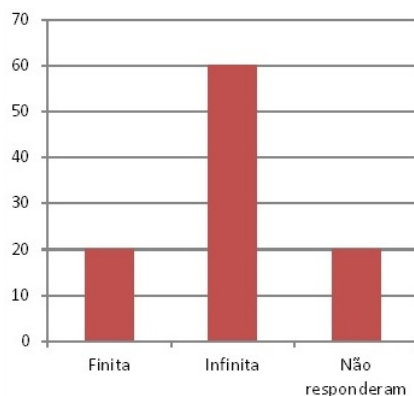


Figura 1.20: Resultados da questão 5 – Questionário dos professores

A partir da análise dos questionários concluí-se que embora 80% dos professores, tenham respondido corretamente às questões 3 e 4, o quantitativo de 60% dos professores afirmam, erroneamente, que a referida sucessão de inclusões é infinita. Neste ponto,

destaque-se que a questão foi formulada com as hipóteses do teorema de Frobenius (veja a seção 6.3).

Capítulo 2

Uma proposta de sequência didática

2.1 Fundamentação teórica

Os resultados obtidos no capítulo 1, a partir dos questionários aplicados para estudantes e professores, reafirmam as informações/discussões apresentadas na introdução, no que tange aos obstáculos oriundos das relações de ensino, os quais podem influenciar no aprendizado dos estudantes. Também reforçam as discussões vistas em [18], face aos livros didáticos analisados.

Assumindo como referência a análise dos questionários apresentados no capítulo 1, observa-se que existem vários pontos das relações de ensino e aprendizagem que merecem uma atenção especial dos professores. No entanto, face aos objetivos do presente trabalho, escolhemos um item desta lista de elementos, o qual merece uma atenção especial, a saber: **a motivação dos estudantes para estudar os números complexos** (haja vista que 80% dos alunos não apresentam motivação ou raramente apresentam motivação para o estudo dos números complexos, na visão dos professores que participaram da pesquisa), para apresentar uma contribuição na direção de trabalhar este aspecto, o qual compreendemos de extrema relevância, principalmente, no ciclo básico de ensino. Assim sendo, apresentamos uma sequência didática¹ estruturada a partir de um eixo central, a saber: uma questão desafiadora/motivadora.

Para além das questões de aprendizagem dos estudantes, referidas anteriormente, buscamos contribuir com a discussão sobre os processos de ensino, inserindo o *software* livre Geogebra² no desenvolvimento das atividades propostas, buscando contribuir, desta forma, com o desenvolvimento dos conteúdos procedimentais e atitudinais, favorecendo

¹uma sequência didática é uma sequência de atividades as quais precisam ser sequenciadas de acordo com uma proposta de progressão de desafios ou de problemas a serem resolvidos pelos alunos. ([21], 2006, p. 34).

²O Geogebra foi criado por Markus Hohenwarter. Existem inúmeros tutoriais disponíveis para consulta sobre o Geogebra, veja, por exemplo, [16].

o aprendizado do estudante a partir da (re)significação dos conceitos. Neste contexto, apresentaremos alguns conceitos sobre números complexos e, em seguida, propomos o estudo destes conceitos associados ao Geogebra. Ressalta-se que esta abordagem não visa construir uma lista de exercícios, ou mesmo esgotar todo o conhecimento sobre os tópicos apresentados, esta metodologia visa, tão somente, contribuir com a reflexão sobre a importância deste estudo, associado ao Geogebra. Assim sendo, apresentaremos, a solução de alguns exercícios como habitualmente são resolvidos no ensino básico e, em seguida, faremos a discussão das soluções destes exercícios usando o Geogebra, permitindo uma reflexão sobre estas diferentes abordagens.

2.2 Conceitos básicos sobre números complexos

Nossa principal referência para esta seção foi o livro [31].

Definição 2.2.1. *Definimos o conjunto dos números complexos, e denotamos por \mathbb{C} , como sendo um conjunto no qual estão definidas as operações de adição (indicada pelo sinal $+$) e de multiplicação (indicado pela simples justaposição de letras) satisfazendo as seguintes propriedades:*

- (1) *A adição e a multiplicação são comutativas, isto é, se z_1 e z_2 são números complexos, então $z_1 + z_2 = z_2 + z_1$ e $z_1 \cdot z_2 = z_2 \cdot z_1$.*
- (2) *A adição e a multiplicação são associativas, isto é, se z_1, z_2, z_3 são números complexos, $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$ e $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$.*
- (3) *A multiplicação é distributiva relativamente à adição, isto é, se z_1, z_2, z_3 são números complexos, $z_1(z_2 + z_3) = z_1z_2 + z_1z_3$.*
- (4) *Existem e são únicos os números 0 e 1 satisfazendo as condições: $z_1 + 0 = z_1$ e $z_1 \cdot 1 = z_1$, para todo z_1 complexo.*
- (5) *A todo complexo z_1 corresponde um único número complexo $(-z_1)$, e se $z_1 \neq 0$, um único número complexo $\frac{1}{z_1}$, tais que $z_1 + (-z_1) = 0$ e $z_1 \cdot \frac{1}{z_1} = 1$.*
 - (a) *Existe um número complexo $i \in \mathbb{C}$ com $i^2 = -1$;*
 - (b) *Todo número complexo pode ser escrito de uma maneira única na forma $z = a + bi$ com a e b números reais (a é chamado parte real e b parte imaginária do complexo $a + bi$). Usa-se a notação $Re(a + bi) = a$ e $Im(a + bi) = b$.*

Observação 2.2.2. *Decorre da definição que todo número real é também um número complexo.*

Definição 2.2.3. Dados dois complexos $w, z \neq 0$, definimos o quociente $\frac{w}{z}$ como sendo o produto $w \left(\frac{1}{z} \right)$.

A partir desta definição surge a seguinte questão:

Questão 2.2.4. Dado um número complexo $0 \neq z = a + bi$ existem c, d reais, tais que $\frac{1}{z} = c + di$? Para responder a esta questão, observe, inicialmente, que dado um número complexo $z \neq 0$, deve existir um complexo $\frac{1}{z}$ tal que $z \frac{1}{z} = 1$. Para determinar o complexo $\frac{1}{z}$, $z \neq 0$, na forma $c + di$, convém definir:

- (a) o conjugado de um número complexo $z = a + bi$ como o número complexo $\bar{z} = a - bi$.
- (b) o módulo de um número complexo $z = a + bi$, denotado por $|z|$, como sendo o número real não negativo $|z| = \sqrt{a^2 + b^2}$.

Observação 2.2.5. Decorre de (a) e (b) acima que o produto de um complexo z pelo seu conjugado é igual ao quadrado do módulo de z . De fato, $z\bar{z} = (a + bi)(a - bi) = a^2 + b^2$.

Agora, com base nas discussões acima, podemos responder a questão 2.2.4, da seguinte forma.

Note, inicialmente, que $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2}$. Como $z = a + bi$, temos que

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

Ou seja, nas condições da questão 2.2.4, temos que $c = \frac{a}{a^2 + b^2}$ e $d = -\frac{b}{a^2 + b^2}$.

Definição 2.2.6. Sejam $\alpha \in \mathbb{R}$ e $z = a + bi \in \mathbb{C}$, definimos a multiplicação $\alpha \cdot z$ como sendo $\alpha \cdot z_1 = \alpha \cdot (a + bi) = \alpha \cdot a + \alpha \cdot bi$.

As questões 2.2.7, 2.2.8, 2.2.9 e 2.2.10, a seguir, serão resolvidas com base nas discussões acima. As soluções destas questões exigem apenas a aplicação direta das definições. Apresentamos tais exercícios, pois na próxima seção retomaremos com as soluções, utilizando o Geogebra, o que permitirá uma reflexão sobre os processos de ensino e aprendizagem, notadamente, no que tange a utilização, neste contexto, do software Geogebra.

Questão 2.2.7. Sendo $z_1 = -3 + 6i$ e $z_2 = 5 - 2i$, temos que:

$$(a) \quad z_1 + z_2 = (-3 + 5) + (6 + (-2))i = 2 + 4i.$$

$$(b) z_1 - z_2 = (-3 - (+5)) + (6 - (-2))i = -8 + 8i.$$

$$(c) z_1 \cdot z_2 = (-3 + 6i) \cdot (5 - 2i) = ((-3) \cdot 5 - 6 \cdot (-2)) + ((-3) \cdot (-2) + 6 \cdot 5)i = (-15 + 12) + (6 + 30)i = -3 + 36i.$$

$$(d) \frac{z_1}{z_2} = \frac{(-3) \cdot 5 + 6 \cdot (-2)}{5^2 + (-2)^2} + i \cdot \frac{6 \cdot 5 - (-3) \cdot 6}{5^2 + (-2)^2} = \frac{-15 - 12}{25 + 4} + i \cdot \frac{15 + 18}{25 + 4} = \frac{-27}{29} + i \cdot \frac{33}{29}.$$

Questão 2.2.8. Sendo z_1, z_2, z_3 e z_4 vetores obtidos no exercício anterior, determine $\frac{z_1 \cdot z_2 + z_3}{z_4}$. Inicialmente, deve-se calcular $z_1 \cdot z_2$. Esta etapa já foi cumprida anteriormente, sendo $z_1 \cdot z_2 = -3 + 36i$. Posteriormente, deve-se calcular $(-3 + 36i) + z_3$. A partir da definição de adição de complexos tem-se que $(-3 + 36i) + (2 + 4i) = -1 + 40i$. Finalmente, deve-se calcular $\frac{-1 + 40i}{z_4} = \frac{-1 + 40i}{-8 + 8i}$. A partir da definição de divisão de complexos, tem-se que $\frac{z_1 \cdot z_2 + z_3}{z_4} = 2,56 + 2,44 \cdot i$

Questão 2.2.9. Sendo $z = 1 + 2i$ e $w = -2 + 3i$, temos que:

$$(a) (1 + 2i) \cdot i = i + 2i^2 = i - 2 = -2 + i.$$

$$(1 + 2i) \cdot (-i) = -i - 2i^2 = i + 2 = 2 + i.$$

$$(b) (-2 + 3i) \cdot i = -2i + 3i^2 = -2i - 3 = -3 - 2i.$$

$$-2 + 3i \cdot (-i) = 2i - 3i^2 = -2i + 3 = 3 - 2i.$$

Questão 2.2.10. Dados os complexos $z = 1 + 2i$ e $w = -2 + 3i$, temos que

$$(a) (1 + 2i) \cdot (-1) = 1 \cdot (-1) + 2i \cdot (-1) = -1 - 2i.$$

$$(1 + 2i) \cdot 0 = 1 \cdot 0 + 2i \cdot 0 = 0.$$

$$(1 + 2i) \cdot \frac{1}{2} = 1 \cdot \frac{1}{2} + 2i \cdot \frac{1}{2} = \frac{1}{2} + i.$$

$$(1 + 2i) \cdot 3 = 1 \cdot 3 + 2i \cdot 3 = 3 + 6i.$$

$$(b) (-2 + 3i) \cdot (-1) = -2 \cdot (-1) + 3i \cdot (-1) = 2 - 3i.$$

$$(-2 + 3i) \cdot 0 = -2 \cdot 0 + 3i \cdot 0 = 0.$$

$$(-2 + 3i) \cdot \frac{1}{2} = -2 \cdot \frac{1}{2} + 3i \cdot \frac{1}{2} = -1 + \frac{3}{2}i.$$

$$(-2 + 3i) \cdot 3 = -2 \cdot 3 + 3i \cdot 3 = -6 + 9i.$$

É possível associar o número complexo $z = a + bi$ como o ponto (a, b) do plano, cujas coordenadas são a e b , com isto, temos que o complexo z pode ser representado pelo vetor \overrightarrow{Oz} .³ Veja a figura abaixo.

³O ponto (a, b) é chamado de imagem do complexo $z = a + bi$ e os números a e b são chamados componentes do vetor \overrightarrow{Oz} .

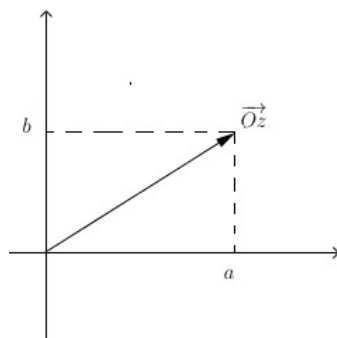


Figura 2.1: Representação geométrica de complexos

As figuras 2.2 e 2.3 representam, geometricamente, a soma e a diferença dos números complexos $z_1 = a + bi$ e $z_2 = c + di$.

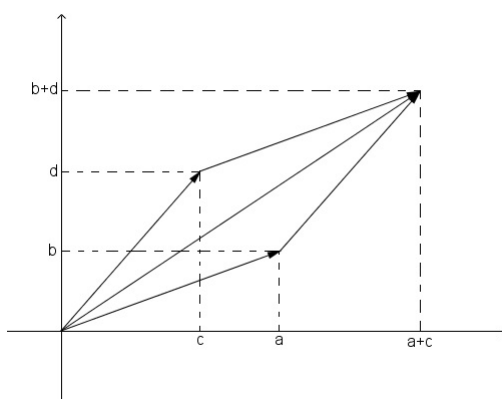


Figura 2.2: Interpretação geométrica da adição de complexos

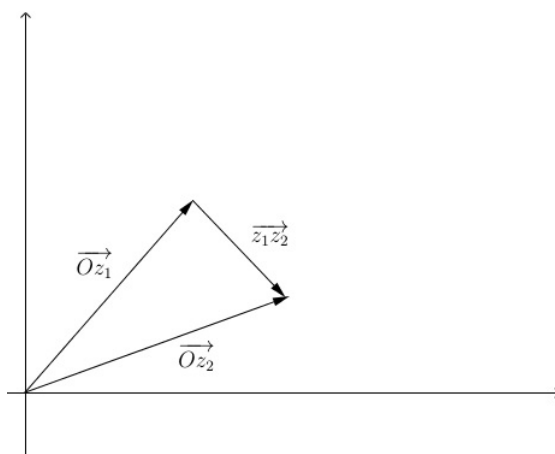


Figura 2.3: Interpretação geométrica da subtração de complexos

A figura 2.4 nos dá uma interpretação geométrica do módulo de um número complexo z .

Observação 2.2.11. *Ainda do ponto de vista geométrico, é fácil ver que dado um número*

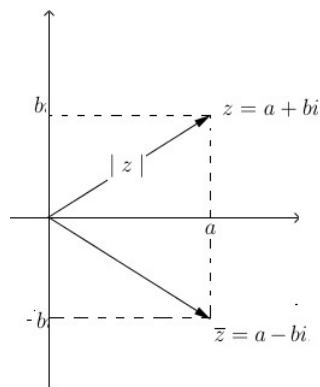


Figura 2.4: Interpretação geométrica do conjugado de um complexo

complexo z o seu módulo, $|z|$, mede o módulo do vetor que representa este complexo.

É também possível estabelecer uma interpretação geométrica para a multiplicação de números complexos.⁴ Para tanto, consideremos o número complexo $z = a + bi$ e $r = |z| = \sqrt{a^2 + b^2}$ o seu módulo, o qual vamos supor não nulo. Consideremos, ainda, o ângulo positivo θ , conforme a figura abaixo.

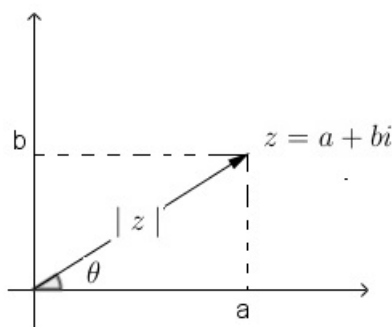


Figura 2.5: Complexo e coordenadas trigonométricas

Da trigonometria, sabemos que $\frac{a}{r} = \cos \theta$ e $\frac{b}{r} = \sin \theta$. Com isto, podemos escrever:

$$\begin{aligned} z &= a + bi \\ &= r \cos \theta + ir \sin \theta \\ &= r(\cos \theta + i \sin \theta) \end{aligned}$$

A representação $z = r(\cos \theta + i \sin \theta)$ é chamada *forma trigonométrica* do complexo z .

Observação 2.2.12. Observe que substituindo θ na expressão acima $\theta + 2k\pi$, em que k é um inteiro positivo, negativo ou nulo, o complexo z não se altera. Em muitos casos é conveniente usar esta expressão mais geral: $z = r(\cos(\theta + 2k\pi) + i \sin(\theta + 2k\pi))$.

⁴Para maiores detalhes, veja, por exemplo, os capítulos 6 e 7 de [31].

A partir da forma trigonométrica dos números complexos é possível estabelecer uma interpretação geométrica da operação de multiplicação de complexos. Para tanto, consideremos, inicialmente, dois complexos unitários z e w . Desta forma, temos que:

$$\begin{aligned} zw &= [\cos(\theta_1) + i \sin(\theta_1)] \cdot [\cos(\theta_2) + i \sin(\theta_2)] \\ &= \cos(\theta_1) \cos(\theta_2) + i \cos(\theta_1) \sin(\theta_2) + i \sin(\theta_1) \cos(\theta_2) - \sin(\theta_1) \sin(\theta_2) \\ &= \cos(\theta_1) \cos(\theta_2) - \sin(\theta_1) \sin(\theta_2) + i(\cos(\theta_1) \sin(\theta_2) + \sin(\theta_1) \cos(\theta_2)) \\ &= \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2) \end{aligned}$$

A figura abaixo ilustra a multiplicação de dois complexos unitários z e w .

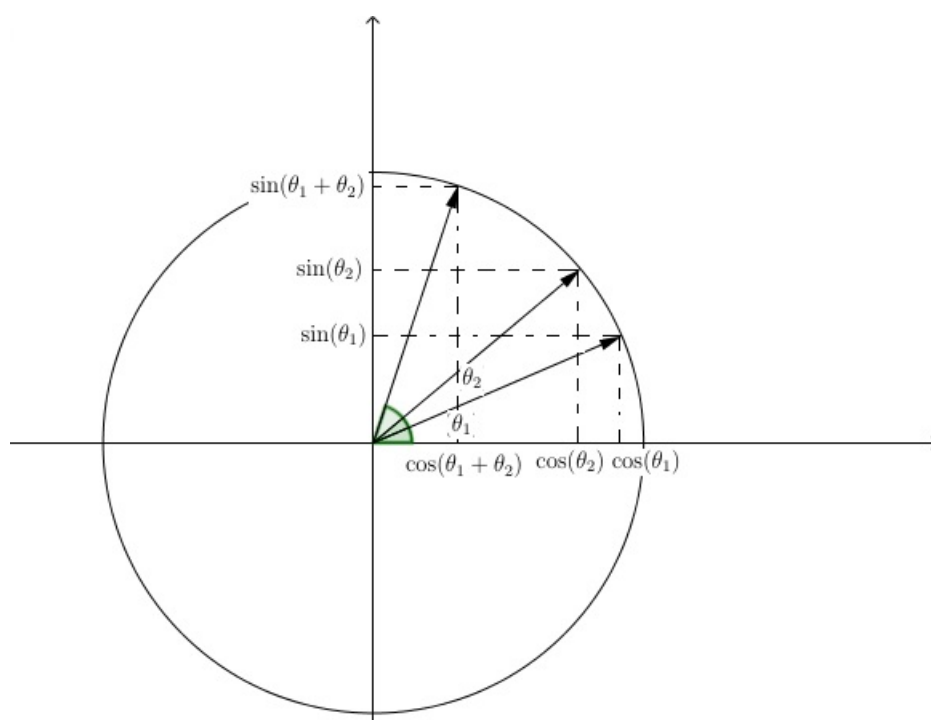


Figura 2.6: Multiplicação de complexos unitários

Conclusão: multiplicar dois complexos unitários w_1 e w_2 significa, geometricamente, dar a um deles uma rotação positiva de ângulo igual ao ângulo do outro.

No caso de dois complexos não serem unitários, z_1 e z_2 escrevemos $z_1 = r_1 w_1$ e $z_2 = r_2 w_2$, com $|w_1| = |w_2| = 1$, e o produto será simplesmente: $z_1 z_2 = r_1 w_1 r_2 w_2 = r_1 r_2 w_1 w_2$.

As questões 2.2.13 e 2.2.14 serão resolvidas com base nas discussões acima. Apresentamos tais exercícios, pois na próxima seção retomaremos com as soluções, utilizando o Geogebra, o que, conforme já mencionado, permitirá uma reflexão sobre os processos de ensino e aprendizagem, notadamente, no que tange a utilização, neste contexto, do software Geogebra.

Questão 2.2.13. *Encontre as novas coordenadas do ponto $A(3,4)$ após uma rotação de 90° no sentido anti-horário em relação a origem. Denotemos por $A'(x,y)$ o ponto obtido após esta rotação. Para resolver esta questão, observe, inicialmente, que o ponto $A(3,4)$ representa geometricamente o complexo $z_1 = 3 + 4i$. Daí, uma rotação de 90° no sentido anti-horário significa uma multiplicação de z_1 por i , como visto anteriormente. Portanto, $A' = (3 + 4i) \cdot i = -4 + 3i = (-4, 3)$.*

Questão 2.2.14. *Encontre as novas coordenadas do segmento \overline{AB} com $A(2,2)$ e $B(4,5)$ após uma rotação de 90° no sentido anti-horário em torno do ponto A . Procedendo como na questão anterior, observa-se que o ponto $A(2,2)$ e o ponto $B(4,5)$ representam geometricamente os complexos $z_1 = 2 + 2i$ e $z_2 = 4 + 5i$, respectivamente. Como a rotação ocorrerá em relação ao ponto A devemos realizar a rotação apenas do complexo t equivalente a diferença entre z_2 e z_1 , ou seja, $t = (4 + 5i) - (2 + 2i) = 2 + 3i$ e por fim somar t a z_1 . Através dos exemplos anteriores nota-se que rotacionar 90° em sentido anti-horário corresponde a multiplicar t por i . Assim,*

$$\begin{aligned} B' &= (t \cdot i) + z_1 \\ &= [(z_2 - z_1) \cdot i] + z_1 \\ &= [(2 + 3i) \cdot i] + z_1 \\ &= (-3 + 2i) + 2 + 2i \\ &= -1 + 4i \end{aligned}$$

Dessa forma, o segmento \overline{AB} rotacionado em torno de A em 90° se tornará o segmento $\overline{AB'}$, em que $A = (2,2) = 2 + 2i$ e $B' = (-1,4) = -1 + 4i$.

2.3 Sequência didática

Segue abaixo uma proposta de sequência didática que visa auxiliar no ensino aprendido das operações com números complexos. No desenvolvimento da sequência didática será apresentada a solução de cada atividade com o auxílio do Geogebra.

2.3.1 Roteiro da sequência didática

- Tema: “Movimentos complexos”;
- Público Alvo: 3º ano (ensino médio);

- **Problematização:** Sabendo que os complexos admitem uma representação geométrica, é natural a indagação quanto à interpretação geométrica das operações com complexos⁵;
- **Pré-requisitos de conteúdo:** Noções básicas do Geogebra;
- **Objetivos:** Analisar o efeito rotação no plano complexo, de forma contextualizada, possibilitando ao estudante o desenvolvimento de intuição sobre o comportamento das operações com os números complexos, as quais poderão ser apresentadas na sequência à esta atividade, pelo professor da disciplina;
- **Estimativa de Tempo de Duração desta atividade:** 1, 5h (uma hora e trinta minutos);
- **Avaliação:** A cada passo da atividade, o professor acompanha o desenvolvimento e realiza as intervenções necessárias, por meio de observação e registros variados, tendo como referência o aluno por ele mesmo. Conforme o andamento, o professor avalia a necessidade de replanejamento e/ou disponibilidade e organização do tempo e das atividades;
- **Desenvolvimento:** A atividade consiste na realização dos exercícios de iniciação apresentados abaixo, seguidos de uma atividade que visa induzir os alunos a investigar a interpretação geométrica da multiplicação de complexos não-nulos pelo complexo i e, finalmente, a resolução de uma situação problema proposta.

2.3.2 Atividade 1 - Exercícios de iniciação aos números complexos

Conforme mencionado anteriormente, retomaremos os exercícios apresentados na seção anterior, agora resolvendo-os com o auxílio do Geogebra. Assim sendo, considere os números complexos $z_1 = -3 + 6i$ e $z_2 = 5 - 2i$, vamos determinar $z_1 + z_2$, $z_1 - z_2$, $z_1 \cdot z_2$ e $\frac{z_1}{z_2}$, usando o Geogebra.

Solução utilizando o Geogebra 2.3.2.1. *Introduzir no Geogebra, especificamente no “campo de entrada” os complexos z_1 e z_2 . Para tanto, siga os seguintes passos:*

(1) *Digitar no campo de entrada o comando “ $-3 + 6i$ ”, para introduzir z_1 ;*

(2) *Digitar no campo de entrada o comando “ $5 - 2i$ ”, para introduzir z_2 ;*

⁵Ressalte-se que esta indagação esta intimamente relacionada com a motivação do William Rowan Hamilton, ao iniciar os estudos sobre os quatérnios

Já com os complexos z_1 e z_2 expostos no Geogebra, para realizar as operações solicitadas, basta introduzir no campo de entrada os comandos exibidos nas aspas abaixo.

(a) $z_1 + z_2 = z_3 = "z_1 + z_2";$

(b) $z_1 - z_2 = z_4 = "z_1 - z_2";$

(c) $z_1 \cdot z_2 = z_5 = "z_1 * z_2";$

(d) $\frac{z_1}{z_2} = z_6 = "z_1/z_2".$

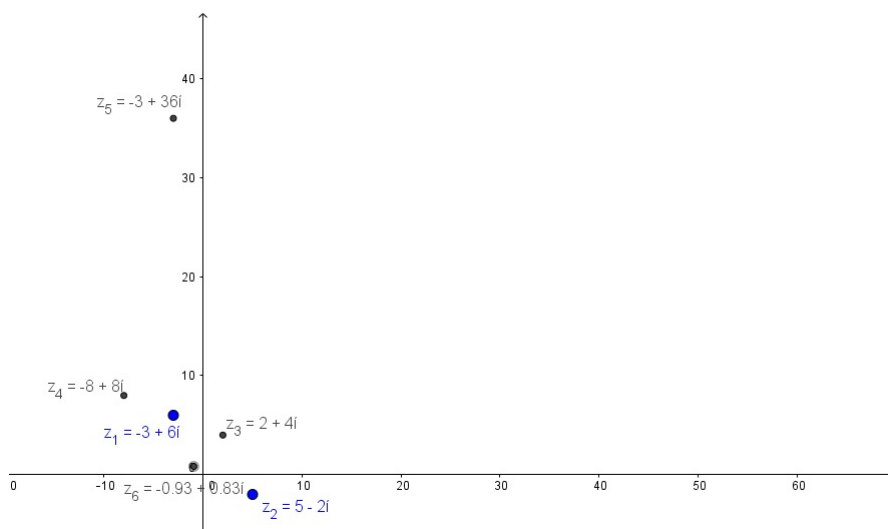


Figura 2.7: Operações com complexos

Retornaremos ao exercício 2.2.8, agora, resolvendo-o com o auxílio do Geogebra.

Solução utilizando o Geogebra 2.3.2.2. *Parte do trabalho já foi executado anteriormente, pois já temos os vetores z_1, z_2, z_3 e z_4 inseridos. A partir daí, digite no campo de entrada o comando $"(z_1 * z_2 + z_3)/z_4"$, obtendo o vetor $z_5 = 2,56 + 2,44 \cdot i$.*

Compare as soluções apresentadas acima com as soluções analíticas (Questões 2.2.7 e 2.2.8).

2.3.3 Atividade 2 - Análise investigativa da multiplicação de complexos não-nulos pelos complexo i e $-i$

O exercício abaixo busca desenvolver aspectos de investigação quanto à interpretação geométrica da multiplicação de complexos não-nulos pelo complexo i e $-i$. Os complexos apresentados serão os mesmos da questão 2.2.9.

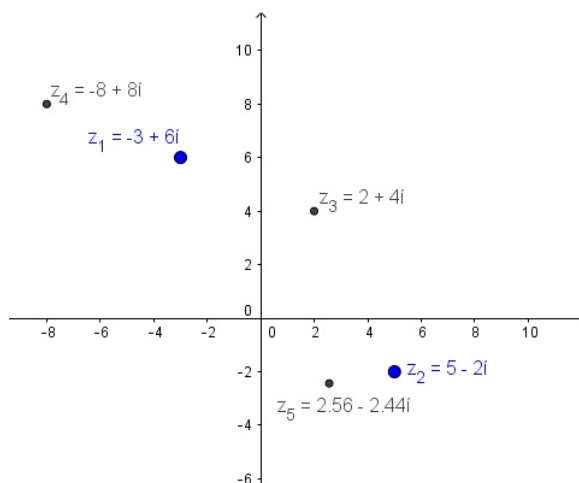


Figura 2.8: Operações com complexos

Questão 2.3.1. Usando o Geogebra, determine $(1 + 2i) \cdot i$, $(1 + 2i) \cdot (-i)$, $(-2 + 3i) \cdot i$ e $(-2 + 3i) \cdot (-i)$.

Solução utilizando o Geogebra 2.3.3.1. Para obter o resultado da multiplicação por i e $-i$, seguiremos passos semelhantes aos expostos no exercício anterior. Mais especificamente, digite no campo de entrada do Geogebra $1 + 2i$ e $-2 + 3i$ para inserir os complexos desejados como z_1 e z_2 . Posteriormente, para efetuar a multiplicação por i , digitemos no campo de entrada os comandos abaixo, efetuando a multiplicação por i e $-i$. Os vetores z_3 , z_4 , z_5 e z_6 representaram, respectivamente, $(1 + 2i) * i$, $(1 + 2i) * (-i)$, $(-2 + 3i) * i$ e $(-2 + 3i) * (-i)$.

- (a) “ $z_3 = z_1 * i$ ”
 “ $z_4 = z_1 * (-i)$ ”
- (b) “ $z_5 = z_2 * i$ ”
 “ $z_6 = z_2 * (-i)$ ”

Para complementar o exercício utilize a opção “Vetor”, demarcando os vetores associados aos complexos z_1, z_2, z_3, z_4, z_5 e z_6 . Ao fim destes passos, a imagem obtida deverá ser semelhante à imagem abaixo.

Questão 2.3.2. Agora, vamos investigar, usando o Geogebra qual foi a rotação proporcionada pela multiplicação por i e por $-i$, aferindo o ângulo formado entre os vetores z_1 e z_3 , z_1 e z_4 , z_2 e z_5 , z_2 e z_6 .

Solução utilizando o Geogebra 2.3.3.2. Para aferir o menor ângulo entre os respectivos vetores deve-se utilizar a opção “Ângulo”. Por exemplo, clicando no par de vetores

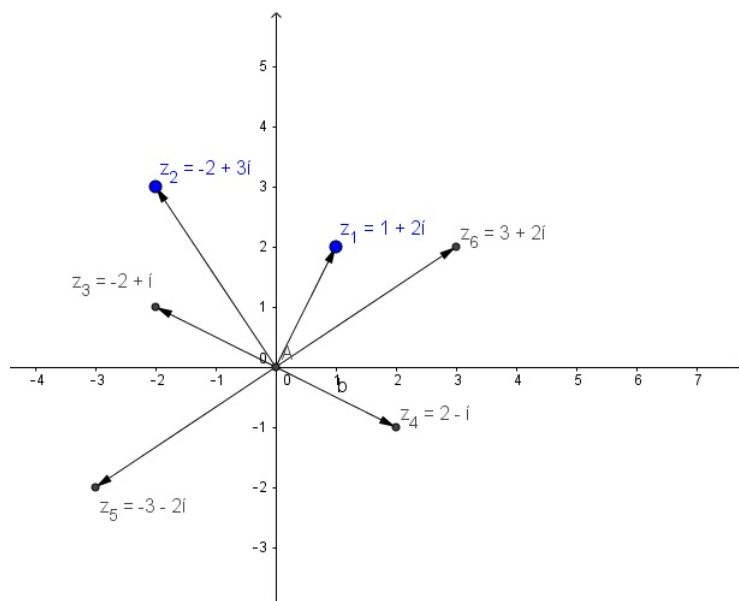


Figura 2.9: Operações com complexos

z_1 e z_3 a imagem obtida será como abaixo e a informação de que o ângulo α entre z_1 e z_3 é igual a 90° . De maneira análoga, pode-se obter o menor ângulo formado pelos vetores associados à z_1 e z_4 , z_2 e z_5 , z_2 e z_6 . Tais ângulos são, respectivamente, iguais a 90° .

Observação 2.3.3. De modo análogo, pode-se utilizar z_2 , z_5 e z_6 . Além disso, um exercício natural seria investigar quanto à multiplicação de z_1 e z_2 por outros complexos como por exemplo $\frac{i}{2}$, $2i$ e outros. Neste caso, se observará a variação do módulo e a rotação proporcionada ao efetuar tais multiplicações.

A figura abaixo ilustra a forma a qual deve-se obter o ângulo entre z_1 e z_3 .

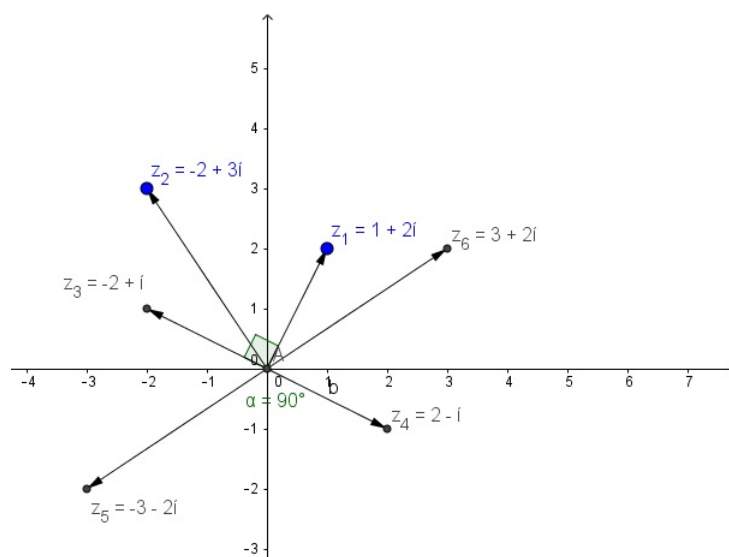


Figura 2.10: Operações com complexos

2.3.4 Atividade 4 - Análise investigativa da multiplicação de complexos não-nulos por números reais

O exercício abaixo visa auxiliar na interpretação geométrica da multiplicação de complexos não-nulos por números reais.

Questão 2.3.4. Usando o Geogebra, realize a multiplicação dos números complexos $z = 1 + 2i$ e $w = -2 + 3i$ por $-1, 0, \frac{1}{2}$ e 3 .

Solução utilizando o Geogebra 2.3.4.1. Para obter o resultado da multiplicação por $-1, 0, \frac{1}{2}$ e 3 , digite no campo de entrada do Geogebra $1 + 2i$ e $-2 + 3i$ para para inserir os complexos desejados como z_1 e z_2 . Posteriormente, para efetuar a multiplicação por $-1, 0, \frac{1}{2}$ e 3 , digita-se no campo de entrada os comandos abaixo, efetuando a multiplicação por $-1, 0, \frac{1}{2}$ e 3 . Os vetores z_3, z_4, z_5 e z_6 representaram, respectivamente, $(1 + 2i) \cdot (-1)$, $(1 + 2i) \cdot 0$, $(1 + 2i) \cdot \frac{1}{2}$ e $(1 + 2i) \cdot 3$. Analogamente os vetores z_7, z_8, z_9 e z_{10} representaram, respectivamente, $(-2 + 3i) \cdot (-1)$, $(-2 + 3i) \cdot 0$, $(-2 + 3i) \cdot \frac{1}{2}$ e $(-2 + 3i) \cdot 3$.

$$(a) \text{ “}z_3 = z_1 * (-1)\text{”}$$

$$\text{“}z_4 = z_1 * 0\text{”}$$

$$\text{“}z_5 = z_1 * \frac{1}{2}\text{”}$$

$$\text{“}z_6 = z_1 * 3\text{”}$$

$$(b) \text{ “}z_7 = z_2 * (-1)\text{”}$$

$$\text{“}z_8 = z_2 * 0\text{”}$$

$$\text{“}z_9 = z_2 * \frac{1}{2}\text{”}$$

$$\text{“}z_{10} = z_2 * 3\text{”}$$

Depois de introduzidos os respectivos comandos, serão obtidas as imagens abaixo com os complexos resultantes das multiplicações. A primeira imagem apresenta os complexos resultantes do item *a*) e a segunda imagem apresenta os complexos resultantes do item *b*). Segue abaixo outra sugestão de exercício a ser construída apenas com o auxílio do Geogebra. O exercício busca despertar a percepção sobre a “influência” da multiplicação de complexos aleatórios por números reais também aleatórios, para tanto será utilizada uma das ferramentas do Geogebra: “o controle deslizante”.

Questão 2.3.5. Utilizando o Geogebra observe o que ocorre com os complexos $1 + 2i$ e $-2 + 3i$ quando multiplicamos os mesmos por respectivos números reais a e b aleatórios?

Para investigar as multiplicações citadas acima, vamos introduzir os comandos abaixo no campo de entrada. O próprio Geogebra irá sugerir a criação de controles

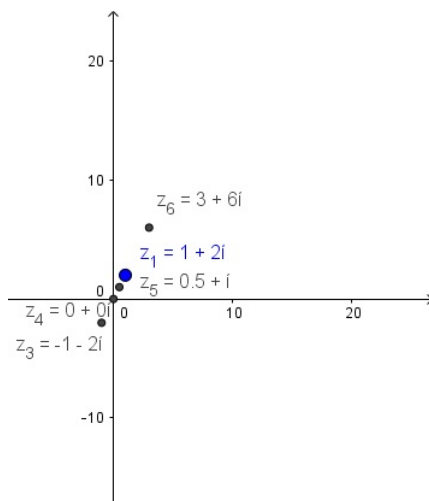


Figura 2.11: Operações com complexos - item a)

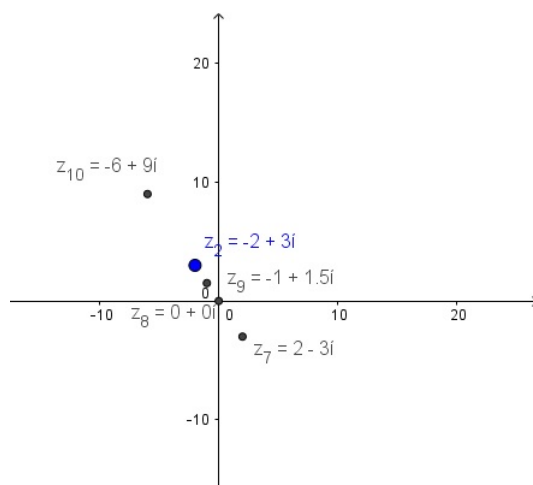


Figura 2.12: Operações com complexos - item b)

deslizantes. Após a criação de tais controles, questiona-se: “Qual(is) modificações podem ser notadas no complexo ao multiplicar o mesmo por números reais variados?”

Solução utilizando o Geogebra 2.3.4.2. *As respostas para a indagação proposta podem ser obtida através da construção abaixo.*

- a) *Introduza no campo de entrada o comando “ $z_1 = 1 + 2i$ ” para introduzir o complexo z_1 ;*
*Digite no campo de entrada o comando “ $z_1 * a$ ” e aceite a criação do controle deslizante a , obtendo um complexo z_3 ;*
Habilite o “rastros” do afixo referente ao complexo z_3 .
- b) *Introduza no campo de entrada o comando “ $z_2 = -2 + 3i$ ” para introduzir o complexo z_2 ;*

Digite no campo de entrada o comando “ $z_2 * b$ ” e aceite a criação do controle deslizante b , obtendo um complexo z_4 ;

Habilite o “rastros” do afixo referente ao complexo z_4 .

Por fim movimente os controles deslizantes e responda os questionamentos. A imagem obtida será semelhante à exibida abaixo, após a inserção dos comandos citados acima.

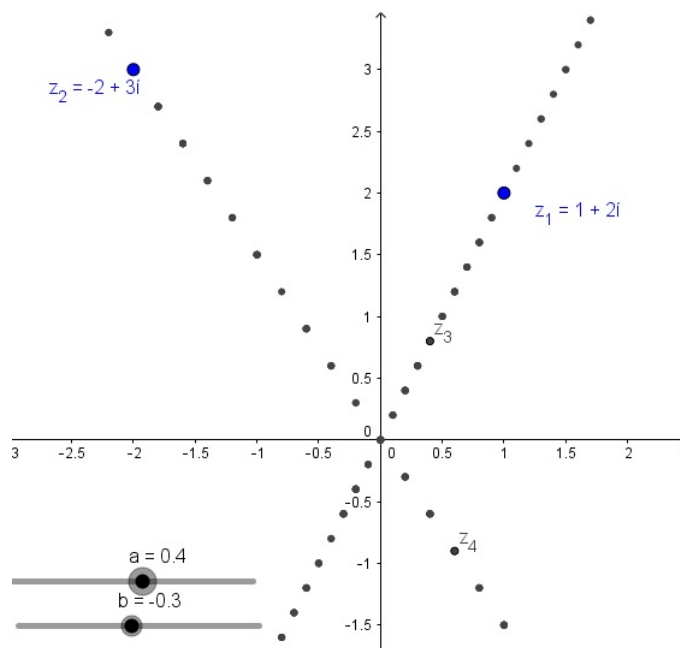


Figura 2.13: Operações com complexos - item b)

2.3.5 Atividade 4 - Situação Problema

Neste ponto, atingimos a culminância da sequência didática, apresentando uma situação problema, resolvendo-a, inicialmente, com o auxílio do Geogebra e, em seguida, apresentando sua solução analítica.

Situação Problema 2.3.5.1. *Um jovem, chamado José, ao casar-se com Luane, ganhou de presente do seu pai, uma área de terra, na qual passava o rio Esperança do Sul. Tal rio era rico em peixes. Daí, José decidiu tornar-se pescador. Para facilitar seu trabalho, José costumava demarcar sua área de pesca com varetas de madeira. No entanto, em certa ocasião, devido a uma forte tempestade, a correnteza, associada aos fortes ventos, arrancarrou duas dessas varetas.*

Sabendo-se que a área de pesca do José tem formato quadrangular, cujas marcações das varetas representam dois vértices consecutivos deste quadrado. A questão do José é a seguinte: como descobrir a posição das varetas arrancadas?

Seja o segmento \overline{AB} um lado de um quadrado determinado pela área de pesca cujas coordenadas de A e B são $A = (1,1)$ e $B = (3,2)$. Determine os outros vértices do quadrado para que os pescadores voltem a ter determinada a sua área de pesca, sabendo que a área se encontra ao norte da ponte. A situação proposta pode ser ilustrada na figura abaixo.⁶

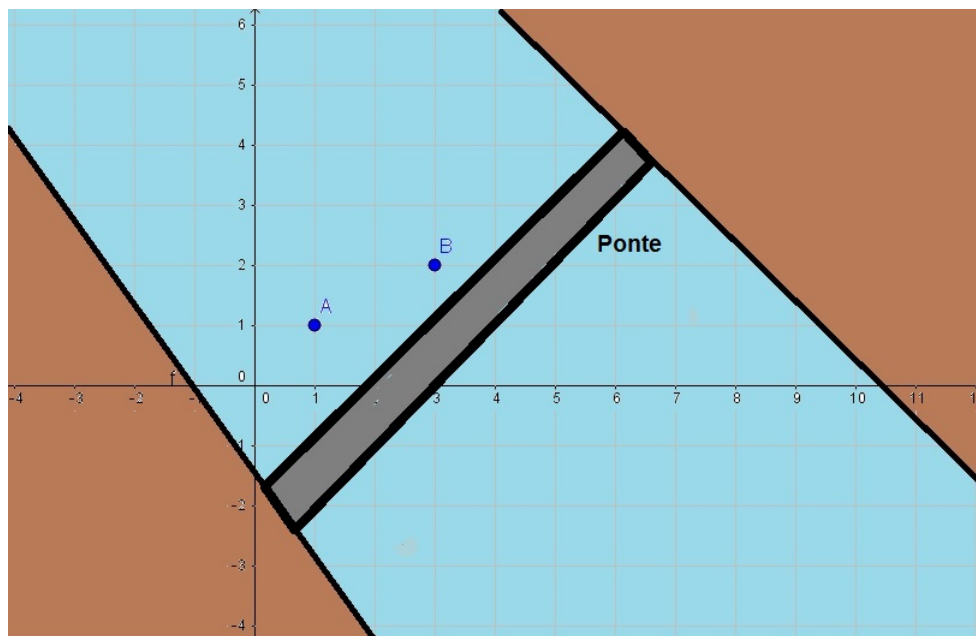


Figura 2.14: Ilustração do rio

⁶Apenas uma curiosidade: este problema é baseado em uma situação real vivenciada pelo autor do presente trabalho, em uma viagem à uma cidade do baixo sul do estado da Bahia. Evidenciando as características de significado que a atividade buscar promover ao estudante.

Solução utilizando o Geogebra 2.3.5.1. *A solução da questão usando o Geogebra será feita em 3 etapas.*

Primeira etapa

Inicialmente, os alunos irão reproduzir a situação proposta no software Geogebra. Esta etapa pode ser realizada através de comandos simples. Os mesmos são apresentados abaixo, numa sequência de passos.

- (1) Marcar o ponto $(1, 1)$;
- (2) Marcar o ponto $(3, 2)$;
- (3) Com o auxílio da ferramenta auxiliar “Renomear”, renomear o ponto $(1, 1)$ como *A* e o ponto $(3, 2)$ como *B*.

Após a realização dos passos citados acima, os alunos devem obter uma imagem semelhante à apresentada abaixo.

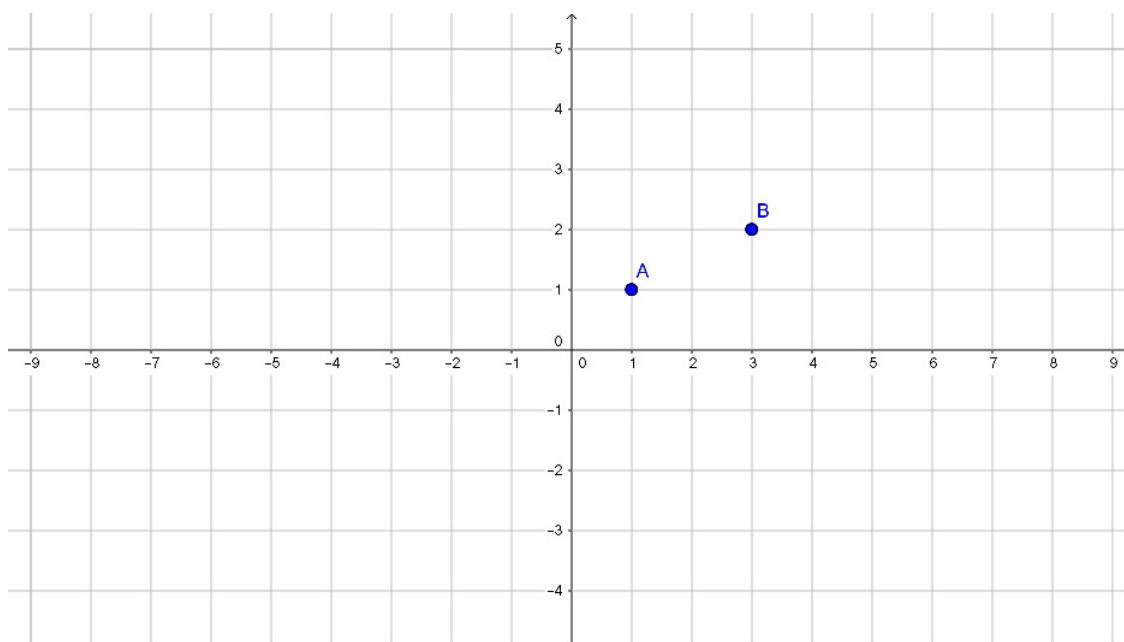


Figura 2.15: Ilustração da primeira etapa do problema

Segunda etapa

Nesta etapa o aluno irá rotacionar, em 90° , o ponto B em torno do ponto A . Para tanto, o mesmo deve seguir a sequência de passos abaixo.

- (1) Marcar o segmento \overline{AB} ;
- (2) Utilizar a opção “controle deslizante” para criar um ângulo α variando entre 0° e 360° (Esta ferramenta possibilitará o aluno visualizar a rotação do ponto B em torno do ponto A a partir de qualquer ângulo entre 0° e 360°);
- (3) Utilizar a opção “rotação em torno de um ponto” e rotacionar o ponto B em torno do ponto A , em α graus, no sentido anti-horário, obtendo o ponto B' . Este ponto é um dos quais são buscados no problema proposto. (Solicite aos alunos que variem o valor de β utilizando o controle deslizante e indague-os à respeito de qual ângulo o controle deslizante β deve ser fixado);
- (4) Fixar o controle deslizante β no valor de 90° ;
- (5) Marcar o segmento $\overline{AB'}$.

Após a realização dos passos citados acima, os alunos devem obter uma imagem semelhante à apresentada abaixo.

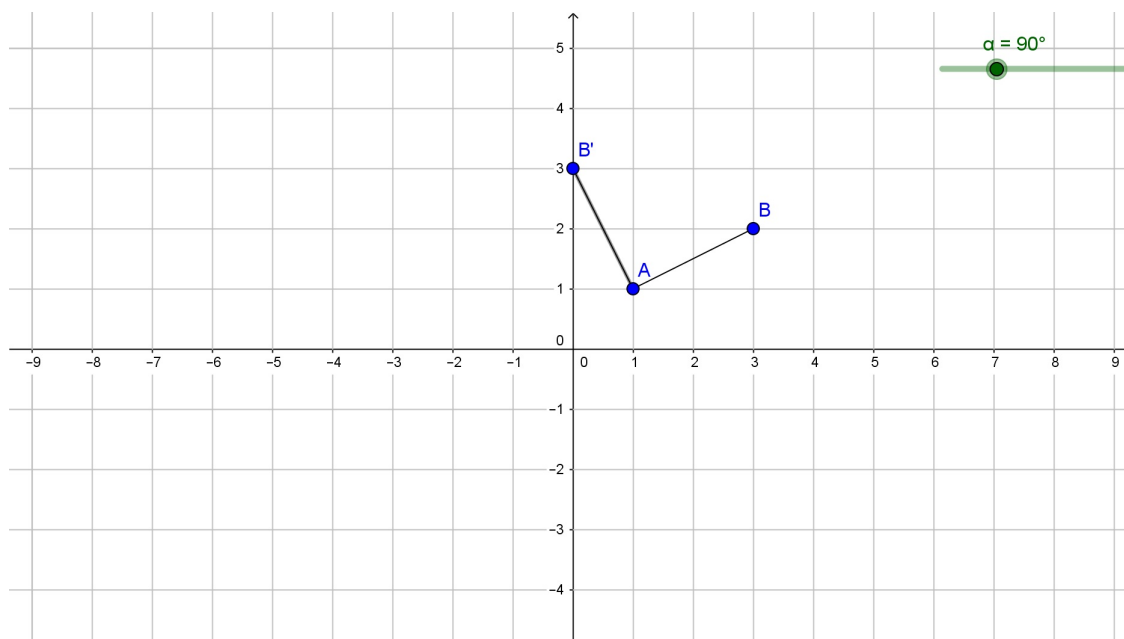


Figura 2.16: Ilustração da segunda etapa do problema

Terceira etapa

De maneira análoga à anterior, o aluno irá rotacionar, em 90° , o ponto A em torno do ponto do ponto B . Nesta etapa, ficará evidente a região associada à área de pesca, quando, ao fim da construção, o aluno marcar os lados restantes do quadrado. Para tanto, o mesmo deve seguir a sequência de passos abaixo.

- (1) Utilizar a opção “controle deslizante” para criar um ângulo β variando entre 0° e 360° (Esta ferramenta possibilitará o aluno visualizar a rotação do ponto A em torno do ponto B a partir de qualquer ângulo entre 0° e 360°);
- (3) Utilizar a opção “rotação em torno de um ponto” e rotacionar o ponto A em torno do ponto B , em β graus, no sentido horário, obtendo o ponto A' . Este ponto é um dos quais são buscados no problema proposto. (Solicite aos alunos que variem o valor de α utilizando o controle deslizante e indague-os à respeito de qual ângulo o controle deslizante α deve ser fixado);
- (4) Fixar o controle deslizante α no valor de 90° ;
- (5) Marcar o segmento $\overline{BA'}$;
- (6) Marcar o segmento $\overline{B'A'}$;
- (7) Utilizar a ferramenta “Polígono” para evidenciar o quadrado $ABA'B'$, o qual representa, justamente, a área de pesca.

Após a realização dos passos citados acima, os alunos devem obter uma imagem semelhante à apresentada abaixo.

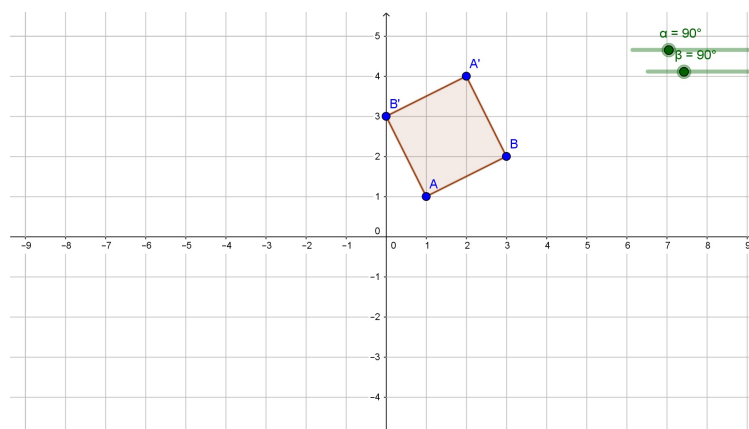


Figura 2.17: Ilustração da terceira etapa do problema

Sobrepondo a solução acima, na área correspondente, no esperança do sul, temos a figura acima.

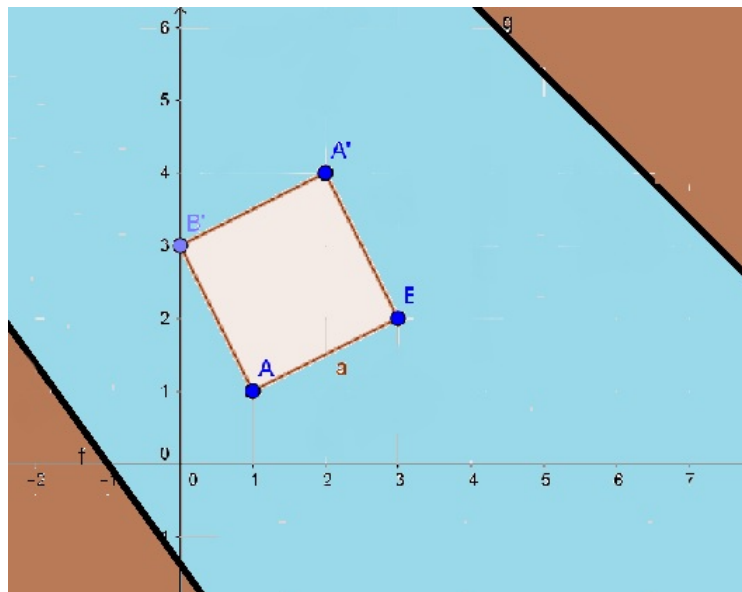


Figura 2.18: Figura conclusiva do problema

Para complementar a atividade, sugere-se que a atividade seja resolvida usando os conteúdos sobre números complexos apresentados anteriormente, como a seguir. Primeiramente rotaciona-se em 90° o ponto B em torno de A , obtendo um ponto D que será um dos vértices do quadrado. Para tanto, seguiremos os seguintes passos:

- Encontrar um ponto $C = B - A$;⁷
- Rotacionar C em 90° no sentido anti-horário obtendo C' , para tanto iremos multiplicar C por i ;
- O ponto $D = C' + A$ será um dos vértices do quadrado.

Analogamente, rotacionaremos em 90° o ponto A em torno de B obtendo um ponto F que será o último vértice do quadrado. Para tanto basta seguir os passos abaixo:

- Encontrar um ponto $E = A - B$;
- Rotacionar E em 90° no sentido horário obtendo E' , para tanto iremos multiplicar E por $-i$;
- O ponto $F = E' + B$ será o vértice que restava ao quadrado.

De fato, $C = B - A = (2, 1) \Rightarrow C' = C \cdot i \Rightarrow C' = (-1, 2) \Rightarrow C' + A = (-1, 2) + (1, 1) = (0, 3) = D$, e, $E = A - B = (-2, -1) \Rightarrow E' = E \cdot (-i) \Rightarrow E' = (-1, 2) \Rightarrow E' + B = (-1, 2) + (3, 2) = (2, 4) = F$.

⁷Como mencionado anteriormente, um ponto do plano está associado à um complexo. Desta maneira, faz sentido tal subtração.

2.4 Reflexões sobre a Sequência Didática

Uma sugestão para a realização da atividade envolvendo a situação problema seria apresentar, inicialmente, um vídeo (ou foto) ilustrativo de um rio.

Uma outra recomendação que consideramos importante é que, inicialmente, o professor descreva a situação problema usando o máximo possível de uma linguagem visual, em outras palavras, ao invés de dizer que uma área de pesca tem o formato quadrangular e que a marcação de seus vértices é feita através de pequenas varetas de madeira, como é feita no problema, ele construa um desenho (que pode ser no quadro de giz), conjuntamente com os estudantes e, a partir daí, concluam que a figura geométrica que (melhor) corresponde a esta descrição é a de um quadrado.

Para concluir, acrescentamos a importância de o professor oferecer a turma a oportunidade de discutir/refletir sobre a atividade, por exemplo, permitindo a discussão sobre a solução obtida da forma analítica com a solução obtida com o Geogebra. Também é relevante questionar sobre as principais dificuldades ao usar o Geogebra para encontrar a solução?

Aqui ressalte-se que, não há reducionismo da complexidade que envolve os processos de ensino e aprendizagem, o que se propôs foi, tão somente, estabelecer o vínculo com resultados oriundos de uma pesquisa com os conteúdos que serão tratados no presente trabalho. A divisão da sequência didática em atividades com diferentes objetivos visa possibilitar ao aluno o avanço em níveis. Tem-se ainda que,

A inclusão dos números complexos nos parâmetros curriculares para o ensino médio e suas relações com o conteúdo de outras disciplinas como a Física, a Engenharia, os Circuitos Elétricos, a Topografia, a Informática e a Cosmologia apontam para a importância destes conteúdos na formação matemática do aluno. ([1], 2006, p. 17-18).

Assim sendo, fica claro que tratar os números complexos, apenas, como ferramentas matemáticas abstratas, sem aplicações, é, sim, um reducionismo das potencialidades que podem ser apresentadas para este conteúdo. A aplicabilidade dos números complexos e das especificidades envolvidas neste viés matemático pode se dar em torno do mesmo. O processo de ensino-aprendizagem construído a partir das etapas propostas suaviza e sugere ao aluno a resolução da situação problema tomando como base as atividades anteriores e portanto o conhecimento de números complexos associado a utilização do Geogebra como ferramenta auxiliar do processo.

Apresentar os números complexos a partir de uma situação problema, desta forma, faz com que a atividade se torne desafiadora e atraente para o estudante, de modo que ele desenvolva habilidades procedimentais e atitudinais, favorecendo o seu aprendizado e buscando uma significação dos conceitos.

Acrescentamos, ainda, a possibilidade natural que o professor tem de explorar, neste ponto, as questões referentes à existência de outros conjuntos numéricos. Apenas propondo o seguinte questionamento aos estudantes.

Questão 2.4.1. *Vocês usaram os números complexos para resolver problemas de rotação no plano. Vocês acham que eles podem ser usados para resolver problemas no espaço tri-dimensional?*

A análise das respostas apresentadas pelos estudantes ao questionamento anterior, pode sugerir um trabalho, como, por exemplo, uma atividade transversal versando sobre o tema: rotações no espaço tri-dimensional, como fazer? Como veremos, esta discussão esta intimamente ligada com os quatérnios de Hamilton, tratada no capítulo 4. Também acrescentamos como uma proposta de atividade, que pode ser desenvolvida pelo professor, visando estimular os estudantes, leituras relacionadas sobre o tema: rotações no plano e no espaço. Na seção 4.3 apresentamos algumas aplicações do tema, que podem servir como referência de leitura. Após a leitura escolhida, sugerimos uma reflexão com a turma sobre a atividade desenvolvida.

Capítulo 3

Conjuntos numéricos: dos naturais aos complexos

Neste capítulo apresentaremos a construção dos números naturais, inteiros, racionais, reais e complexos. As principais referências utilizadas foram [10, 15].

Antes da construção formal dos conjuntos aos quais nos referimos antes, destacamos o seguinte fato (curioso, e talvez surpreendente) sobre os bebês. As pesquisas mostram que os bebês possuem certas habilidades matemáticas de contagem. De fato, as pesquisas nesta direção não afirmam que os participantes envolvidos (os bebês) tenham consciência do conceito formal de número, mas possuem uma certa compreensão do tamanho de pequenos conjuntos, denominada por alguns pesquisadores de numerosidade. Diante disso, não é absurdo afirmar que nascemos com uma certa capacidade matemática já previamente estabelecida, ou ainda que sabemos contar antes mesmo de aprender a falar.¹ Com o desenvolvimento de um idioma, os indivíduos podem dedicar-se com o aprendizado formal do conceito abstrato de número, o qual ocupa, certamente, um lugar de destaque na matemática. Naturalmente a evolução do tempo permite que este indivíduo aprenda conhecimentos matemáticos mais complexos (claro, respeitando as capacidades, habilidades e o tempo de cada indivíduo), como por exemplo, o conceito de classificação. Aqui em destaque: a classificação de números em coleções, denominadas de conjuntos numéricos.

Agora à construção (formal) dos conjuntos numéricos.

¹Pesquisadores constataram que bebês de dois dias de vida podem fazer operações matemáticas de adição e subtração (para detalhes veja, por exemplo, [7]). “grifo nosso”.

3.1 Os números naturais

A construção do conjunto dos números naturais apresentada aqui é atribuída a Giuseppe Peano (1858–1932). Nesta construção, Peano exibe uma lista com três axiomas, denominados posteriormente de Axiomas de Peano, a partir dos quais, o conjunto dos números naturais será visto simplesmente como qualquer conjunto de símbolos que atenda a tais axiomas.

Axiomas de Peano: *Existe um conjunto \mathbb{N} (o qual será chamado de conjunto dos números naturais) e uma função $s : \mathbb{N} \rightarrow \mathbb{N}$ (a qual será chamada de função sucessor), tal que:*

- (A₁) A função s é injetora;
- (A₂) Existe um elemento no conjunto \mathbb{N} , o qual será denotado por 0 (lê-se “zero”), que não está na imagem de s . Simbolicamente, $0 \notin \text{Im}(s)$;
- (A₃) Se $X \subset \mathbb{N}$ é um subconjunto tal que $0 \in X$ e, para todo, $n \in X$, tivermos também $s(n) \in X$, então $X = \mathbb{N}$. Este axioma é referido como o Princípio ou Axioma da Indução.

O próximo teorema nos permitirá compreender a igualdade $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Teorema 3.1.1. *Seja $s : \mathbb{N} \rightarrow \mathbb{N}$ a função sucessor, então:*

- (i) $s(n) \neq n$, para todo $n \in \mathbb{N}$.
- (ii) $\text{Im}(s) = \mathbb{N} \setminus \{0\}$.

Demonstração. De fato,

- (i) Seja $X := \{n \in \mathbb{N} : s(n) \neq n\} \subset \mathbb{N}$. Pelo axioma A_2 , temos que $0 \in X$ pois $0 \neq s(0)$. Pelo axioma A_3 , resta-nos mostrar que para todo $n \in X$, temos $s(n) \in X$. De fato, dado um elemento n de X , temos que $s(n) \neq n$, daí, aplicando a função s em ambos os membros desta desigualdade, e usando o axioma A_1 , obtemos que $s(s(n)) \neq s(n)$ e, portanto, segue que $s(n) \in X$, como queríamos mostrar.
- (ii) Seja $X \subset \mathbb{N}$, tal que $X := \{0\} \cup \text{Im}(s)$, queremos mostrar que $X = \mathbb{N}$. De fato, $0 \in X$ e, além disso, para todo $n \in X$, tem-se que $s(n) \in \text{Im}(s) \subset X$. Dessa forma, pelo axioma da indução, $X = \mathbb{N}$ e, portanto, $\text{Im}(s) = \mathbb{N} \setminus \{0\}$, como queríamos mostrar. \square

Observação 3.1.2. *O item (i) do teorema anterior estabelece que nenhum elemento de \mathbb{N} é sucessor de si mesmo, enquanto que o item (ii) diz que 0 é o único elemento de \mathbb{N} que não é sucessor de nenhum outro elemento de \mathbb{N} .*

Como uma consequência imediata do teorema anterior, temos que:

$$\mathbb{N} = \{0, s(0), s(s(0)), s(s(s(0))), \dots\}.$$

A partir daí, podemos dar significado aos símbolos um, dois, três, quatro e, assim sucessivamente, tal qual conhecemos, hoje, da seguinte forma: $s(0) = 1$ (lê-se “um”); $s(1) = 2$ (lê-se “dois”); $s(2) = 3$ (lê-se “três”); $s(3) = 4$ (lê-se “quatro”); $s(4) = 5$ (lê-se “cinco”) e assim por diante. Dessa forma, $\mathbb{N} = \{0, s(0), s(s(0)), s(s(s(0))), \dots\} = \{0, 1, 2, 3, \dots\}$.

Neste texto, dado um conjunto numérico \mathbb{A} , denotaremos \mathbb{A}^* como sendo $\mathbb{A} \setminus \{0\}$.

3.1.1 Operações com naturais

Definição 3.1.3 (adição de naturais). *Definimos a adição de dois números naturais, m e n , de maneira recursiva, do seguinte modo:*

$$\begin{aligned} (+) : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \\ (m, n) &\mapsto m + n := \begin{cases} m + 0 = m \\ m + s(n) = s(m + n) \end{cases} \end{aligned}$$

Equivalentemente,

$$\begin{aligned} (+) : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \\ (m, n) &\mapsto m + n := \begin{cases} m + 0 = m \\ m + s(0) = s(m + 0) = s(m) \\ m + s(s(0)) = s(m + s(0)) = s(s(m)), \end{cases} \end{aligned}$$

e assim por diante.

Observação 3.1.4 (apenas esclarecendo um pouco da natureza recursiva da definição anterior). *Observe que existem duas possibilidades para adição de dois números naturais m e p . A primeira possibilidade é $p = 0$, neste caso, pela definição da adição no conjunto \mathbb{N} , temos que $m + p = m$. A outra possibilidade é $p \neq 0$, neste caso, temos que p é sucessor de algum natural, digamos n , ou seja, $p = s(n)$. Dessa forma, pela definição da adição no conjunto \mathbb{N} , segue que $m + p = m + s(n) = s(m + n)$.*

Proposição 3.1.5. *A adição de números naturais está bem definida.*

Demonstração. Consideremos o conjunto $S_m = \{m \in \mathbb{N}; m + n \text{ está definida}\}$ para cada $m \in \mathbb{N}$ fixado arbitrariamente. Note que $0 \in S_m$, pois $m + 0 = m$, por definição da operação de adição dos naturais. Além disso, para todo $n \in S_m$, pela construção do conjunto S_m , temos que $m + n$ está bem definida. Sendo assim, $s(n) \in S_m$, pois $m + s(n) = s(m + n)$ está bem definido. Logo, pelo Princípio da indução, $S_m = \mathbb{N}$. \square

Proposição 3.1.6. *Para todo natural m , tem-se $s(m) = m+1$ e $s(m) = 1+m$. Portanto, $m+1 = 1+m$.*

Demonstração. De fato, $m+1 = m+s(0) = s(m+0) = s(m)$. Por outro lado, para mostrar que $s(m) = 1+m$, será utilizado um conjunto $A = \{m \in \mathbb{N}; s(m) = 1+m\}$. Será utilizada a indução para mostrar que $A = \mathbb{N}$. Tem-se que $0 \in A$ pois $s(0) = 1 = 1+0$. Sendo $m \in A$, tem-se que $s(s(m)) = s(1+m) = 1+s(m)$. Dessa forma, se $m \in A$ então $s(m) \in A$ e pelo princípio da indução conclui-se que $A = \mathbb{N}$. \square

Definição 3.1.7 (multiplicação de naturais). *Definimos a multiplicação de dois números naturais, m e n , designada por $m \cdot n$, da seguinte forma:*

$$\begin{aligned} (\cdot) : \mathbb{N} \times \mathbb{N} &\rightarrow \mathbb{N} \\ (m, n) &\mapsto m \cdot n := \begin{cases} m \cdot 0 = 0 \\ m \cdot (n+1) = m \cdot n + m \end{cases} \end{aligned}$$

Usualmente, será utilizada a notação de justaposição para a multiplicação. A utilização da notação “ \cdot ” será feita apenas quando for conveniente ou necessário.

Proposição 3.1.8. *Para todo $m \in \mathbb{N}$, tem-se que $0m = 0$.*

Demonstração. De fato, sendo m um natural fixado arbitrariamente e $A = \{m \in \mathbb{N}; 0m = 0\}$ tem-se que $0 \in A$, pois por definição $0 \cdot 0 = 0$. Além disso, supondo que $k \in A$ tem-se que $0 \cdot k = 0$ então $0 \cdot s(k) = 0 \cdot (k+1) = 0 \cdot k + 0 = 0 \cdot k = 0$ (na última igualdade foi usada a hipótese de indução). Sendo assim, $0 \cdot s(k) = 0$ e tem-se que se $k \in A$ então $s(k) \in A$. Assim, $A = \mathbb{N}$ e, como m foi fixado arbitrariamente, a propriedade é válida para qualquer natural m . \square

Proposição 3.1.9. *Sejam m e n naturais quaisquer. Se $m+n=0$, então $m=n=0$.*

Demonstração. Supondo por absurdo que $n \neq 0$, então $n = s(n_1) = n_1 + 1$, assim $m+n = m+(n_1+1) = (m+n_1)+1 = s(m+n_1)$. Contradição, pois 0 não é sucessor de nenhum natural. \square

Para a construção dos conjuntos \mathbb{Z} e \mathbb{Q} será necessário a introdução do conceito de relação de equivalência, o qual trataremos a seguir.

3.2 Relação de equivalência

Classificar os objetos de uma certa coleção é um importante problema na matemática moderna. Em geral, tal classificação visa estabelecer condições sobre as quais dois objetos desta coleção são essencialmente os mesmos. Uma ferramenta bastante útil e

amplamente utilizada pelos matemáticos para classificar elementos de um dado conjunto fixado é a relação de equivalência.

Definição 3.2.1 (relação de equivalência). *Uma relação binária R é dita ser uma relação de equivalência em um conjunto A , se R for:*

- (i) reflexiva, isto é: aRa , para todo $a \in A$;
- (ii) simétrica: isto é: se $a, b \in A$ e aRb , então bRa ;
- (iii) transitiva: isto é: para $a, b, c \in A$, se aRb e bRc , então aRc .

Dada uma relação de equivalência R em um conjunto A , tal que aRb , $a, b \in A$, diz-se que a é R -equivalente a b ou, simplesmente, a é equivalente a b , quando não houver perigo de confusão, com respeito a relação de equivalência R .

Definição 3.2.2. *Sejam R uma relação de equivalência num conjunto A e $a \in A$ um elemento fixado arbitrariamente. O conjunto $\bar{a} = \{x \in A; xRa\}$ chama-se classe de equivalência de a pela relação R . Ou seja, \bar{a} é o conjunto constituído por todos os elementos de A que são equivalentes a a . O conjunto quociente de A por R , denotado por $\frac{A}{R}$, será usado para significar o conjunto constituído de todas as classes de equivalência em A pela relação R , ou seja, $\frac{A}{R} := \{\bar{a}; a \in A\}$.*

Teorema 3.2.3. *Sejam R uma relação de equivalência em um conjunto A e a e b elementos quaisquer de A , então:*

- (i) $a \in \bar{a}$;
- (ii) $\bar{a} = \bar{b} \Leftrightarrow aRb$;
- (iii) $\bar{a} \neq \bar{b} \Rightarrow \bar{a} \cap \bar{b} = \emptyset$.

Demonstração. Sejam R uma relação de equivalência em um conjunto A e a e b elementos quaisquer de A .

- (i) Temos, por definição, que $\bar{a} = \{x \in A; xRa\}$. Queremos mostrar que $a \in \bar{a}$, ou seja, que aRa , mas, R é uma relação de equivalência, daí, qualquer que seja $a \in A$ vale a propriedade reflexiva e, portanto, $a \in \bar{a}$.
- (ii) Sejam $\bar{a} = \{x \in A; xRa\}$ e $\bar{b} = \{x \in A; xRb\}$.

(\Rightarrow) Pelo item (i), temos que $a \in \bar{a}$, mas, por hipótese da ida, $\bar{a} = \bar{b}$, daí, tem-se que $a \in \bar{b}$, logo aRb .

- (\Leftarrow) Supondo aRb , para mostrar que $\bar{a} = \bar{b}$ é necessário mostrar que $\bar{a} \subset \bar{b}$ e que $\bar{a} \supset \bar{b}$. De fato, seja $a \in \bar{a}$. Por hipótese aRb , então $a \in \bar{b}$, ou seja $\bar{a} \subset \bar{b}$. Por outro lado, seja $b \in \bar{b}$. Por hipótese aRb e, além disso, R é uma relação de equivalência, portanto é simétrica. Daí bRa , conseqüentemente $b \in \bar{a}$;
- (iii) Vamos provar por redução ao absurdo, ou seja, que sendo $\bar{a} \neq \bar{b}$, ocorra que $\bar{a} \cap \bar{b} \neq \emptyset$. Mas, se existe $c \in \bar{a} \cap \bar{b}$, então $c \in \bar{a}$ e $c \in \bar{b}$, mas isto acarreta que cRa e cRb . Do fato que R é uma relação de equivalência, e, portanto, transitiva e simétrica, temos que aRb . Daí, do item (ii), segue $\bar{a} = \bar{b}$, o que contraria a hipótese, do absurdo. \square

A propriedade (ii) do teorema anterior garante que qualquer elemento de uma referida classe de equivalência pode ser o representante da mesma, já o item (iii) evidencia que duas classes de equivalência distintas são disjuntas e, portanto, uma relação de equivalência determina uma partição num determinado conjunto e vice-versa. Além disso, as classes de equivalência determinadas por uma relação são justamente os subconjuntos disjuntos da referida partição.

Exemplo 3.2.4. *Seja A um conjunto e $A = A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n$ uma partição finita de A , isto é, decomposição de A como união finita de uma família de subconjuntos de A que são dois a dois disjuntos e não vazios. Para x e $y \in A$, definimos a seguinte relação R : xRy quando x e y pertencem ao mesmo elemento da partição. Em símbolos: $xRy \Leftrightarrow$ existe $i \in \{1, \dots, n\}$ tal que $x, y \in A_i$.*

A relação R é uma relação de equivalência em A . De fato, a relação citada acima é de equivalência, pois é

- (i) *reflexiva: se $x \in A$, claramente $x \in A_i$ e assim, xRx ;*
- (ii) *Simétrica: se $x, y \in A$ e xRy , então $x, y \in A_i$, portanto, yRx ;*
- (iii) *transitiva: sejam $x, y, z \in A$, xRy e yRz . Dessa forma, $x, y \in A_i$ e $y, z \in A_j$ com $i, j \in \{1, \dots, n\}$. Como y está em A_i e em A_j , e sabemos que os conjuntos são disjuntos dois a dois, concluímos que $i = j$ e portanto, x e z estão no mesmo conjunto $A_{i=j}$, logo, xRz .*

O próximo exemplo tem um interesse especial no presente trabalho, pois será usado na definição do conjunto dos números inteiros. Por este motivo, denotaremos a relação de equivalência pelo símbolo \sim .

Exemplo 3.2.5. *A relação \sim em $\frac{\mathbb{N} \times \mathbb{N}}{\sim}$ definida por $(a, b) \sim (c, d)$ quando $a + d = b + c$ é uma relação de equivalência. De fato, sejam $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$, nota-se que \sim é:*

(i) reflexiva: $(a, b) \sim (a, b)$, pois $a + b = b + a$ já que a adição de naturais é comutativa;

(ii) transitiva: $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$, pois, por hipótese, $a + d = b + c$ e $c + f = d + e$. Daí, Somando as equações membro a membro:

$$\begin{aligned} (a + d) + (c + f) &= (b + c) + (d + e) \Rightarrow \\ (d + a) + (f + c) &= (c + b) + (e + d) \Rightarrow \\ d + (a + f) + c &= c + (b + e) + d \Rightarrow \\ (a + f) &= (b + e) \Rightarrow \\ (a, b) &\sim (e, f). \end{aligned}$$

(iii) Simétrica: $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$, pois $a + d = b + c \Rightarrow c + b = d + a$, já que a adição é comutativa em \mathbb{N} .

Abaixo alguns exemplos de classes de equivalência da relação \sim definida acima.

Exemplo 3.2.6.

- $\overline{(0, 3)} = \{(1, 4), (2, 5), (3, 6), \dots\}$;
- $\overline{(0, 2)} = \{(1, 3), (2, 4), (3, 5), \dots\}$;
- $\overline{(0, 1)} = \{(1, 2), (2, 3), (3, 4), \dots\}$;
- $\overline{(0, 0)} = \{(1, 1), (2, 2), (3, 3), \dots\}$;
- $\overline{(1, 0)} = \{(2, 1), (3, 2), (4, 3), \dots\}$;
- $\overline{(2, 0)} = \{(3, 1), (4, 2), (5, 3), \dots\}$;
- $\overline{(3, 0)} = \{(4, 1), (5, 2), (6, 3), \dots\}$, e assim por diante.

Observação 3.2.7. Note que a notação $\overline{(a, b)}$ expressa essencialmente $a - b$. De fato,

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c \Leftrightarrow a - b = c - d. \quad (3.1)$$

Para a primeira equivalência usa-se a definição da relação \sim , já para segunda, usa-se a noção de elemento simétrico (definição 5.2.17).

3.3 Os números inteiros

Diferentemente da apresentação usual realizada no ciclo escolar básico, nesta seção, o conjunto dos números inteiros será definido como um conjunto de classes de equivalência, o que nos permitirá evidenciar que este não se caracteriza como um mero “espelho” do conjunto dos números naturais (detalhes na seção 3.8).

Definição 3.3.1. *Seja a relação \sim definida no exemplo 3.2.5. Definimos o conjunto dos números inteiros, o qual denotaremos por \mathbb{Z} , como sendo:*

$$\mathbb{Z} := \frac{\mathbb{N} \times \mathbb{N}}{\sim} = \{\overline{(a, b)}; (a, b) \in \mathbb{N} \times \mathbb{N}\}.$$

A partir da observação (3.2.7) podemos associar as classes de equivalência do exemplo 3.2.6, com a apresentação usual do conjunto dos números inteiros. De fato, $\overline{(0, 3)} = -3$; $\overline{(0, 2)} = -2$; $\overline{(0, 1)} = -1$ e assim por diante. Com isto, podemos escrever

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

3.4 Os números racionais

Definição 3.4.1. *Considere o conjunto $\mathbb{Z} \times \mathbb{Z}$ e a relação de equivalência R definida por $(a, b)R(c, d) \Leftrightarrow ad = bc$. Definimos o conjunto dos números racionais, \mathbb{Q} , como sendo:*

$$\mathbb{Q} := \left\{ \overline{(x, y)} \in \frac{\mathbb{Z} \times \mathbb{Z}^*}{R}; (x, y)R(a, b) \right\}. \quad (3.2)$$

Se $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$, então $\frac{a}{b} = \frac{c}{d}$ se, e somente se $ad = bc$. Em particular, dado

$(a, b) \in \frac{\mathbb{Z} \times \mathbb{Z}^*}{R}$, denotaremos por $\frac{a}{b}$ (lê-se a sobre b) a classe de equivalência $\overline{(a, b)}$ pela relação R . Ou seja,

$$(a, b) = \frac{a}{b} = \left\{ (x, y) \in \frac{\mathbb{Z} \times \mathbb{Z}^*}{R}; (x, y)R(a, b) \right\}. \quad (3.3)$$

3.5 Os números reais

Existem algumas maneiras de notar que o conjunto \mathbb{Q} dos números racionais não atende a uma ideia de “completeza”, no sentido de que existem determinadas medidas que não podem ser expressas como racionais. Tal situação pode ser observada, por exemplo, ao tentarmos obter a medida da diagonal de um quadrado de lado 1, a qual pode ser obtida, mediante aplicação direta do teorema de Pitágoras, como sendo $\sqrt{2}$, o qual não é um número racional. De fato, suponha que exista $\frac{a}{b}$, com a e b primos entre si, tal que

$\left(\frac{a}{b}\right)^2 = 2$. Neste caso, $a^2 = 2b^2$, portanto a^2 é par pois é o dobro de b^2 . Para que a^2 seja par é necessário que a seja par, ou seja, $a = 2s$, $s \in \mathbb{Z}$. Dessa forma, $(2s)^2 = 2b^2$ e de maneira análoga conclui-se que b^2 é par e portanto b é par. Porém, sendo a e b pares há uma contradição com a hipótese de que a e b são primos entre si.

A ideia intrínseca da construção dos números reais é justamente completar o conjunto dos números racionais criando um sistema contínuo de números. Usualmente o estudo/construção dos números é feito via cortes de Dedekind ou seqüências de Cauchy. Embora ambas as construções guardem uma riqueza de detalhes matemáticos que mereçam ser explorados, neste trabalho será feita a construção dos reais via Cortes de Dedekind. A noção de corte foi introduzida por R. Dedekind, mas as ideias gerais remontam à Eudoxio (408-353 a.C.).

Definição 3.5.1. *Um conjunto α de números racionais diz-se um corte se satisfizer as seguintes condições:*

- (i) $\emptyset \neq \alpha \neq \mathbb{Q}$;
- (ii) Se $r \in \alpha$, $s \in \mathbb{Q}$ e $s < r$ então $s \in \alpha$;
- (iii) Em α não existe elemento máximo.

Exemplos 3.5.2. *Seguem abaixo alguns exemplos de conjuntos e as respectivas avaliações se os mesmos são cortes ou não.*

$$(a) \alpha_1 = \left\{ x \in \mathbb{Q}; x < \frac{2}{3} \right\};$$

De fato, α_1 é um corte, pois:

- (i) É notável que $\alpha_1 \neq \emptyset$ pois $0 \in \alpha_1$. Além disso, $\alpha_1 \neq \mathbb{Q}$ pois $1 \notin \alpha_1$;
- (ii) Se $r \in \alpha_1$, $s \in \mathbb{Q}$ e $s < r$ tem-se que $r < \frac{2}{3}$, sendo assim, $s < \frac{2}{3}$ e assim, $s \in \alpha_1$;
- (iii) Suponha que α_1 possua elemento máximo m . Dessa forma, $m > r$, qualquer que seja $r \in \alpha_1$. Porém, é possível provar que: $x < y \Rightarrow x < \frac{x+y}{2} < y$ (ver [?]). Consequentemente, $m < \frac{(m + \frac{2}{3})}{2} < \frac{2}{3}$. Isto contradiz a maximalidade de m . Logo, α_1 não possui elemento máximo.

$$(b) \alpha_2 = \left\{ x \in \mathbb{Q}; x > \frac{3}{5} \right\};$$

Note que α_2 não é um corte, pois não atende ao item (ii) da definição de corte. De fato,

- (ii) Note que $\frac{4}{5} \in \alpha_2$, $\frac{2}{5} \in \mathbb{Q}$ e $\frac{2}{5} < \frac{4}{5}$ porém $\frac{2}{5} \notin \alpha_2$.

$$(c) \alpha_3 = \left\{x \in \mathbb{Q}; x \leq \frac{3}{5}\right\};$$

Note que α_3 não é um corte, pois não atende ao item (iii) da definição de corte. De fato,

$$(iii) \alpha_3 \text{ possui elemento máximo } \frac{3}{5};$$

$$(d) \alpha_4 = \left\{x \in \mathbb{Q}; -3 < x < \frac{8}{5}\right\};$$

Note que α_4 não é um corte, pois não atende ao item (ii) da definição de corte. De fato,

$$(ii) \text{ Note que } -2 \in \alpha_4, -3 \in \mathbb{Q} \text{ e } -3 < -2 \text{ porém } -3 \notin \alpha_4.$$

$$(e) \alpha_5 = \mathbb{Q}^*;$$

Note que α_5 não é um corte, pois não atende ao item (ii) da definição de corte. De fato,

$$(ii) \text{ Note que } 1 \in \alpha_5, 0 \in \mathbb{Q} \text{ e } 0 < 1 \text{ porém } 0 \notin \alpha_5.$$

$$(f) \alpha_6 = \left\{1, 4, \frac{3}{5}\right\};$$

Note que α_6 não é um corte, pois não atende aos itens (ii) e (iii) da definição de corte. De fato,

$$(ii) \text{ Note que } 4 \in \alpha_6, 3 \in \mathbb{Q} \text{ e } 3 < 4 \text{ porém } 3 \notin \alpha_6;$$

$$(iii) \alpha_6 \text{ possui elemento máximo } 4.$$

Observação 3.5.3. O corte $\alpha = \{x \in \mathbb{Q}; x < r, \text{ com } r \in \mathbb{Q}\}$ é denominado corte racional, representado por r^* e o corte $\alpha = \{x \in \mathbb{Q}_+; x^2 < 2\} \cup \mathbb{Q}_+^*$ é denominado corte irracional.

Definição 3.5.4. O conjunto formado por todos os cortes, racionais ou irracionais, é chamado de conjunto dos números reais e seus elementos de números reais e denotado por \mathbb{R} .

Note que, de acordo com as definições acima, um número real é um corte. Além disso, um número racional é um corte racional e um número irracional é um corte irracional.

3.6 Os números complexos

Definição 3.6.1. Sejam $(a, b), (c, d) \in \mathbb{R}^2$. Definimos o conjunto dos números complexos, e denotamos por \mathbb{C} , como sendo o conjunto \mathbb{R}^2 munido das operações de adição e multiplicação, definidas da seguinte forma:

$$\begin{aligned} (+) : \mathbb{R}^2 \times \mathbb{R}^2 &\rightarrow \mathbb{R}^2 \\ ((a, b); (c, d)) &\mapsto (a, b) + (c, d) := (a + c, b + d) \end{aligned}$$

$$\begin{aligned} (\cdot) : \mathbb{R}^2 \times \mathbb{R}^2 &\rightarrow \mathbb{R}^2 \\ ((a, b); (c, d)) &\mapsto (a, b) \cdot (c, d) := (ac - bd, ad + bc) \end{aligned}$$

Um elemento $z \in \mathbb{C}$ será denotado por $z = a + bi$.

Cabe ressaltar que a notação $a + bi$ não representa verdadeiramente uma soma, já que a e bi não podem ser adicionados.

No século *XIX* o matemático irlandês, William Rowan Hamilton mostrou que os números complexos e o conjunto \mathbb{R}^2 são isomorfos. Tal fato, justifica a identificação usual de um número complexo $z = a + bi$ com o par ordenado $(a, b) \in \mathbb{R}^2$. De fato, a definição aqui apresentada (3.6.1) é baseada neste resultado provado por Hamilton. Mais ainda, esta identificação no permite observar, de forma natural, um elemento $z \in \mathbb{C}$, como um elemento do conjunto $\mathbb{R} + \mathbb{R}i$.

No que segue nos proporemos a mostrar as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Para tanto, precisaremos do conceito de relação de ordem, o qual apresentamos a seguir.

3.7 Relação de ordem

Nesta seção, trataremos de um outro importante conceito em matemática, a saber: relação de ordem, o qual será necessário para formalizar as inclusões de conjuntos com certas propriedades algébricas importantes no contexto de estudo deste trabalho.

Intuitivamente, uma relação de ordem é uma relação binária que pretende captar o sentido de maior e menor, em um dado conjunto. Precisamente,

Definição 3.7.1 (relação de ordem). *Uma relação binária R em conjunto não vazio A diz-se uma relação de ordem em A quando satisfizer as condições seguintes, para quaisquer $x, y, z \in A$:*

- (i) reflexiva: xRx ;
- (ii) antissimétrica: Se xRy e yRx , então $x = y$;
- (iii) transitiva: Se xRy e yRz , então xRz .

Se um conjunto não vazio A for munido de uma relação de ordem, diz-se que o conjunto A é ordenado.

Exemplo 3.7.2. *Seja A um conjunto qualquer e $P(A)$ o conjunto das partes de A . A relação de “inclusão” sobre $P(A)$ é uma relação de ordem. De fato, sejam $X, Y, Z \in P(A)$, tem-se que \subset é:*

- (i) reflexiva, pois todo conjunto está contido nele mesmo;
- (ii) transitiva, pois $X \subset Y$ e $Y \subset Z$ implica que $X \subset Z$;
- (iii) antissimétrica, pois $X \subset Y$ e $Y \subset X$ implica que $X = Y$.

3.7.1 Relação de ordem em \mathbb{N}

Definição 3.7.3. *Sejam $m, n \in \mathbb{N}$, diremos que m é menor do que ou igual a n e indicamos por $m \leq n$, se existir $p \in \mathbb{N}$ tal que $n = m + p$. No caso em que, $m \leq n$, mas $m \neq n$, diremos que m é menor que n e indicamos por $m < n$.*

Observação 3.7.4. *Dizer que m é menor do que ou igual a n é equivalente a dizer que n é maior do que ou igual a m . Analogamente, se $n < m$ diz-se que m é maior do que n .*

Proposição 3.7.5. *A relação \leq citada na definição acima é uma relação de ordem em \mathbb{N} .*

Demonstração. Para que a relação \leq seja uma relação de ordem é necessário que a mesma seja: reflexiva, antissimétrica e transitiva. De fato,

- (i) \leq é reflexiva: Seja m um natural qualquer, tem-se que $m = m + 0$. Sendo assim, $m \leq m$.
- (ii) \leq é antissimétrica: Sejam m e n números naturais quaisquer. Se $m \leq n$ e $n \leq m$ então existem p_1 e p_2 , também naturais, tais que $n = m + p_1$ e $m = n + p_2$. Sendo assim, $m = m + p_1 + p_2 \Rightarrow p_1 + p_2 = 0$. Já foi mostrado que, neste caso, $p_1 = p_2 = 0$ e conseqüentemente $m = n$.
- (iii) \leq é transitiva: Sejam m, n, l naturais quaisquer. Se $m \leq n$ e $n \leq l$ então existem p_1 e p_2 , também naturais, tais que $n = m + p_1$ e $l = n + p_2$. Sendo assim, $l = m + p_1 + p_2 \Rightarrow l = m + p$ para $p = p_1 + p_2 \in \mathbb{N}$. Dessa forma $m \leq l$.

Dessa forma, \leq é uma relação de ordem em \mathbb{N} , como queríamos mostrar. \square

Proposição 3.7.6 (tricotomia dos naturais). *Para quaisquer $m, n \in \mathbb{N}$, uma, e apenas uma, das seguintes situações pode ocorrer: ou (i) $m < n$; ou (ii) $m = n$; ou (iii) $m > n$.*

Demonstração. Para demonstrar a proposição acima, será evidenciado que duas delas não podem ocorrer de forma simultânea e que obrigatoriamente uma delas deve ocorrer.

De fato, supondo que (i) e (ii) ocorrem ao mesmo tempo, $n = m + p$ ($p \in \mathbb{N}^*$) e $m = n$. Daí, $m = m + p$ ($p \in \mathbb{N}^*$), e conseqüentemente $p = 0$, o que é contradição. De forma análoga, (ii) e (iii) não podem ocorrer simultaneamente. Caso (i) e (iii) ocorressem

ao mesmo tempo, $n = m + p_1$ ($p_1 \in \mathbb{N}^*$) e $m = n + p_2$ ($p_2 \in \mathbb{N}^*$) então $m = (m + p_1) + p_2 = m + (p_1 + p_2)$. Assim, $p_1 + p_2 = 0 \Rightarrow p_1 = p_2 = 0$ o que é contradição, pois $p_1, p_2 \in \mathbb{N}^*$.

Seja $M = \{n \in \mathbb{N}; m < n \text{ ou } m = n \text{ ou } m > n\}$, então $0 \in M$ pois $0 = m$ ou $m \neq 0$. Caso $m \neq 0$, então, como mostrado anteriormente, $m > 0$. Se $k \in M$ então $m < k$ ou $m = k$ ou $m > k$. Analisando os três casos separadamente:

- (1) Se $m < k$ então $k = m + p$ ($p \in \mathbb{N}^*$). Sendo assim, $s(k) = k + 1 = (m + p) + 1 = m + (p + 1) \Rightarrow k + 1 = m + p_1$ ($p_1 = s(p)$), conseqüentemente, $k + 1 > m$ e dessa forma, $s(k) \in M$;
- (2) Se $m = k$ então $m + 1 = k + 1$. Sendo assim, $k + 1 > m$ e dessa forma, $s(k) \in M$;
- (3) Se $k < m$ então $m = k + p$ ($p \in \mathbb{N}^*$). Sendo assim, $p = p' + 1 \Rightarrow m = k + (p' + 1) = k + (1 + p') = (k + 1) + p'$. Se $p' = 0$ então $m = k + 1$ e conseqüentemente, $s(k) \in M$. Se $p' \neq 0$, então $m < k + 1$ e dessa maneira, $s(k) \in M$.

Dessa forma, pelo princípio da indução, $M = \mathbb{N}$. Assim, a Lei da tricotomia é válida para todos os naturais. \square

Assim como nos naturais, será estabelecida uma relação de ordem nos inteiros. Para tanto serão utilizadas as mesmas noções e motivações usadas nas definições de adição e multiplicação.

3.7.2 Relação de ordem em \mathbb{Z}

Definição 3.7.7. Dados os inteiros $\overline{(a, b)}$ e $\overline{(c, d)}$, escrevemos $\overline{(a, b)} \leq \overline{(c, d)}$ (lê-se $\overline{(a, b)}$ é menor do que ou igual a $\overline{(c, d)}$), quando $a + d \leq b + c$.

Teorema 3.7.8. A relação \leq definida anteriormente é uma relação de ordem em \mathbb{Z} , ou seja, para $\alpha = \overline{(a, b)}, \beta = \overline{(c, d)}, \gamma = \overline{(e, f)} \in \mathbb{Z}$, tem-se que \leq é:

- (i) reflexiva: $\alpha \leq \alpha$;
- (ii) antissimétrica: $\alpha \leq \beta$ e $\beta \leq \alpha \Rightarrow \alpha = \beta$;
- (iii) transitiva: $\alpha \leq \beta$ e $\beta \leq \gamma \Rightarrow \alpha \leq \gamma$.

Demonstração.

- (i) De fato, $a + b = b + a \Rightarrow \overline{(a, b)} = \overline{(a, b)} \Rightarrow \alpha = \alpha \Rightarrow \alpha \leq \alpha$;
- (ii) Por hipótese, $\overline{(a, b)} \leq \overline{(c, d)}$ e $\overline{(c, d)} \leq \overline{(e, f)}$. Sendo assim, $a + d \leq b + c$ e $c + f \leq d + e$. Dessa forma, pela tricotomia dos naturais, tem-se que $a + d = b + c$, ou seja, $\alpha = \beta$;

(iii) Tem-se, como consequência da hipótese, que $a + d \leq b + c$ e $c + f \leq d + e$. Sendo assim, existem p e q naturais tais que $a + d + p = b + c$ e $c + f + q = d + e$. Daí,

$$\begin{aligned} a + d + p + e &= b + c + e \Rightarrow \\ a + p + d + e &= b + c + e \Rightarrow \\ a + p + c + f + q &= b + c + e \Rightarrow \\ a + f + p + q &= b + e \Rightarrow \\ a + f &\leq b + e \Rightarrow \\ \overline{(a, b)} &\leq \overline{(e, f)}. \end{aligned}$$

□

É importante observar que a relação de ordem em \mathbb{Z} está bem definida. A proposição abaixo irá evidenciar isto.

Proposição 3.7.9. *Sejam $\overline{(a, b)}, \overline{(c, d)}, \overline{(a', b')}, \overline{(c', d')} \in \mathbb{Z}$ e $p \in \mathbb{N}$ tais que $\overline{(a, b)} = \overline{(a', b')}$ e $\overline{(c, d)} = \overline{(c', d')}$. Se $\overline{(a, b)} \leq \overline{(c, d)}$ então $\overline{(a', b')} \leq \overline{(c', d')}$.*

Demonstração. Por hipótese, tem-se que:

- $a + b' = b + a' \Rightarrow a = b + a' - b'$;
- $c + d' = d + c' \Rightarrow c = d + c' - d'$;
- $a + d \leq b + c \Rightarrow b + c = a + d + p$.

Dessa maneira, $a' - b' + p = c' - d' \Rightarrow a' + d' \leq c' + b' \Rightarrow \overline{(a', b')} \leq \overline{(c', d')}$.

Analogamente,

- $\overline{(a, b)} \geq \overline{(c, d)} \Rightarrow \overline{(a', b')} \geq \overline{(c', d')}$;
- $\overline{(a, b)} > \overline{(c, d)} \Rightarrow \overline{(a', b')} > \overline{(c', d')}$;
- $\overline{(a, b)} < \overline{(c, d)} \Rightarrow \overline{(a', b')} < \overline{(c', d')}$.

□

Teorema 3.7.10. *A relação \leq é compatível com as operações em \mathbb{Z} , isto é, para $\alpha = \overline{(a, b)}, \beta = \overline{(c, d)}$ e $\gamma = \overline{(e, f)}$ inteiros, vale:*

$$(i) \alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma;$$

$$(ii) \alpha \leq \beta \text{ e } \gamma \geq \overline{(0, 0)} \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma.$$

Demonstração.

- (i) De fato, tem-se que $a + d \leq b + c$. Consequentemente $a + d + e + f \leq b + c + e + f$, então $a + e + d + f \leq b + f + c + e$, ou seja, $\overline{(a + e, b + f)} \leq \overline{(c + e, d + f)}$. Sendo assim, $\overline{(a, b)} + \overline{(e, f)} \leq \overline{(c, d)} + \overline{(e, f)}$ e assim, $\alpha + \gamma \leq \beta + \gamma$.
- (ii) Tem-se que $a + d \leq b + c$ e $e + 0 \geq f + 0 \Rightarrow e \geq f$. Daí, existem p e q naturais, tais que:

$$(1) \quad b + c = a + d + p \Rightarrow bf + cf = af + df + pf$$

$$(2) \quad b + c = a + d + p \Rightarrow be + ce = ae + de + pe$$

$$(3) \quad e = f + q \Rightarrow pe = pf + pq$$

Somando o primeiro membro da equação (1) com o segundo membro da equação (2) e vice-versa tem-se que:

$$ae + bf + cf + de + pe = be + ce + af + df + pf \Rightarrow$$

Substituindo a equação (3) na equação anterior, tem-se que:

$$ae + bf + cf + de + pf + pq = be + ce + af + df + pf \Rightarrow$$

$$ae + bf + cf + de + pq = be + ce + af + df \Rightarrow$$

$$ae + bf + cf + de \leq af + be + ce + df \Rightarrow$$

$$\overline{(ae + bf, af + be)} \leq \overline{(ce + df, cf + de)} \Rightarrow$$

$$\overline{(a, b)} \cdot \overline{(e, f)} \leq \overline{(c, d)} \cdot \overline{(e, f)} \Rightarrow$$

$$\alpha \cdot \gamma \leq \beta \cdot \gamma. \quad \square$$

Proposição 3.7.11. Para $\alpha = \overline{(a, b)}$ inteiro arbitrário, apenas uma das situações ocorre: $\alpha = \overline{(0, 0)}$ ou $\alpha < \overline{(0, 0)}$ ou $\alpha > \overline{(0, 0)}$.

Demonstração. Suponhamos que $\alpha < \overline{(0, 0)}$ e $\alpha = \overline{(0, 0)}$ simultaneamente. Dessa forma, tem-se $a < b$ e $a = b$, respectivamente. Isto é uma contradição devido a tricotomia dos naturais. Analogamente, supondo $\alpha < \overline{(0, 0)}$ e $\alpha > \overline{(0, 0)}$, tem-se $a < b$ e $a > b$ e supondo ainda $\alpha > \overline{(0, 0)}$ e $\alpha = \overline{(0, 0)}$, tem-se $a > b$ e $a = b$. As duas possibilidades supostas são contradições pois de forma semelhante à primeira são contrárias à tricotomia dos naturais. \square

Proposição 3.7.12 (tricotomia nos inteiros). Para $\alpha = \overline{(a, b)}$ e $\beta = \overline{(c, d)}$ inteiros, ocorre: $\alpha = \beta$ ou $\alpha < \beta$ ou $\alpha > \beta$.

Demonstração. Suponhamos que $\alpha < \beta$ e $\alpha = \beta$ simultaneamente. Dessa forma, tem-se $a + d < b + c$ e $a + d = b + c$, respectivamente. Isto é uma contradição devido à tricotomia dos naturais. Analogamente, supondo $\alpha < \beta$ e $\alpha > \beta$, tem-se $a + d < b + c$ e $a + d > b + c$ e

supondo ainda $\alpha > \beta$ e $\alpha = \beta$, tem-se $a + d > b + c$ e $a + d = b + c$. As duas possibilidades supostas são contradições pois de forma semelhante à primeira são contrárias à tricotomia dos naturais. \square

3.7.3 Relação de ordem em \mathbb{Q}

Definição 3.7.13. Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais com $b, d > 0$. Escrevemos $\frac{a}{b} \leq \frac{c}{d}$ quando $ad \leq bc$ e dizemos que $\frac{a}{b}$ é menor do que ou igual a $\frac{c}{d}$.

Os símbolos $\geq, <$ e $>$ definem-se de forma análoga ao feito com os naturais e inteiros.

Proposição 3.7.14. A relação \leq apresentada na definição 3.7.13 está bem definida.

Demonstração. De fato, se $\frac{a}{b} = \frac{a'}{b'}$, ou seja, $ab' = ba'$ e $\frac{a}{b} \leq \frac{c}{d}$, ou seja $ad \leq bc$, então $adb' \leq bcb'$, já que $b' > 0$. Sendo assim, $ab'd \leq bcb' \Rightarrow ba'd \leq bcb' \Rightarrow a'd \leq cb' \Rightarrow a'd \leq b'c \Rightarrow \frac{a'}{b'} \leq \frac{c}{d}$. De forma análoga, se $\frac{c}{d} = \frac{c'}{d'}$ e $\frac{a'}{b'} \leq \frac{c}{d}$ então: $a'd \leq b'c$ e $cd' = dc' \Rightarrow a'dd' \leq b'cd' \leq a'dd' \leq b'dc' \Rightarrow a'd' \leq b'c' \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}$.

Dessa maneira, $\frac{a}{b} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}$. Concluindo assim que $\frac{a}{b} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}$, ou seja, \leq está bem definida. \square

Proposição 3.7.15. A relação \leq apresentada na definição 3.7.13 é uma relação de ordem em \mathbb{Q} .

Demonstração. Deseja-se provar que \leq é reflexiva, antissimétrica e transitiva. De fato, sejam $r = \frac{a}{b}$, $s = \frac{c}{d}$ e $t = \frac{e}{f}$ racionais arbitrários, então:

$$(i) \leq \text{ é reflexiva: } r \leq r; r \leq r \Leftrightarrow \frac{a}{b} \leq \frac{a}{b} \Leftrightarrow ab \leq ab.$$

$$(ii) \leq \text{ é antissimétrica: } r \leq s \text{ e } s \leq r \Rightarrow r = s.$$

$$(a) r \leq s \Rightarrow \frac{a}{b} \leq \frac{c}{d} \Rightarrow ad \leq bc$$

$$(b) s \leq r \Rightarrow \frac{c}{d} \leq \frac{a}{b} \Rightarrow cb \leq da$$

Sendo assim, pela tricotomia dos inteiros, $ad = bc$. Então $\frac{a}{b} = \frac{c}{d}$, ou seja, $r = s$.

$$(iii) \leq \text{ é transitiva: } r \leq s \text{ e } s \leq t \Rightarrow r \leq t; r \leq s \Leftrightarrow ad \leq bc \text{ e } s \leq t \Leftrightarrow cf \leq de \Rightarrow adf \leq bcf \text{ e } bcf \leq bde \Rightarrow adf \leq bde \Rightarrow af \leq be \Rightarrow r \leq t.$$

\square

Proposição 3.7.16. (compatibilidade da ordem com as operações em \mathbb{Q}) Sejam $r, s, t \in \mathbb{Q}$, vale:

$$(1) r \leq s \Leftrightarrow r + t \leq s + t;$$

$$(2) r \leq s \text{ e } t \geq \frac{0}{1} \Rightarrow rt \leq st;$$

$$(3) r \leq s \text{ e } t \leq \frac{0}{1} \Rightarrow rt \geq st.$$

Demonstração. Sejam $r = \frac{a}{b}$, $s = \frac{c}{d}$ e $t = \frac{e}{f}$.

$$(1) r \leq s \Leftrightarrow \frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc \Leftrightarrow adf \leq bcf \Leftrightarrow adf + dbe \leq bcf + dbe \Leftrightarrow d(af + be) \leq b(cf + de) \Leftrightarrow df(af + be) \leq bf(cf + de) \Leftrightarrow \frac{af + be}{bf} \leq \frac{cf + de}{df} \Leftrightarrow \frac{a}{b} + \frac{e}{f} \leq \frac{c}{d} + \frac{e}{f} \Leftrightarrow r + t \leq s + t;$$

$$(2) r \leq s \text{ e } t \geq \frac{0}{1} \Leftrightarrow ad \leq bc \text{ e } e \geq 0 \Leftrightarrow aedf \leq bcef \Leftrightarrow aedf \leq bfce \Leftrightarrow \frac{ae}{bf} \leq \frac{ce}{df} \Leftrightarrow \frac{ae}{bf} \leq \frac{ce}{df} \Leftrightarrow rt \leq st;$$

$$(3) r \leq s \text{ e } t \leq \frac{0}{1} \Leftrightarrow ad \leq bc \text{ e } e \leq 0 \Leftrightarrow aedf \geq bcef \Leftrightarrow aedf \geq bfce \Leftrightarrow \frac{ae}{bf} \geq \frac{ce}{df} \Leftrightarrow \frac{ae}{bf} \geq \frac{ce}{df} \Leftrightarrow rt \geq st; \quad \square$$

Teorema 3.7.17. (tricotomia nos racionais) Dados $r, s \in \mathbb{Q}$ uma, e apenas uma, das seguintes situações ocorre: ou $r = s$; ou $r < s$; ou $r > s$.

Demonstração. Sejam $r = \frac{a}{b}$ e $s = \frac{c}{d}$ com $b, d > 0$ tem-se que:

- $r = s \Leftrightarrow ad = bc$
- $r < s \Leftrightarrow ad < bc$
- $r > s \Leftrightarrow ad > bc$

Porém, a validade de uma das afirmações acima exclui as outras pela tricotomia dos inteiros. \square

3.7.4 Relação de ordem em \mathbb{R}

Definição 3.7.18. Sejam $\alpha, \beta \in \mathbb{R}$ diz-se que α é menor do que β e escreve-se $\alpha < \beta$ quando $\beta - \alpha \neq \emptyset$

Definição 3.7.19. Se $\alpha \in C$ e $\alpha > 0^*$, α chama-se corte positivo. Caso $\alpha < 0^*$, α é dito negativo. Se $\alpha \geq 0^*$, α é dito corte não-negativo. Caso $\alpha \leq 0^*$, α é dito corte não-positivo.

Se $\alpha, \beta \in \mathbb{R}$ é possível mostrar que $\alpha < \beta \Leftrightarrow \alpha \subset \beta$ e $\alpha \neq \beta$ e que $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$. Além disso, vale o seguinte resultado.

Teorema 3.7.20 (tricotomia nos reais). *Sejam $\alpha, \beta \in \mathbb{R}$, uma, e somente uma, das possibilidades abaixo ocorre: ou $\alpha = \beta$; ou $\alpha < \beta$; ou $\alpha > \beta$.*

Demonstração. A demonstração desta proposição pode ser encontrada em ([10], p. 89). □

Teorema 3.7.21. *A relação \leq é uma relação de ordem.*

Demonstração. De fato, \leq é:

- (1) reflexiva: Seja $\alpha \in C$ tem-se que $\alpha = \alpha$ logo $\alpha \leq \alpha$.
- (2) antissimétrica: Sejam $\alpha, \beta \in C$ tem-se que $\alpha \leq \beta$ e $\beta \leq \alpha \Rightarrow \alpha \subset \beta$ e $\beta \subset \alpha \Rightarrow \alpha = \beta$.
- (3) transitiva: Sejam $\alpha, \beta, \gamma \in C$ tem-se que $\alpha \leq \beta$ e $\beta \leq \gamma \Rightarrow \alpha \subset \beta$ e $\beta \subset \gamma \Rightarrow \alpha \subset \gamma \Rightarrow \alpha \leq \gamma$. □

3.8 Cópias algébricas

O próximo resultado mostra precisamente o significado da afirmação $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Teorema 3.8.1. *Sejam as funções $f : \mathbb{N} \rightarrow \mathbb{Z}$ dada por $f(m) = \overline{(m, 0)}$, para todo $m \in \mathbb{N}$, $g : \mathbb{Z} \rightarrow \mathbb{Q}$ tal que $g(n) = \frac{n}{1}$, para todo $n \in \mathbb{Z}$ e $j : \mathbb{Q} \rightarrow \mathbb{R}$ dada por $j(r) = r^*$, para todo $r \in \mathbb{Q}$. Então f , g e j são injetoras. Além disso,*

$$(N1) \quad f(m + n) = f(m) + f(n);$$

$$(N2) \quad f(m \cdot n) = f(m) \cdot f(n);$$

$$(N3) \quad m \leq n \Rightarrow f(m) \leq f(n);$$

$$(Z1) \quad g(m + n) = g(m) + g(n);$$

$$(Z2) \quad g(mn) = g(m)g(n);$$

$$(Z3) \quad m \leq n \Rightarrow g(m) \leq g(n);$$

$$(Q1) \quad j(p) + j(q) = j(p + q), \text{ ou seja, } p^* + q^* = (p + q)^*;$$

$$(Q2) \quad j(p) \cdot j(q) = j(p \cdot q), \text{ ou seja, } p^* \cdot q^* = (p \cdot q)^*;$$

(Q3) $j(p) < j(q) \Leftrightarrow p < q$, ou seja, $p^* < q^* \Leftrightarrow p < q$;

(Q4) $j(p) = j(q) \Leftrightarrow p = q$, ou seja, $p^* = q^* \Leftrightarrow p = q$.

Demonstração. De fato, supondo $m, n \in \mathbb{N}$, tal que $f(m) = f(n)$, então $\overline{(m, 0)} = \overline{(n, 0)} \Rightarrow m + 0 = 0 + n = m + n$. Sendo assim, f é injetora. Além disso,

(N1) $f(m + n) = \overline{(m + n, 0)} = \overline{(m, 0)} + \overline{(n, 0)} = f(m) + f(n)$;

(N2) $f(m \cdot n) = \overline{(m \cdot n, 0)} = \overline{(m \cdot n + 0 \cdot 0, m \cdot 0 + 0 \cdot n)} = \overline{(m, 0)} \cdot \overline{(n, 0)} = f(m) \cdot f(n)$;

(N3) $m \leq n \Rightarrow m + 0 \leq n + 0 \Rightarrow \overline{(m, 0)} \leq \overline{(n, 0)} \Rightarrow f(m) \leq f(n)$.

Por outro lado, sejam $m, n \in \mathbb{Z}$, suponha que $g(m) = g(n) \Rightarrow \frac{m}{1} = \frac{n}{1} \Rightarrow m \cdot 1 = 1 \cdot n \Rightarrow m = n$. Sendo assim, g é injetora.

Além disso,

(Z1) $g(m + n) = \frac{m + n}{1} = \frac{m \cdot 1 + 1 \cdot n}{1 \cdot 1} = \frac{m}{1} + \frac{n}{1} = g(m) + g(n)$;

(Z2) $g(mn) = \frac{mn}{1} = \frac{m}{1} \frac{n}{1} = g(m)g(n)$;

(Z3) $m \leq n \Rightarrow m \cdot 1 \leq n \cdot 1 \Rightarrow \frac{m}{1} \leq \frac{n}{1} \Rightarrow g(m) \leq g(n)$;

Tem-se ainda que, supondo $m, n \in \mathbb{Q}$, $j(m) = j(n) \Rightarrow m^* = n^* \Rightarrow m = n$. Sendo assim, j é injetora. Além disso,

(Q1) $p^* + q^* = (p + q)^*$;

De fato,

(a) Seja $a \in p^* + q^*$ então $a = r + s$, $r \in p^*$ e $s \in q^*$, ou seja, $r < p$ e $s < q$. Sendo assim, $a = r + s < p + q$, ou seja, $a \in (p + q)^*$;

(b) Seja $b \in (p + q)^*$ então $b < p + q$. Sejam $h = p + q - b$, $s = p - \frac{h}{2}$ e $t = q - \frac{h}{2}$, tem-se que $s < p$ e $t < q$, ou seja, $s \in p^*$ e $t \in q^*$. Assim, $b = s + t \in p^* + q^*$.

(Q2) $p^* \cdot q^* = (p \cdot q)^*$; A demonstração será feita para $p^* > 0$ e $q^* > 0$. Os outros casos são demonstrados de maneira análoga.

(a) Seja $a \in p^*q^*$ então $a < 0$ ou $a = rs$; $r \in p^*$, $s \in q^*$, $r \geq 0$ e $s \geq 0$. Assim, $r < p$ e $s < q$, conseqüentemente, $rs < pq$, ou ainda, $rs < 0$. Sendo assim, $r \in (pq)^*$;

(b) Seja $b \in (pq)^*$ então $b < 0$ ou $0 \leq b < pq$. Se $b < 0$ então $b \in p^*q^*$ pela definição de produto de cortes. Se $0 \leq b < pq$ então existem p_1 e q_1 racionais, tais que $0 < p_1 < p$, $0 < q_1 < q$, $r < p_1q_1 < pq$. Dessa forma, $p_1 \in p$ e $q_1 \in q$ e conseqüentemente $p_1q_1 \in p^*q^* \Rightarrow b \in p^*q^*$;

(Q3) $p^* < q^* \Leftrightarrow p < q$;

De fato,

(\Rightarrow) Se $p^* < q^*$ então existe $r \in q^*$ tal que $r \notin p^*$, ou seja, $r < q$ e $r \geq p$. Dessa maneira, $p \leq r < q \Rightarrow p < q$.

(\Leftarrow) Se $p < q$ então $p \in q^*$. Como $p \notin p^*$ então tem-se que $(q^* - p^*) \neq \emptyset$, ou seja, $p^* < q^*$;

(Q4) $p^* = q^* \Leftrightarrow p = q$.

De fato,

(\Rightarrow) Se $p^* = q^*$, tem-se que $p \notin p^* \Rightarrow p \notin q^* \Rightarrow p \geq q$, analogamente, $q \notin q^* \Rightarrow q \notin p^* \Rightarrow q \geq p$. Consequentemente, pela tricotomia, tem-se $p = q$.

(\Leftarrow) Se $p = q$ então é notável que $p^* = q^*$; □

Exemplo 3.8.2. *Seguem alguns exemplos do fato evidenciado no teorema acima.*

- $3 + 10 = 13$ corresponde a $\overline{(3, 0)} + \overline{(10, 0)} = \overline{(13, 0)}$ (via f);
- $3 \cdot 10 = 30$ corresponde a $\overline{(3, 0)} \cdot \overline{(10, 0)} = \overline{(30, 0)}$ (via f);
- $3 \leq 10$ corresponde a $\overline{(3, 0)} \leq \overline{(10, 0)}$.

Com base no Teorema 3.8.1 concluímos que o conjunto $f(\mathbb{N}) = \mathbb{Z}_+$ mantém a estrutura algébrica de \mathbb{N} já que tem-se um homomorfismo injetor². A preservação da ordem confirma a ideia de que a ordem em \mathbb{Z} é uma extensão da ordem em \mathbb{N} . Assim, diferentemente do citado no ensino médio, tem-se que \mathbb{N} não é subconjunto de \mathbb{Z} . Na verdade, \mathbb{N} e \mathbb{Z}_+ são semelhantes no que diz respeito às estruturas algébricas e ao ordenamento, no entanto, estes conjuntos são de “naturezas” diferentes. Dessa forma, considera-se \mathbb{Z}_+ uma cópia algébrica de \mathbb{N} . Sendo assim, \mathbb{Z}_+ está contido em \mathbb{Z} .

Analogamente, o conjunto $g(\mathbb{Z}) = \left\{ \frac{n}{1}; n \in \mathbb{Z} \right\}$ é uma cópia algébrica de \mathbb{Z} em \mathbb{Q} . Assim, novamente, fazendo um comparativo com o ensino básico, tem-se que \mathbb{Z} não é, propriamente, subconjunto de \mathbb{Q} . De fato, \mathbb{Z} e $g(\mathbb{Z})$ são semelhantes no que diz respeito às estruturas algébricas e ao ordenamento.

Note ainda que existe um homomorfismo injetor entre o corpo ordenado de todos os números racionais e o corpo ordenado de todos os cortes racionais, isto é, $j(\mathbb{Q})$ é uma cópia algébrica de \mathbb{Q} em \mathbb{R} . Isto permite identificar o corte racional r^* como número racional r , ou seja, no que diz respeito às operações de adição, multiplicação e da relação

²Um homomorfismo é uma aplicação que preserva a estrutura entre duas estruturas algébricas (como por exemplo grupos, anéis, espaços vetoriais ou álgebras)

de ordem, não há distinção entre \mathbb{Q} e o conjunto dos cortes racionais. Claramente r e r^* não são o mesmo elemento, mas as propriedades que interessam (aritméticas e de ordem) são as mesmas nos dois corpos ordenados. Por fim, note que $(\mathbb{R} - j(\mathbb{Q})) \neq \emptyset$, pois existem cortes não racionais em \mathbb{R} .

Capítulo 4

Conjuntos numéricos: quatérnios e octônios

Neste capítulo apresentaremos os conjuntos numéricos, a saber: os quatérnios e os octônios, denotados por \mathbb{H} e \mathbb{O} , respectivamente. Como veremos, tais conjuntos representarão duas extensões para a sequência de inclusões: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Explicitamente, mostraremos que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$.

Inicialmente, apresentaremos um breve histórico quanto ao surgimento de tais conjuntos, em seguida, formalizaremos suas construções.

As principais referências utilizadas neste capítulo foram [8, 20, 23, 28].

4.1 Os quatérnios

No século *XIX*, ao mostrar que um número complexo $a + bi$ nada mais é do que um par ordenado (a, b) , Hamilton criou uma álgebra, que possibilitaria tratar com os vetores no plano. Uma questão natural surge a partir desta formulação apresentada por Hamilton para os números complexos, a saber: é possível definir uma estrutura algébrica, similar a apresentada para os números complexos, que permita operar com vetores no espaço? Ele trabalhou durante dez anos com este objetivo, e primeiramente criou uma estrutura ao qual denominou “Hipercomplexos”, os quais poderiam ser representados através de ternas. No entanto, a estrutura algébrica das ternas continha um problema ao qual relata em uma carta enviada ao seu filho *Archibald* em outubro de 1843:

Toda manhã, quando descia para o café, teu irmão William Edwin e você mesmo costumavam perguntar-me “Bem, pai, você já pode multiplicar ternas?” A isso eu sempre me via obrigado a responder, com um triste balanço de cabeça, “Não, eu apenas posso somá-las e subtrai-las”. ([22], p 34, 2004).

Na tentativa de tornar viável a multiplicação daquilo que denominava “ternas”, Hamilton as representou de forma análoga aos complexos, acrescentando a estes uma outra “unidade imaginária” (j). A partir daí, ele tentou desenvolver o produto $(a+bi+cj)(x+yi+zj)$ e representar o mesmo como uma terna, sem sucesso. Além disso, Hamilton buscava que o comprimento do produto dos vetores fosse igual ao produto dos comprimentos, ou seja, $|(a+bi+cj)(x+yi+zj)| = |(a+bi+cj)||x+yi+zj|$, sendo que o módulo ou comprimento das ternas era obtido no sentido euclidiano. Hamilton chamava isto de “Lei dos Módulos”.

Supondo verdadeira a Lei dos Módulos, uma expressão consequente ilustra o principal questionamento de Hamilton,

$$\begin{aligned}
\|(a+bi+cj)(a+bi+cj)\| &= \|(a+bi+cj)\|(a+bi+cj)\| \\
\|(a+bi+cj)^2\| &= \|(a+bi+cj)\|^2 \\
\|a^2 - b^2 - c^2 + 2abi + 2acj + bcij + cbji\| &= (\sqrt{a^2 + b^2 + c^2})^2 \\
\|a^2 - b^2 - c^2 + 2abi + 2acj + 2bcij\| &= (\sqrt{a^2 + b^2 + c^2})^2 \\
\sqrt{(a^2 - b^2 - c^2)^2 + (2ab)^2 + (2ac)^2 + (2bc)^2} &= a^2 + b^2 + c^2 \\
&\vdots \\
a^4 + b^4 + c^4 + 2a^2b^2 + 2b^2c^2 + 2a^2c^2 + 4b^2c^2 &= (a^2 + b^2 + c^2)^2
\end{aligned}$$

Note que esta igualdade só é verdadeira se o termo $4b^2c^2$ for nulo. Numa primeira análise, Hamilton decidiu tornar $ij = 0$ para assim tornar o respectivo termo nulo, no entanto, esta tentativa não o satisfaz. Numa nova tentativa, Hamilton faz $ij = k$ e $ji = -k$, daí,

$$\begin{aligned}
\|a^2 - b^2 - c^2 + 2abi + 2acj + bcij + cbji\| &= (\sqrt{a^2 + b^2 + c^2})^2 \\
\|a^2 - b^2 - c^2 + 2abi + 2acj + bck - cbk\| &= (\sqrt{a^2 + b^2 + c^2})^2 \\
\|a^2 - b^2 - c^2 + 2abi + 2acj\| &= (\sqrt{a^2 + b^2 + c^2})^2 \\
\sqrt{(a^2 - b^2 - c^2)^2 + (2ab)^2 + (2ac)^2} &= a^2 + b^2 + c^2 \\
&\vdots \\
a^4 + b^4 + c^4 + 2a^2b^2 + 2b^2c^2 + 2a^2c^2 &= (a^2 + b^2 + c^2)^2
\end{aligned}$$

O que torna válida a “lei dos módulos”. Os trechos abaixo evidenciam a decisão de Hamilton em acrescentar o termo k .

“Eis-me, portanto, tentado por um momento a imaginar que $ij = 0$. Mas isso pareceu-me estranho e desconfortável, e percebi que a supressão do termo a mais, pode ser obtida supondo o que me pareceu menos chocante, isto é, que $ij = k, ji = -k$, reservando-me a pergunta se k era ou não 0. ([8], 2013 apud [5], 2012, p.197).

[...]e transferindo este paradoxo para a álgebra devemos admitir um terceiro símbolo imaginário k , que não deve ser confundido com i ou $j \dots$ e fui assim conduzido a introduzir quatérnios tais como $a+bi+cj+dk$ ou (a, b, c, d) ”. ([22], p 34, 2004).

Em mais um trecho das cartas enviadas a seu filho, Hamilton relata o momento da descoberta final.

“Mas no dia 16 do mesmo mês [outubro de 1843] - que era uma segunda-feira e dia de reunião do Conselho da Real Sociedade da Irlanda - eu ia andando para participar e presidir, e tua mãe andava comigo, ao longo do Royal Canal, \dots , embora ela falasse comigo ocasionalmente, uma corrente subjacente de pensamento estava acontecendo na minha mente, que finalmente teve um resultado, cuja importância senti imediatamente. Pareceu como se um circuito elétrico tivesse se fechado; e saltou uma faísca, o heraldo de muitos anos vindouros de pensamento e trabalho dirigidos, por mim, se poupado, e de qualquer forma por parte de outros, se eu vivesse o suficiente para comunicar minha descoberta. Nesse instante eu peguei uma libreta de anotações que ainda existe e fiz um registro naquela hora. Não pude resistir ao impulso - tão não filosófico quanto possa ser - de gravar com um canivete numa pedra da ponte de Brougham, quando a cruzamos, a fórmula fundamental dos símbolos i, j, k [...].

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

[...] que contém a solução do problema”. ([22], p 34, 2004)

Hamilton considerava Jhon Graves o seu melhor amigo e foi a ele que relatou sua descoberta, mencionando o acréscimo do k e a sua relação com os cálculos com as ternas ou ternos, como o próprio se referia:

“[...] e ali me dei conta que temos de admitir, em certo sentido, uma quarta dimensão do espaço, para se conseguir calcular com ternos”. ([8], 2013 apud [5], 2012, p.197).

Através da maneira como Hamilton define k fica claro que não é válida a comutatividade nos quatérnios. Posteriormente será visto que o anel dos quatérnios configura-se como o primeiro anel não comutativo com divisão. Vale ressaltar que a forma como se calcula k evidencia a validade da propriedade associativa para os quatérnios. De fato,

$$k^2 = (ij)(ij) = i(ji)j = -i(ij)j = -i^2j^2 = -1$$

Com isto, temos a seguinte tábua multiplicativa para os elementos i, j, k .

\cdot	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Tabela 4.1: Tábua multiplicativa

Na prática, usa-se ao invés da tábua multiplicativa acima, o diagrama circular abaixo, no qual as setas indicam se o sinal da multiplicação será positivo ou negativo.

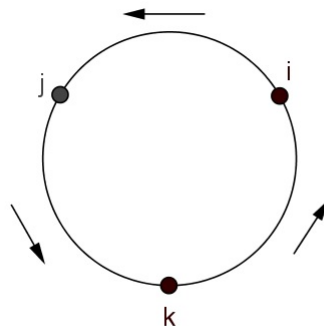


Figura 4.1: Diagrama multiplicativo dos quatérnios

Abaixo, apresentamos uma formulação atual para a definição dos quatérnios.

Definição 4.1.1. *Dados $a_1 = (w_1, x_1, y_1, z_1)$ e $a_2 = (w_2, x_2, y_2, z_2)$ elementos do \mathbb{R}^4 e $\alpha \in \mathbb{R}$, definimos o conjunto dos quatérnios, e denotamos por \mathbb{H}^1 , como sendo o conjunto \mathbb{R}^4 munido das operações de adição, multiplicação e da multiplicação por escalar:*

$$\begin{aligned}
 (+) : \mathbb{R}^4 \times \mathbb{R}^4 &\rightarrow \mathbb{R}^4 & (\cdot) : \mathbb{R} \times \mathbb{R}^4 &\rightarrow \mathbb{R}^4 \\
 (a_1; a_2) &\mapsto (w_1 + w_2, x_1 + x_2, y_1 + y_2, z_1 + z_2) & (\alpha; a_1) &\mapsto (\alpha w_1, \alpha x_1, \alpha y_1, \alpha z_1) \\
 (\cdot) : \mathbb{R}^4 \times \mathbb{R}^4 &\rightarrow \mathbb{R}^4 \\
 (a_1, a_2) &\mapsto (w_1 w_2 - (x_1 x_2 + y_1 y_2 + z_1 z_2); w_1 x_2 + x_1 w_2 + y_1 z_2 - z_1 y_2; \\
 &w_1 y_2 - x_1 z_2 + y_1 w_2 + z_1 x_2; w_1 z_2 + x_1 y_2 - y_1 x_2 + z_1 w_2).
 \end{aligned}$$

Note que a partir da definição podemos identificar um quatérnio w , como sendo um elemento do conjunto $\mathbb{C} + \mathbb{C}j$.

¹o \mathbb{H} utilizado para denotar os quatérnios foi escolhido em homenagem a Hamilton

4.1.1 Um argumento para a regra da multiplicação dos quatérnios

Usando a tábua multiplicativa e o fato que dados $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ e $k = (0, 0, 0, 1)$ elementos de \mathbb{R}^4 , podemos escrever quaisquer elementos a_1 e a_2 de \mathbb{R}^4 da seguinte forma:

$$\begin{aligned} a_1 &= w_1 \cdot 1 + x_1 \cdot i + y_1 \cdot j + z_1 \cdot k = w_1 + x_1 i + y_1 j + z_1 k \\ a_2 &= w_2 \cdot 1 + x_2 \cdot i + y_2 \cdot j + z_2 \cdot k = w_2 + x_2 i + y_2 j + z_2 k. \end{aligned}$$

Temos que

$$\begin{aligned} a_1 \cdot a_2 &= (w_1, x_1, y_1, z_1) \cdot (w_2, x_2, y_2, z_2) \\ &= (w_1 \cdot 1 + x_1 \cdot i + y_1 \cdot j + z_1 \cdot k) \cdot (w_2 \cdot 1 + x_2 \cdot i + y_2 \cdot j + z_2 \cdot k). \end{aligned}$$

Aplicando a propriedade distributiva para as coordenadas dos vetores da igualdade anterior, temos que:

$$\begin{aligned} a_1 \cdot a_2 &= w_1 \cdot w_2 + w_1 \cdot x_2 \cdot i + w_1 \cdot y_2 \cdot j + w_1 \cdot z_2 \cdot k + x_1 \cdot i \cdot w_2 + x_1 \cdot i \cdot x_2 \cdot i + x_1 \cdot i \cdot y_2 \cdot j + x_1 \cdot i \cdot z_2 \cdot k + \\ &+ y_1 \cdot j \cdot w_2 + y_1 \cdot j \cdot x_2 \cdot i + y_1 \cdot j \cdot y_2 \cdot j + y_1 \cdot j \cdot z_2 \cdot k + z_1 \cdot k \cdot w_2 + z_1 \cdot k \cdot x_2 \cdot i + \\ &+ z_1 \cdot k \cdot y_2 \cdot j + z_1 \cdot k \cdot z_2 \cdot k \Rightarrow \end{aligned}$$

$$\begin{aligned} a_1 \cdot a_2 &= w_1 w_2 + w_1 x_2 i + w_1 y_2 j + w_1 z_2 k + x_1 w_2 i - x_1 x_2 + x_1 y_2 k - x_1 z_2 j + \\ &+ y_1 w_2 j - y_1 x_2 k - y_1 y_2 + y_1 z_2 i + z_1 w_2 k + z_1 x_2 j - z_1 y_2 i - z_1 z_2 \Rightarrow \end{aligned}$$

$$\begin{aligned} a_1 \cdot a_2 &= w_1 w_2 - x_1 x_2 - y_1 y_2 - z_1 z_2 + w_1 x_2 i + x_1 w_2 i + y_1 z_2 i - z_1 y_2 i + \\ &+ w_1 y_2 j - x_1 z_2 j + y_1 w_2 j + z_1 x_2 j + w_1 z_2 k + x_1 y_2 k - y_1 x_2 k + z_1 w_2 k \Rightarrow \end{aligned}$$

$$\begin{aligned} a_1 \cdot a_2 &= w_1 w_2 - (x_1 x_2 + y_1 y_2 + z_1 z_2) + (w_1 x_2 + x_1 w_2 + y_1 z_2 - z_1 y_2) i + \\ &+ (w_1 y_2 - x_1 z_2 + y_1 w_2 + z_1 x_2) j + (w_1 z_2 + x_1 y_2 - y_1 x_2 + z_1 w_2) k. \end{aligned}$$

4.2 Os octônios

A descoberta dos octônios é atribuído a Jhon Graves (1806 – 1870). Os octônios são tão intrigantes quanto os quatérnios, no entanto, a operação de multiplicação não é comutativa e nem associativa.

Inicialmente, não se percebia uma aplicação geométrica para os octônios o que justifica o desinteresse de Hamilton por este conjunto, já que para ele a matemática deveria estar associada à realidade. Este fato contribuiu para que as ideias de Graves não fossem amplamente divulgadas na época. Somente no ano de 1845, Arthur Cayley (1821 – 1895) mostrou como descrever rotações usando multiplicação de octônios. Por essa razão os octônios são conhecidos como números de Cayley.

Há de se notar algo quanto a relação entre Graves e Cayley. Ambos foram matemáticos e advogados e durante a conferência de Hamilton sobre os Quatérnios em que os dois assistiram em Dublin, eles se conheceram e passaram a trocar ideias matemáticas por muitos anos. Graves estava ansioso para que Cayley avançasse os estudos e descobrisse algo sobre os Octônios. Cayley e Graves eram contatos do *University College*.

A seguir apresentaremos a construção formal dos octônios.

Definição 4.2.1. *Dados $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ e $y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$ elementos do \mathbb{R}^8 e α um elemento qualquer do conjunto dos números reais, definimos como sendo o conjunto dos octônios, e denotamos por \mathbb{O} ,² o conjunto \mathbb{R}^8 munido das operações de adição, multiplicação e da multiplicação por escalar:*

$$\begin{aligned} (+) : \mathbb{R}^8 \times \mathbb{R}^8 &\rightarrow \mathbb{R}^8 & (\cdot) : \mathbb{R}^8 \times \mathbb{R}^8 &\rightarrow \mathbb{R}^8 & \mathbb{R} \times \mathbb{R}^8 &\rightarrow \mathbb{R}^8 \\ (x, y) &\mapsto x + y & (x, y) &\mapsto x \cdot y & (\alpha, x) &\mapsto \alpha \cdot x \end{aligned}$$

A fim de compreendermos a definição da multiplicação de octônios (por não ser, em princípio, tão natural), somente na próxima seção é que apresentaremos as definições de adição e multiplicação por escalar, de octônios, conjuntamente com a definição de multiplicação de octônios, seguida de um argumento para esta regra de multiplicação.

Antes, porém, observemos que sendo x um octônio, podemos denotar, $x = x_1 + x_2i + x_3j + x_4k + x_5il + x_6jl + x_7kl + x_8l$, em que $x_1, x_2, x_3, \dots, x_8 \in \mathbb{R}$ (x_1 é chamado parte real de x e $x_2i + x_3j + x_4k + x_5il + x_6jl + x_7kl + x_8l$ é chamada parte imaginária de x). Além disso, dados dois octônios $x = x_1 + x_2i + x_3j + x_4k + x_5il + x_6jl + x_7kl + x_8l$ e $y = y_1 + y_2i + y_3j + y_4k + y_5il + y_6jl + y_7kl + y_8l$ eles serão iguais, quando $x_m = y_m$, com $m \in \{1, 2, 3, \dots, 8\}$.

4.2.1 Um argumento para a regra da multiplicação dos octônios

A adição de octônios e a multiplicação por escalar seguem os mesmos “padrões” estabelecidos nos quatérnios. A definição das mesmas segue abaixo:

$$\begin{aligned} x + y &:= (x_1 + y_1) + (x_2 + y_2)i + (x_3 + y_3)j + (x_4 + y_4)k + \\ &\quad + (x_5 + y_5)il + (x_6 + y_6)jl + (x_7 + y_7)kl + (x_8 + y_8)l \\ \alpha \cdot x &:= \alpha x_1 + \alpha x_2i + \alpha x_3j + \alpha x_4k + \\ &\quad + \alpha x_5il + \alpha x_6jl + \alpha x_7kl + \alpha x_8l. \end{aligned}$$

Já a manipulação da regra de multiplicação acima é um mero exercício de contas, que a priori não tem sentido. No entanto, é possível justificar o porquê da definição

²também conhecidos como números de Cayley

se apresentar como tal, da seguinte forma: segundo [?], para construirmos a álgebra de multiplicação dos octônios é possível observar que são necessários os elementos i, j, k , tal qual definidos para os quatérnios, e uma outra componente, denotada por l , a qual obedece as seguintes condições: $l^2 = -1$ e $(il)^2 = (jl)^2 = (kl)^2 = -1$. A multiplicação dos elementos que compõem a base é ilustrada pelo diagrama e pela tabela abaixo:

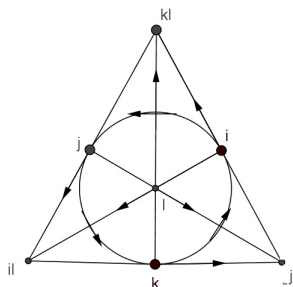


Figura 4.2: Diagrama multiplicativo dos octônios

De maneira análoga ao diagrama apresentado nos quatérnios, tem-se que os pontos do diagrama são os elementos da base dos octônios e as setas indicam o sinal do multiplicação.

\cdot	1	i	j	k	il	jl	kl	l
1	1	i	j	k	il	jl	kl	l
i	i	-1	k	$-j$	$-l$	$-kl$	jl	il
j	j	$-k$	-1	$-i$	kl	$-l$	$-il$	jl
k	k	j	$-i$	-1	$-jl$	il	$-l$	kl
il	il	l	$-kl$	jl	-1	$-k$	j	$-i$
jl	jl	kl	l	$-il$	k	-1	$-i$	$-j$
kl	kl	$-jl$	il	l	$-j$	i	-1	$-k$
l	l	$-il$	$-jl$	$-kl$	i	j	k	-1

Tabela 4.2: Tábua multiplicativa dos octônios

Desta forma, a adição, a multiplicação por escalar e a multiplicação de octônios segue o mesmo princípio empregado nos quatérnios. De fato, sejam $\alpha \in \mathbb{R}$ e $x = x_1 + x_2i + x_3j + x_4k + x_5il + x_6jl + x_7kl + x_8l$ e $y = y_1 + y_2i + y_3j + y_4k + y_5il + y_6jl + y_7kl + y_8l$ dois octônios quaisquer, tem-se que:

$$\begin{aligned}
x + y &= x_1 + x_2i + x_3j + x_4k + x_5il + x_6jl + x_7kl + x_8l + \\
&\quad + y_1 + y_2i + y_3j + y_4k + y_5il + y_6jl + y_7kl + y_8l \\
&= (x_1 + y_1) + (x_2 + y_2)i + (x_3 + y_3)j + (x_4 + y_4)k + \\
&\quad + (x_5 + y_5)il + (x_6 + y_6)jl + (x_7 + y_7)kl + (x_8 + y_8)l
\end{aligned}$$

$$\begin{aligned}
\alpha \cdot x &= \alpha(x_1 + x_2i + x_3j + x_4k + x_5il + x_6jl + x_7kl + x_8l) \\
&= \alpha x_1 + \alpha x_2i + \alpha x_3j + \alpha x_4k + \alpha x_5il + \alpha x_6jl + \alpha x_7kl + \alpha x_8l
\end{aligned}$$

$$\begin{aligned}
x \cdot y &= x_1y_1 + x_1y_2i + x_1y_3j + x_1y_4k + x_1y_5il + x_1y_6jl + x_1y_7kl + x_1y_8l + \\
&\quad + x_2iy_1 + x_2iy_2i + x_2iy_3j + x_2iy_4k + x_2iy_5il + x_2iy_6jl + x_2iy_7kl + x_2iy_8l + \\
&\quad + x_3jy_1 + x_3jy_2i + x_3jy_3j + x_3jy_4k + x_3jy_5il + x_3jy_6jl + x_3jy_7kl + x_3jy_8l + \\
&\quad + x_4ky_1 + x_4ky_2i + x_4ky_3j + x_4ky_4k + x_4ky_5il + x_4ky_6jl + x_4ky_7kl + x_4ky_8l + \\
&\quad + x_5ily_1 + x_5ily_2i + x_5ily_3j + x_5ily_4k + x_5ily_5il + x_5ily_6jl + x_5ily_7kl + x_5ily_8l + \\
&\quad + x_6jly_1 + x_6jly_2i + x_6jly_3j + x_6jly_4k + x_6jly_5il + x_6jly_6jl + x_6jly_7kl + x_6jly_8l + \\
&\quad + x_7kly_1 + x_7kly_2i + x_7kly_3j + x_7kly_4k + x_7kly_5il + x_7kly_6jl + x_7kly_7kl + x_7kly_8l + \\
&\quad + x_8ly_1 + x_8ly_2i + x_8ly_3j + x_8ly_4k + x_8ly_5il + x_8ly_6jl + x_8ly_7kl + x_8ly_8l \Rightarrow
\end{aligned}$$

$$\begin{aligned}
x \cdot y &= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8) + \\
&\quad + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 - x_5y_6 + x_6y_5 - x_7y_8 + x_8y_7)i + \\
&\quad + (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 - x_5y_7 + x_6y_8 + x_7y_5 - x_8y_6)j + \\
&\quad + (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 - x_5y_8 - x_6y_7 + x_7y_6 + x_8y_5)k + \\
&\quad + (x_1y_5 + x_2y_6 + x_3y_7 + x_4y_8 + x_5y_1 - x_6y_2 - x_7y_3 - x_8y_4)il + \\
&\quad + (x_1y_6 - x_2y_5 - x_3y_8 + x_4y_7 + x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3)jl + \\
&\quad + (x_1y_7 + x_2y_8 - x_3y_5 - x_4y_6 + x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2)kl + \\
&\quad + (x_1y_8 - x_2y_7 + x_3y_6 - x_4y_5 + x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1)l.
\end{aligned}$$

4.3 Aplicações

Existe uma ampla literatura sobre aplicações dos quatérnios e dos octônios, apresentamos abaixo uma pequena lista de trabalhos que debatem aspectos das aplicações destes conjuntos.

Em [23] é feita uma apresentação sobre o trabalho de Hamilton dando ênfase para a interpretação da multiplicação desses objetos via rotação no espaço. Em [12] é feita uma abordagem alternativa ao problema de planejamento de trajetórias empregando quatérnios como operadores espaciais, além disso é feita uma revisão da álgebra de quatérnios objetivando formar uma base sólida para a implementação de uma álgebra computacional equivalente, com o intuito de utilizar algoritmos para aproximar trajetórias de robôs em coordenadas cartesianas. Ainda em [2], [6] e [26], a rotação é feita através dos quatérnios e suas operações, assim como em [25] onde a rotação também é tratada, porém associada a um estudo comparativo baseado em critérios de custo computacional, operacionalidade e qualidade gráfica.

Em [11] é feita uma abordagem sobre a resolução de equações algébricas com coeficientes quatérnios, com ênfase nas equações quadráticas. Já em [29], além da abordagem teórica sobre os quatérnios, é feita uma extensão a suas formas menos usuais, como a forma matricial e com vetores. São apresentadas ainda importantes aplicações dos quatérnios como a rotação, computação gráfica e jogos digitais, geração de fractais, análise de circuitos elétricos, aerodinâmica e biomecânica.

Em [27] são listadas aplicações diretas dos quatérnios e rotações como estudo de atividades esportivas e lesões causadas pelas mesmas. De forma mais específica é apresentada uma “Descrição do Movimento de Rotação do Tornozelo Durante o Chute no Futebol Via Quatérnios e Ângulos de Euler” e “Simulações de movimentos para a associação dos quatérnios à nomenclatura clínica dos movimentos articulares”. Em [8] os quatérnios são associados à Astronomia.

Em [28] são apresentadas, além de outros itens, a relação entre os quatérnios e a aeronáutica, além de aplicações dos mesmos na física. Seguindo um viés semelhante, [20] cita que a teoria dos octônios em suma contribui fortemente para a Física Teórica, mais precisamente à mecânica quântica.

Capítulo 5

Estruturas Algébricas

Neste capítulo apresentaremos algumas estruturas algébricas abstratas, classificando os conjuntos numéricos apresentados nos capítulos anteriores, com respeito a estas estruturas. Para além do exercício matemático salutar de classificar objetos, esta abordagem será essencial para o desenvolvimento que será realizado no próximo capítulo. Nossas principais referências para este capítulo foram [15, 24].

Definição 5.0.1. *Seja X um conjunto não vazio. Uma estrutura algébrica em X é o par $(X, *)$, em que “ $*$ ” é o símbolo usado para representar operação binária em X . Diz-se ainda que X é o suporte da estrutura $(X, *)$.*

Para que os conjuntos possam ser classificados como estruturas algébricas, serão apresentadas a seguir as definições das operações, seguindo a formalidade matemática.

5.1 Operações nos conjuntos numéricos

5.1.1 Operações com inteiros

Definição 5.1.1 (adição de inteiros). *Dados $\overline{(a, b)}$ e $\overline{(c, d)}$ em \mathbb{Z} , define-se adição de inteiros da seguinte forma:*

$$\begin{aligned} (+) : \quad \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ (\overline{(a, b)}; \overline{(c, d)}) &\mapsto \overline{(a, b)} + \overline{(c, d)} := \overline{(a + c, b + d)} \end{aligned}$$

Uma vez que a definição da adição de inteiros envolve classes de equivalência, faz-se necessário verificar que esta não depende dos representantes da classe escolhidos, o qual demonstraremos no teorema 5.1.2 abaixo.

Teorema 5.1.2. *Se $\overline{(a, b)} = \overline{(a', b')}$ e $\overline{(c, d)} = \overline{(c', d')}$ então $\overline{(a, b)} + \overline{(c, d)} = \overline{(a', b')} + \overline{(c', d')}$*

Demonstração. Tem-se, por hipótese, que:

$$(i) \quad a + b' = b + a'$$

$$(ii) \quad c + d' = d + c'$$

Por definição, $\overline{(a, b)} + \overline{(c, d)} := \overline{(a + c, b + d)}$ e $\overline{(a', b')} + \overline{(c', d')} := \overline{(a' + c', b' + d')}$.

Note que, por (i) e (ii) tem-se que $(a + c) + (b' + d') = (b + d) + (a' + c') \Leftrightarrow \overline{(a + c, b + d)} = \overline{(a' + c', b' + d')} \Leftrightarrow \overline{(a, b)} + \overline{(c, d)} = \overline{(a', b')} + \overline{(c', d')}$. \square

Exemplo 5.1.3. Note que, pela definição acima: $\overline{(4, 1)} + \overline{(5, 2)} = \overline{(9, 3)}$. Como $\overline{(6, 3)} = \overline{(4, 1)}$, $\overline{(7, 4)} = \overline{(5, 2)}$ e $\overline{(6, 3)} + \overline{(7, 4)} = \overline{(13, 7)}$. Além disso, $\overline{(13, 7)} = \overline{(9, 3)}$ já que $13 + 3 = 7 + 9$.

Definição 5.1.4 (multiplicação de inteiros). Dados $\overline{(a, b)}$ e $\overline{(c, d)}$ em \mathbb{Z} , define-se multiplicação de inteiros como abaixo:

$$\begin{aligned} (\cdot) : \quad \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z} \\ ((a, b); (c, d)) &\mapsto \overline{(a, b)} \cdot \overline{(c, d)} := \overline{(ac + bd, ad + bc)} \end{aligned}$$

Exemplo 5.1.5. Seguindo a definição de multiplicação de inteiros apresentada acima, tem-se que $\overline{(3, 5)} \cdot \overline{(10, 7)} = \overline{(3 \cdot 10 + 5 \cdot 7, 3 \cdot 7 + 5 \cdot 10)} = \overline{(65, 71)} = 65 - 71 = -6$. Note ainda que $\overline{(3, 5)} \cdot \overline{(10, 7)} = 2 \cdot (-3) = -6$.

5.1.2 Uma motivação para a definição das operações com inteiros

No capítulo 3, mais especificamente na observação 3.2.7 foi exposto que $\overline{(a, b)}$ expressa “essencialmente” $a - b$, ou seja, pode-se dizer que $\overline{(a, b)} = a - b$ e $\overline{(c, d)} = c - d$. Daí, pretendo-se definir:

(a) a adição $\overline{(a, b)} + \overline{(c, d)}$, procedemos como a seguir.

$$\overline{(a, b)} + \overline{(c, d)} = (a + c) - (b + d) = \overline{(a + c, b + d)}.$$

E, portanto, é conveniente definir a adição $\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$.

(b) a multiplicação $\overline{(a, b)} \cdot \overline{(c, d)}$, procedemos como a seguir.

$$\begin{aligned} \overline{(a, b)} \cdot \overline{(c, d)} &= (a - b) \cdot (c - d) \\ &= (a - b) \cdot c - (a - b) \cdot d \\ &= ac - bc - ad + bd \\ &= ac + bd - (ad + bc) \\ &= \overline{(ac + bd, ad + bc)}. \end{aligned}$$

E, portanto, é conveniente definir a multiplicação $\overline{(a, b)} \cdot \overline{(c, d)}$ como sendo $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac + bd, ad + bc)}$.

5.1.3 Operações com racionais

Definição 5.1.6 (adição e multiplicação de racionais). *Sejam $\frac{a}{b}$ e $\frac{c}{d}$ números racionais. Definem-se as operações chamadas de adição e multiplicação, respectivamente, por:*

$$\begin{aligned} (+) : \mathbb{Q} \times \mathbb{Q} &\rightarrow \mathbb{Q} & (\cdot) : \mathbb{Q} \times \mathbb{Q} &\rightarrow \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} & \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} \end{aligned}$$

Observação 5.1.7. *Na multiplicação dos racionais também será utilizado a notação por justaposição, ou seja, $\frac{a}{b} \cdot \frac{c}{d}$ em determinadas oportunidades será denotado por $\frac{a}{b} \frac{c}{d}$.*

Exemplo 5.1.8. *Seguindo a definição de adição e multiplicação de racionais exposta acima, seguem alguns exemplos:*

- $\frac{1}{2} + \frac{4}{2} = \frac{1 \cdot 2 + 2 \cdot 4}{2 \cdot 2} = \frac{2 + 8}{4} = \frac{10}{4}$;
- $\frac{1}{2} + \frac{2}{3} = \frac{1 \cdot 3 + 2 \cdot 2}{2 \cdot 3} = \frac{3 + 4}{6} = \frac{7}{6}$;
- $\frac{14}{22} = \frac{1 \cdot 4}{2 \cdot 2} = \frac{4}{4}$;
- $\frac{12}{23} = \frac{1 \cdot 2}{2 \cdot 3} = \frac{2}{6}$.

A verificação que as operações de adição e multiplicação em \mathbb{Q} estão bem definidas é imediata e, por isso, omitiremos.

5.1.4 Operações com reais

Serão definidas a seguir as operações de adição e multiplicação no conjunto dos números reais.

Definição 5.1.9 (adição de números reais). *Para $\alpha, \beta \in \mathbb{R}$, define-se $\alpha + \beta$ como sendo o corte $\gamma = \{r + s; r \in \alpha \text{ e } s \in \beta\}$, ou seja,*

$$\begin{aligned} (+) : \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R} \\ (\alpha, \beta) &\mapsto \gamma = \alpha + \beta := \{r + s; r \in \alpha \text{ e } s \in \beta\} \end{aligned}$$

Definição 5.1.10 (multiplicação de reais). *Sejam $\alpha, \beta \in \mathbb{R}$, define-se a operação de multiplicação, como sendo o corte $\alpha\beta$, da seguinte forma:*

$$\begin{aligned} (\cdot) : \mathbb{R} \times \mathbb{R} &\rightarrow \mathbb{R} \\ (\alpha, \beta) &\mapsto \alpha\beta \end{aligned}$$

em que, $\alpha\beta := \mathbb{Q}_-^* \cup \{r \in \mathbb{Q}; r = pq \text{ com } p \in \alpha, q \in \beta, p \geq 0 \text{ e } q \geq 0\}$, quando $\alpha, \beta \geq 0^*$

$$\text{ou } \alpha\beta := \begin{cases} -(|\alpha||\beta|), & \text{se } \alpha \leq 0^* \text{ e } \beta \geq 0^* \\ -(|\alpha||\beta|), & \text{se } \alpha \geq 0^* \text{ e } \beta \leq 0^*, \\ |\alpha||\beta|, & \text{se } \alpha < 0^* \text{ e } \beta < 0^* \end{cases} \quad \text{quando } \alpha, \beta \geq 0^*, \text{ sendo}$$

$$|\alpha| := \begin{cases} \alpha, & \text{se } \alpha \geq 0^* \\ -\alpha, & \text{se } \alpha < 0^*. \end{cases}$$

A adição e multiplicação de complexos, quatérnios e octônios já foi apresentada neste trabalho nos capítulos anteriores. A seguir serão apresentadas algumas estruturas algébricas e os conjuntos serão utilizados para exemplificar tais estruturas.

5.2 Relações entre as estruturas algébricas e os conjuntos numéricos

Os conjuntos apresentados nos capítulos 3 e 4 serão os modelos utilizados nesta seção, para exemplificar algumas estruturas algébricas. Os referidos conjuntos serão sempre associados às suas respectivas operações de adição e multiplicação apresentadas na seção 5.1.

5.2.1 Magmas

Definição 5.2.1. *Seja X um conjunto não vazio e $*$ uma operação qualquer que possua X como suporte. Chama-se magma e denota-se por $(X, *)$ o conjunto X munido com esta operação.*

Decorre imediatamente do fato que não há nenhuma característica ou propriedade associada à operação inserida na definição de magma, que todos os conjuntos assinalados na tabela abaixo são exemplos de magma.

operação/conjunto	N	Z	Q	R	C	H	O
adição	x	x	x	x	x	x	x
multiplicação	x	x	x	x	x	x	x

Tabela 5.1: Exemplos de magmas

5.2.2 Semigrupos

Definição 5.2.2. *Uma operação $*$ que tem um conjunto X como suporte é dita associativa quando, para todos $a, b, c \in X$ tem-se $a * (b * c) = (a * b) * c$.*

Proposição 5.2.3. *A adição e a multiplicação de naturais é associativa. Explicitamente,*

(i) *Sejam m, n e p naturais quaisquer, tem-se que $m + (n + p) = (m + n) + p$;*

(ii) Sejam m, n e p naturais arbitrários, tem-se que $m(np) = (mn)p$.

Demonstração.

(i) Sejam m e n dois naturais fixados arbitrariamente e $A_{m,n} = \{p \in \mathbb{N}; m + (n + p) = (m + n) + p\}$, tem-se que $0 \in A_{m,n}$ pois $m + (n + 0) = (m + n) + 0$, pela definição de adição. Supondo que $k \in A_{m,n}$ então $m + (n + k) = (m + n) + k$, como a função s é injetora, tem-se que $s(m + (n + k)) = s((m + n) + k)$. Aplicando a definição de adição:

$$m + (n + s(k)) = m + s(n + k) = s(m + (n + k)) = s((m + n) + k) = (m + n) + s(k)$$

Portanto, $A_{m,n} = \mathbb{N}$. Como m e n foram fixados arbitrariamente, então a propriedade (i) é válida para quaisquer naturais m, n e p .

(ii) Sejam m e n naturais fixados arbitrariamente e $S_{m,n} = \{p \in \mathbb{N}; m(np) = (mn)p\}$. Tem-se que $0 \in S_{m,n}$ pois $m(n \cdot 0) = m \cdot 0 = 0$ e $(mn) \cdot 0 = 0$. Se $k \in S_{m,n}$ então $m \cdot (nk) = (mn) \cdot k$. Dessa forma, $m(n \cdot s(k)) = m \cdot (n \cdot (k + 1)) = m(nk + n) = m \cdot (nk) + mn = (mn)k + mn \cdot 1 = mn(k + 1) = (mn) \cdot s(k)$. Sendo assim, $m(n \cdot s(k)) = (mn) \cdot s(k)$, ou seja, $s(k) \in S_{m,n}$. Consequentemente, através do princípio da indução, $S_{m,n} = \mathbb{N}$ e, como m e n foi fixado arbitrariamente, $m(np) = (mn)p$ é válido para quaisquer m, n e p naturais. \square

Proposição 5.2.4. *A adição e a multiplicação de inteiros é associativa. Explicitamente,*

(i) Dados $\overline{(a, b)}, \overline{(c, d)}$ e $\overline{(e, f)}$ inteiros, tem-se que: $[\overline{(a, b)} + \overline{(c, d)}] + \overline{(e, f)} = \overline{(a, b)} + [\overline{(c, d)} + \overline{(e, f)}]$;

(ii) Sejam $\alpha = \overline{(a, b)}, \beta = \overline{(c, d)}$ e $\gamma = \overline{(e, f)}$ inteiros, tem-se que $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

Demonstração.

(i) De fato, $[\overline{(a, b)} + \overline{(c, d)}] + \overline{(e, f)} = \overline{(a + c, b + d)} + \overline{(e, f)} = \overline{((a + c) + e, (b + d) + f)} = \overline{(a + (c + e), b + (d + f))} = \overline{(a, b)} + [\overline{(c, d)} + \overline{(e, f)}]$;

(ii) Sejam m e n naturais fixados arbitrariamente e $S_{m,n} = \{p \in \mathbb{N}; m(np) = (mn)p\}$. Tem-se que $0 \in S_{m,n}$ pois $m(n \cdot 0) = m \cdot 0 = 0$ e $(mn) \cdot 0 = 0$. Se $k \in S_{m,n}$ então $m \cdot (nk) = (mn) \cdot k$. Dessa forma, $m(n \cdot s(k)) = m \cdot (n \cdot (k + 1)) = m(nk + n) = m \cdot (nk) + mn = (mn)k + mn \cdot 1 = mn(k + 1) = (mn) \cdot s(k)$. Sendo assim, $m(n \cdot s(k)) = (mn) \cdot s(k)$, ou seja, $s(k) \in S_{m,n}$. Consequentemente, através do princípio da indução, $S_{m,n} = \mathbb{N}$ e, como m e n foi fixado arbitrariamente, $m(np) = (mn)p$ é válido para quaisquer m, n e p naturais. \square

Proposição 5.2.5. *A adição e a multiplicação de racionais é associativa. Explicitamente, sejam $r, s, t \in \mathbb{Q}$ com $r = \frac{a}{b}$, $s = \frac{c}{d}$ e $t = \frac{e}{f}$ então,*

$$(i) \quad (r + s) + t = r + (s + t);$$

$$(ii) \quad r(st) = (rs)t.$$

Demonstração.

$$(i) \quad \text{De fato, } (r + s) + t = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \left(\frac{ad + bc}{bd}\right) + \frac{e}{f} = \frac{(ad + bc)f + bde}{bdf} = \frac{adf + bcf + bde}{bdf} = \frac{a}{b} + \left(\frac{cf + de}{df}\right) = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = r + (s + t);$$

$$(ii) \quad \text{De fato, } r(st) = \frac{a}{b} \left(\frac{c}{d} \frac{e}{f}\right) = \frac{a}{b} \frac{ce}{df} = \frac{ace}{bdf} = \left(\frac{ac}{bd}\right) \frac{e}{f} = \left(\frac{a}{b} \frac{c}{d}\right) \frac{e}{f} = (rs)t. \quad \square$$

Proposição 5.2.6. *A adição e a multiplicação de reais é associativa. Explicitamente, sejam $\alpha, \beta, \gamma \in \mathbb{R}$, tem-se que:*

$$(i) \quad (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma);$$

$$(ii) \quad \alpha(\beta\gamma) = (\alpha\beta)\gamma.$$

Demonstração. A demonstração desta proposição pode ser encontrada em [10] (p. 90). □

Proposição 5.2.7. *A adição e a multiplicação de complexos é associativa. Explicitamente, sejam $(a, b), (c, d), (e, f) \in \mathbb{C}$, tem-se que:*

$$(i) \quad (a, b) + [(c, d) + (e, f)] = [(a, b) + (c, d)] + (e, f);$$

$$(ii) \quad (a, b) \cdot [(c, d) \cdot (e, f)] = [(a, b) \cdot (c, d)] \cdot (e, f).$$

Demonstração.

(i) De fato,

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

(ii) De fato,

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

□

A demonstração das proposições 5.2.8 e 5.2.9, a seguir, é análoga à demonstração da proposição 5.2.7, por isso será omitida.

Proposição 5.2.8. *A adição e a multiplicação de quatérnios é associativa. Explicitamente, sejam $a, b, c \in \mathbb{H}$, tem-se que:*

$$(i) \quad (a + b) + c = a + (b + c);$$

$$(ii) \quad (ab)c = a(bc).$$

Proposição 5.2.9. *A adição de octônios é associativa. Explicitamente, sejam $a, b, c \in \mathbb{O}$, tem-se que $(a + b) + c = a + (b + c)$.*

Decorre imediatamente da definição anterior que todo magma associativo é um semigrupo. Note que o magma (\mathbb{O}, \cdot) não é um semigrupo, uma vez que a multiplicação de octônios não é associativa, conforme evidenciado no capítulo 4. Na tabela abaixo todos os conjuntos assinalados são exemplos de semigrupos.

operação/conjunto	\mathbb{N}	\mathbb{Z}	\mathbb{Q}	\mathbb{R}	\mathbb{C}	\mathbb{H}	\mathbb{O}
adição	x	x	x	x	x	x	x
multiplicação	x	x	x	x	x	x	

Tabela 5.2: Exemplos de semigrupos

5.2.3 Monóides

Definição 5.2.10. *Seja $*$ uma operação que tem como suporte X e seja $e \in X$ tal que $x * e = e * x = x$, sendo x um elemento qualquer de X . Diz-se que e é elemento neutro dessa operação.*

Proposição 5.2.11 (elemento neutro nos naturais). *Seja m um natural arbitrário, tem-se que:*

$$(i) \quad m + 0 = 0 + m = m, \text{ isto é, } 0 \text{ é o elemento neutro da adição em } \mathbb{N}.$$

$$(ii) \quad 1 \cdot m = m \cdot 1 = m, \text{ isto é, } 1 \text{ é o elemento neutro multiplicativo em } \mathbb{N}.$$

Demonstração.

$$(i) \quad \text{Por definição } m + 0 = m, \text{ resta mostrar que } 0 + m = m. \text{ Seja } A = \{m \in \mathbb{N}; 0 + m = m\}, \text{ tem-se que:}$$

(a) $0 \in A$, pois $0+0=0$, por definição.

(b) Seja $k \in A$, ou seja, $0 + k = k$, tem-se que $0 + s(k) = s(0 + k) = s(k)$. Sendo assim, $s(k) \in A$.

Dessa forma, através do princípio da indução tem-se que $A = \mathbb{N}$. Assim, $m + 0 = 0 + m = m$ para todo $m \in \mathbb{N}$.

(ii) Note que $m \cdot 1 = m(0 + 1) = m \cdot 0 + m = m$. Sejam m um natural fixado arbitrariamente e $S = \{m \in \mathbb{N}; 1 \cdot m = m\}$ tem-se que $0 \in S$ pois $1 \cdot 0 = 0$ por definição. Se $k \in S$ então $1 \cdot k = k$. Dessa forma, $1 \cdot s(k) = 1(k + 1) = 1 \cdot k + 1 = k + 1 = s(k)$ (na penúltima igualdade foi utilizada a hipótese de indução). Assim, $1 \cdot s(k) = s(k)$, ou seja, $s(k) \in S$. Consequentemente, através do princípio da indução, $S = \mathbb{N}$. E, como m foi fixado arbitrariamente, para qualquer natural m , $1 \cdot m = m \cdot 1 = m$. \square

Proposição 5.2.12 (elemento neutro nos inteiros). *Seja $(\overline{a, b})$ inteiro arbitrário, tem-se que:*

(i) *A adição apresenta elemento neutro $(\overline{0, 0})$.*

(ii) *A multiplicação apresenta $(\overline{1, 0})$ como elemento neutro multiplicativo.*

Demonstração.

(i) De fato, $(\overline{a, b}) + (\overline{0, 0}) = (\overline{a + 0, b + 0}) = (\overline{a, b})$;

(ii) De fato, $(\overline{a, b}) \cdot (\overline{1, 0}) = (\overline{a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1}) = (\overline{a, b})$. \square

Proposição 5.2.13 (elemento neutro nos racionais). *Seja $r \in \mathbb{Q}$, com $r = \frac{a}{b}$, então:*

(i) $\frac{0}{1}$ *é o elemento neutro aditivo;*

(ii) $\frac{1}{1}$ *é o neutro multiplicativo.*

Demonstração.

(i) De fato, $r + \frac{0}{1} = \frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b} = r$;

(ii) De fato, $r \cdot \frac{1}{1} = \frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b} = r$. \square

Proposição 5.2.14 (elemento neutro nos reais). *Seja $\alpha \in \mathbb{R}$, tem-se que:*

(i) 0^* *é o elemento neutro da adição, ou seja, $\alpha + 0^* = \alpha$;*

(ii) 1^* é o elemento neutro da multiplicação, ou seja, $\alpha \cdot 1^* = \alpha$.

Demonstração.

(i) Deseja-se provar que $\alpha + 0^* = \alpha; \forall \alpha \in \mathbb{R}$, ou seja, $\alpha + 0^* \subset \alpha$ e $\alpha \subset \alpha + 0^*$. De fato, seja $r \in \alpha + 0^*$ então $r = p + q; p \in \alpha$ e $q \in 0^*$, ou seja, $q < 0$ e daí $r < p$ e assim $r \in \alpha$. Portanto, $\alpha + 0^* \subset \alpha$. Por outro lado, seja $r \in \alpha$ e $s \in \alpha$ tal que $s > r$ então $r = s + (r - s); r - s < 0$ e assim $r - s \in 0^*$. Conseqüentemente $r = s + (r - s) \in \alpha + 0^*$. Portanto, $\alpha \subset \alpha + 0^*$. Sendo assim, $\alpha + 0^* = \alpha$.

(ii) Seja $r \in \alpha \cdot 1^*$ e $r < 0$. Se $\alpha = 0^*$ tem-se $r \in \alpha$ já que $r < 0 \Rightarrow r \in 0^* = \alpha$.

Seja agora $r \in \alpha \cdot 1^*$ e $r \geq 0$ tem-se que $r = pq; p \in \alpha, q \in 1^*, p \geq 0, q \geq 0$. Como $q \in 1^*$ então $q < 1 \Rightarrow pq < p \cdot 1 \Rightarrow r < p$. Conseqüentemente $r \in \alpha$, já que α é corte. Sendo assim, $\alpha \cdot 1^* \subset \alpha$.

Supondo $r \in \alpha$ e $r < 0$ tem-se que, $r \in \alpha \cdot 1^*$, por definição de produto. Caso $r \in \alpha$ e $r \geq 0$, tem-se que existe $p \in \alpha$ tal que $0 \leq r \leq p$ pois, como α é corte, α não possui elemento máximo. Seja $q = \frac{r}{p}$ então $0 \leq q < 1$ e assim $q \in 1^*$. Dessa forma, $r = pq; p \in \alpha, q \in 1^*, p \geq 0, q \geq 0$, ou seja, $\alpha \subset \alpha \cdot 1^*$.

Assim, $\alpha \cdot 1^* = \alpha$. □

Proposição 5.2.15 (elemento neutro nos complexos). *Seja $(a, b) \in \mathbb{C}$, tem-se que:*

(i) *A adição tem $(0, 0)$ como elemento neutro, ou seja, $(a, b) + (0, 0) = (a, b)$;*

(ii) *A multiplicação tem $(1, 0)$ como elemento neutro, ou seja, $(a, b) \cdot (1, 0) = (a, b)$.*

Demonstração.

(i) De fato, $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$;

(ii) De fato, $(a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a - 0, 0 + b) = (a, b)$. □

Note que os quatérnios apresentam $0 = (0, 0, 0, 0)$ como elemento neutro aditivo e $1 = (1, 0, 0, 0)$ como elemento neutro multiplicativo. De maneira análoga, os octônios apresentam $0 = (0, 0, 0, 0, 0, 0, 0, 0)$ como elemento neutro aditivo e $1 = (1, 0, 0, 0, 0, 0, 0, 0)$ como elemento neutro multiplicativo. A demonstração deste fato é construída de forma análoga ao feito com os complexos, por isso, será omitida.

Definição 5.2.16. *Seja X um conjunto não vazio munido de uma operação binária associativa $*$, ou seja, $x * (y * z) = (x * y) * z$, para todo $x, y, z \in X$. Diremos que X é um monóide, se $*$ tem elemento neutro em X .*

Todos os conjuntos assinalados na tabela abaixo são exemplos de monóide.

operação/conjunto	\mathbb{N}	\mathbb{Z}	\mathbb{Q}	\mathbb{R}	\mathbb{C}	\mathbb{H}	\mathbb{O}
adição	x	x	x	x	x	x	x
multiplicação	x	x	x	x	x	x	

Figura 5.1: Exemplos de monóides

5.2.4 Grupos

Definição 5.2.17. *Considere um conjunto X não vazio, um elemento $x \in X$ e $*$ uma operação que tem X como suporte. Diz-se que x é invertível se, e somente se, existe $y \in X$ tal que $x*y = e$. Neste caso, y é o inverso à direita de x . Caso $y*x = e$ diz-se que y é o inverso à esquerda de x . Em particular, na adição é comum chamar “simétrico” ao inverso aditivo y de $x \in X$ e representar $y = -x$. Já na notação multiplicativa, se y é o inverso de x denota-se $y = x^{-1}$.*

Proposição 5.2.18. *Seja X um semigrupo, se $x \in X$ tem inverso à direita y , e inverso à esquerda z , então $y = z$.*

Demonstração. De fato, por hipótese tem-se que $z * e = z$, $*$ é associativa, ou seja, $z * (x * y) = (z * x) * y$, $x * y = e$ e $z * x = e$. Sendo assim, tem-se que $x * y = e \Rightarrow z * (x * y) = z \Rightarrow (z * x) * y = z \Rightarrow e * y = z \Rightarrow y = z$. \square

Observação 5.2.19. *A partir de agora iremos nos referir ao inverso aditivo como simétrico e ao inverso multiplicativo apenas como inverso.*

Proposição 5.2.20 (elemento simétrico nos inteiros). *Seja $\overline{(a, b)} \in \mathbb{Z}$. Existe um único $\overline{(c, d)} \in \mathbb{Z}$ tal que $\overline{(a, b)} + \overline{(c, d)} = \overline{(0, 0)}$. Neste caso, diz-se que $\overline{(c, d)}$ é o simétrico de $\overline{(a, b)}$ e $\overline{(c, d)} = \overline{(b, a)}$.*

Demonstração. De fato, sendo $\overline{(c, d)} = \overline{(b, a)}$, tem-se que:

$$\begin{aligned}
 \overline{(a, b)} + \overline{(c, d)} &= \overline{(e, f)} \Rightarrow \\
 \overline{(a, b)} + \overline{(b, a)} &= \overline{(e, f)} \Rightarrow \\
 \overline{(a + b, b + a)} &= \overline{(e, f)} \Rightarrow \\
 (a + b) + e &= (b + a) + f \Rightarrow \\
 e + 0 &= f + 0 \Rightarrow \\
 \overline{(e, f)} &= \overline{(0, 0)}.
 \end{aligned}$$

Supondo que, além de $\overline{(c, d)}$, exista $\overline{(c', d')}$ tal que $\overline{(a, b)} + \overline{(c, d)} = \overline{(0, 0)} = \overline{(a, b)} + \overline{(c', d')}$ e que $\overline{(c, d)} \neq \overline{(c', d')}$, tem-se que:

$$\begin{aligned}
\overline{(a, b)} + \overline{(c, d)} &= \overline{(a, b)} + \overline{(c', d')} \Rightarrow \\
\overline{(a + c, b + d)} &= \overline{(a + c', b + d')} \Rightarrow \\
(a + c) + (b + d') &= (b + d) + (a + c') \Rightarrow \\
c + d' &= d + c' \Rightarrow \\
\overline{(c, d)} &= \overline{(c', d')}.
\end{aligned}$$

O que é uma contradição, logo o simétrico de $\overline{(a, b)}$ é $\overline{(b, a)}$ e é único. \square

Proposição 5.2.21 (elementos simétrico e inverso nos racionais). *Seja $r \in \mathbb{Q}$ com $r = \frac{a}{b}$, tem-se que os itens abaixo são verdadeiros.*

- (i) *Todo racional possui simétrico ou oposto, ou seja, existe $r' \in \mathbb{Q}$ com $r' = \frac{-a}{b}$ tal que $r + r' = r' + r = \frac{0}{1}$;*
- (ii) *Todo racional não nulo possui inverso multiplicativo, ou seja, existe $r'' \in \mathbb{Q}$ com $r'' = \frac{b}{a}$ tal que $r \cdot r'' = \frac{1}{1}$.*

Demonstração.

- (i) De fato, existe r' tal que $r + r' = \frac{0}{1}$ e $r' = \frac{-a}{b}$. Note que, $r + r' = \frac{a}{b} + \frac{-a}{b} = \frac{ab + (-ab)}{bb} = \frac{ab - ab}{bb} = \frac{0}{bb} = \frac{0}{1}$. Denota-se o oposto ou simétrico de $r = \frac{a}{b}$ como $-r = \frac{-a}{b}$.

- (ii) De fato, se $r \neq \frac{0}{1}$, existe r'' tal que $r \cdot r'' = \frac{1}{1}$. Seja $r'' = \frac{b}{a}$, note que:

$$r \cdot r'' = \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{a}{a} \frac{b}{b} = \frac{11}{11} = \frac{1}{1}.$$

Denota-se o inverso multiplicativo de $r = \frac{a}{b}$ como $r^{-1} = \frac{b}{a}$. \square

Proposição 5.2.22 (elemento simétrico nos reais). *Seja $\alpha \in \mathbb{R}$ tal que $\alpha + \beta = 0^*$. Como nos inteiros e racionais, β é denotado por $-\alpha$ e é chamado de simétrico, oposto ou inverso aditivo de α .*

Demonstração. A demonstração desta proposição encontra-se em [10], p. 91. \square

Abaixo um caso particular da proposição anterior, para elucidar a ideia de simétrico de um corte.

Exemplo 5.2.23. *Seja $\alpha = 10^*$, o simétrico de α é $-(10)^* = (-10)^*$.*

De fato, tem-se que $10^ = \{x \in \mathbb{Q}; x < 10\}$, $(-10)^* = \{y \in \mathbb{Q}; y < -10\}$ e $10^* + (-10)^* = \{x + y; x \in 10^* \text{ e } y \in (-10)^*\}$. Note que, $10^* + (-10)^* \subset 0^*$. Seja $t \in 10^* + (-10)^*$ então $t = x + y$; $x \in 10^*$ e $y \in (-10)^*$, sendo assim $x < 10$ e $y < -10$. Consequentemente, $x + y < 10 + (-10)$, ou seja, $x + y < 0$ e assim $t = x + y \in 0^*$*

Tem-se ainda que $0^ \subset 10^* + (-10)^*$. Seja $t \in 0^*$ então $t < 0$. Analisando um caso particular, tomando-se $t = -3$, pelo lema anterior existe $x \in 10^*$ e $y \notin 10^*$ com $y \neq 10^*$ tais que $y - x = 3$, ou seja, $-3 = x + (-y)$. Como $y > 10$ então $-y < -10$, ou seja, $-y \in (-10)^*$ e daí $-3 \in 10^* + (-10)^*$.*

Dessa forma, ao generalizar o caso particular citado acima tem-se que $10^ + (-10)^* = 0^*$.*

Definição 5.2.24 (elemento inverso nos reais). *Seja α um corte tal que $\alpha \neq 0^*$. Se $\alpha > 0^*$, então o corte β do teorema anterior é denotado por α^{-1} e chamado de inverso de α . Se $\alpha < 0^*$, então define-se o inverso de α como $-|\alpha|^{-1}$.*

Teorema 5.2.25. *Seja $\alpha \in \mathbb{R}$ tal que $\alpha \neq 0^*$ então $\alpha \cdot \alpha^{-1} = 1^*$. Além disso, o inverso de α é único.*

Demonstração. A demonstração desta proposição pode ser encontrada em [10] (p. 97). □

Proposição 5.2.26 (elementos simétrico e inverso nos complexos). *Sejam $(a, b) \in \mathbb{C}$, tem-se que os itens abaixo são verdadeiros:*

(i) *Todo complexo possui simétrico ou oposto, ou seja, existe $(-a, -b) \in \mathbb{C}$ tal que $(a, b) + (-a, -b) = (0, 0)$;*

(ii) *Todo complexo não nulo possui inverso multiplicativo, em outras palavras, existe $\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) \in \mathbb{C}$ tal que $(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1, 0)$.*

Demonstração.

(i) De fato, $(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0, 0)$;

(ii) De fato, $(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(\frac{a^2}{a^2 + b^2} + \frac{b^2}{a^2 + b^2}, \frac{-ab}{a^2 + b^2} + \frac{ab}{a^2 + b^2}\right) = (1, 0)$. □

Proposição 5.2.27 (elementos simétrico e inverso nos quatérnios). *Sejam $a, b, c \in \mathbb{H}$. As operações em \mathbb{H} têm as seguintes propriedades:*

(i) *O simétrico de a existe e é $-a$;*

(ii) Se $a \neq 0$ então o inverso de a existe e é a^{-1} .

A demonstração do Teorema acima é feita de maneira análoga ao feito com os números complexos.

Definição 5.2.28. Dado um conjunto X não vazio, diremos que $(X, *)$ é um grupo se as seguintes condições são satisfeitas:

- (1) Dados $a, b, c \in X$ então $(a * b) * c = a * (b * c)$ (associatividade);
- (2) Existe elemento $e \in X$ tal que, para todo $a \in X$, $a * e = a = e * a$ (existência do elemento neutro);
- (3) Para todo $a \in X$, existe elemento $a^{-1} \in X$ tal que, $a * a^{-1} = e = a^{-1} * a$ (existência de elemento inverso referente à operação $*$).

Decorre imediatamente da definição acima que um grupo também pode ser caracterizado como um monóide que atende a condição (3) da definição 5.2.28.

Exemplo 5.2.29. Note que os monóides $(\mathbb{N}, +)$ e (\mathbb{N}, \cdot) não são grupos, uma vez que o conjunto dos naturais não apresenta simétrico (elemento inverso aditivo) tampouco inverso (elemento inverso multiplicativo).

Exemplo 5.2.30. O monóide (\mathbb{Z}, \cdot) não é um grupo, pois nem todo inteiro apresenta inverso multiplicativo.

Exemplo 5.2.31. Seja $A = \{-1, 1\}$, (A, \cdot) é um grupo.

Note que os únicos elementos invertíveis de \mathbb{Z} são 1 e -1 e que (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) , (\mathbb{H}, \cdot) não são grupos. Os mesmos serão classificados como grupo quando excludo os seus respectivos elementos neutros aditivos, já que estes elementos não são invertíveis. Dessa forma, a tabela abaixo avalia quais conjuntos associados a operação de adição ou multiplicação são caracterizados como grupo. Para que a mesma fosse mais efetiva, os conjuntos inseridos foram substituídos.

operação/conjunto	\mathbb{N}	\mathbb{Z}	\mathbb{Q}^*	\mathbb{R}^*	\mathbb{C}^*	\mathbb{H}^*	\mathbb{O}^*
adição		x	x	x	x	x	x
multiplicação			x	x	x	x	

Tabela 5.3: Exemplos de grupos

5.2.5 Grupos abelianos

Definição 5.2.32. Uma operação $*$ que tem um conjunto X como suporte é dita comutativa quando $\forall a, b \in X$ tem-se $a * b = b * a$.

Proposição 5.2.33 (comutatividade nos naturais). *Sejam m e n naturais quaisquer, tem-se que:*

- (i) $m + n = n + m$ (propriedade comutativa da adição);
- (ii) $nm = mn$ (propriedade comutativa da multiplicação).

Demonstração.

- (i) Seja m natural fixado arbitrariamente e $A_m = \{n \in \mathbb{N}; m + n = n + m\}$. Tem-se que $0 \in A_m$ pois $m + 0 = 0 + m$. Supondo que $k \in A_m$ então $m + k = k + m$. Dessa forma,

$$m + s(k) = s(m + k) = s(k + m) = (k + m) + 1 = k + (m + 1) = k + (1 + m) = (k + 1) + m = s(k) + m.$$

Assim, $A_m = \mathbb{N}$ e, como m foi fixado arbitrariamente, tem-se que a propriedade i) é válida para quaisquer naturais m e n .

- (ii) Sejam m um natural fixado arbitrariamente e $S_m = \{n \in \mathbb{N}; mn = nm\}$. Tem-se que $0 \in S_m$ pois $m \cdot 0 = 0$ por definição e, tem-se que $0 \cdot m = 0$. Se $k \in S_m$ então $m \cdot k = k \cdot m$. Dessa forma, $m \cdot s(k) = m \cdot (k + 1) = m \cdot k + m = km + 1 \cdot m = (k + 1) \cdot m = s(k) \cdot m$, assim $s(k) \in S_m$. Logo, $S_m = \mathbb{N}$ e, como m foi fixado de forma arbitrária, $mn = nm$ é válido para quaisquer m e n naturais. □

Proposição 5.2.34 (comutatividade nos inteiros). *Sejam $\overline{(a, b)}$ e $\overline{(c, d)}$ inteiros, tem-se que:*

- (i) $\overline{(a, b)} + \overline{(c, d)} = \overline{(c, d)} + \overline{(a, b)}$ (propriedade comutativa da adição);
- (ii) $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(c, d)} \cdot \overline{(a, b)}$ (propriedade comutativa da multiplicação).

Demonstração.

- (i) De fato, $\overline{(a, b)} + \overline{(c, d)} := \overline{(a + c, b + d)} = \overline{(c + a, d + b)} = \overline{(c, d)} + \overline{(a, b)}$;
- (ii) De fato, $\overline{(a, b)} \cdot \overline{(c, d)} := \overline{(ac + bd, ad + bc)} = \overline{(ca + bd, da + cb)} = \overline{(ca + db, cb + da)} = \overline{(c, d)} \cdot \overline{(a, b)}$; □

Proposição 5.2.35 (comutatividade nos racionais). *Sejam $r, s \in \mathbb{Q}$ com $r = \frac{a}{b}$ e $s = \frac{c}{d}$ então:*

(i) $r + s = s + r$ (*propriedade comutativa da adição*);

(ii) $rs = sr$ (*propriedade comutativa da multiplicação*).

Demonstração.

(i) De fato, $r + s = \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b} = s + r$.

(ii) De fato, $rs = \frac{a}{b} \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \frac{a}{b} = sr$. □

Proposição 5.2.36 (comutatividade nos reais). *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$, tem-se que:*

(i) $\alpha + \beta = \beta + \alpha$ (*propriedade comutativa da adição*);

(ii) $\alpha\beta = \beta\alpha$ (*propriedade comutativa da multiplicação*).

Demonstração.

(i) Vamos mostrar que $\alpha + \beta \subset \beta + \alpha$ e $\beta + \alpha \subset \alpha + \beta$. Com efeito, seja $a = r + s \in \alpha + \beta$. Como r e s são racionais, segue que $r + s = s + r$, assim, $a = s + r$. E, portanto, $a \in \beta + \alpha$. De forma análoga, tem-se que $\beta + \alpha \subset \alpha + \beta$. Consequentemente, $\beta + \alpha = \alpha + \beta$, ou seja, a adição de cortes é comutativa.

(ii) Temos dois casos a considerar:

(1) se $r < 0$. Neste caso, pela definição de produto, se $r \in \alpha\beta$, então $r \in \beta\alpha$.

(2) se $r \geq 0$. Neste caso, podemos reescrever $r = pq$, com $p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$, como $r = qp$, com $q \in \beta$, $p \in \alpha$, $q \geq 0$ e $p \geq 0$, desde que p e q são racionais. Logo, $\alpha\beta \subset \beta\alpha$. A inclusão contrária é análoga. □

Proposição 5.2.37 (comutatividade nos complexos). *Sejam $(a, b), (c, d) \in \mathbb{C}$, então:*

(i) $(a, b) + (c, d) = (c, d) + (a, b)$ (*propriedade comutativa da adição*);

(ii) $(a, b) \cdot (c, d) = (c, d) \cdot (a, b)$ (*propriedade comutativa da multiplicação*).

Demonstração.

(i) De fato, $(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)$.

(ii) De fato, $(a, b) \cdot (c, d) = (ac - bd, ad + bc) = (ca - db, cb + da) = (c, d) \cdot (a, b)$. □

Proposição 5.2.38 (comutatividade da adição nos quatérnios e octônios). *Sejam $a, b \in \mathbb{H}$ e $c, d \in \mathbb{O}$*

(i) $a + b = b + a$ (*propriedade comutativa da adição nos quatérnios*);

(ii) $c + d = d + c$ (*propriedade comutativa da adição nos octônios*).

A demonstração da proposição acima segue os mesmos princípios do feito com os números complexos, por isso a mesma foi omitida.

Além disso, como nos quatérnios e octônios tem-se $ij = k$ e $ji = -k$, fica claro que (\mathbb{H}, \cdot) (\mathbb{O}, \cdot) não atendem à propriedade comutativa da multiplicação.

Definição 5.2.39. *Um grupo $(X, *)$ é dito grupo abeliano quando a operação $*$ é comutativa.*

Observação 5.2.40. *Como $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) , (\mathbb{C}, \cdot) , (\mathbb{H}, \cdot) e (\mathbb{O}, \cdot) não se caracterizam como grupos então não cabe avaliá-los como grupo abeliano. Ainda assim, é válido ressaltar que alguns destes possuem a propriedade comutativa em relação a adição e a multiplicação como será evidenciado abaixo.*

As tabelas abaixo evidenciam em quais casos a associação dos conjuntos às respectivas operações caracterizam um grupo abeliano. Ainda assim, vale lembrar que (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) e (\mathbb{C}^*, \cdot) são grupos abelianos, já que neste caso está sendo excluído o elemento nulo de cada um destes conjuntos.

operação/conjunto	\mathbb{N}	\mathbb{Z}	\mathbb{Q}	\mathbb{R}	\mathbb{C}	\mathbb{H}	\mathbb{O}
adição		x	x	x	x	x	x
multiplicação							

Tabela 5.4: Exemplos de grupos abelianos

operação/conjunto	\mathbb{N}	\mathbb{Z}	\mathbb{Q}^*	\mathbb{R}^*	\mathbb{C}^*	\mathbb{H}^*	\mathbb{O}^*
adição		x	x	x	x	x	x
multiplicação			x	x	x		

Tabela 5.5: Exemplos de grupos abelianos

5.2.6 Anéis

Definição 5.2.41. *Sejam $+$ e \cdot operações definidas num conjunto suporte X . Diz-se que \cdot é distributiva em relação à $+$ quando $\forall a, b, c \in X$ tem-se $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Proposição 5.2.42 (distributividade da multiplicação em relação à adição nos naturais). *Sejam m, n e p naturais arbitrários, então $m(n + p) = mn + mp$ e $(m + n)p = mp + np$;*

Demonstração. Sejam m e n naturais fixados arbitrariamente e $S_{m,n} = \{p \in \mathbb{N}; m(n+p) = mn + mp\}$. Tem-se que $0 \in S_{m,n}$ pois $m(n+0) = mn$ e $mn + m \cdot 0 = mn$. Se $k \in S_{m,n}$ então $m(n+k) = mn + mk$. Dessa forma, $m(n + s(k)) = m(n + (k+1)) = m((n+k) + 1) = m(n+k) + m = mn + mk + m = mn + m(k+1) = mn + m \cdot s(k)$. Sendo assim, $m(n+s(k)) = mn + m \cdot s(k)$, ou seja, $s(k) \in S_{m,n}$. Consequentemente, através do princípio da indução, $S_{m,n} = \mathbb{N}$ e, como m e n foram fixados arbitrariamente, $m(n+p) = mn + mp$ é válido para quaisquer m, n e p naturais.

Por outro lado, sejam m e n naturais fixados arbitrariamente e $S_{m,n} = \{p \in \mathbb{N}; (m+n)p = mp + np\}$. Tem-se que $0 \in S_{m,n}$ pois $(m+n) \cdot 0 = 0 = m \cdot 0 + n \cdot 0$. Se $k \in S_{m,n}$ então $(m+n)k = mk + nk$. Dessa forma, $(m+n)s(k) = (m+n) \cdot (k+1) = (m+n) \cdot k + (m+n) = mk + nk + (m+n) = (mk + m) + (nk + n) = m(k+1) + n(k+1) = m \cdot s(k) + n \cdot s(k)$. Sendo assim, $(m+n)s(k) = m \cdot s(k) + n \cdot s(k)$, ou seja, $s(k) \in S_{m,n}$. Consequentemente, $S_{m,n} = \mathbb{N}$ e, como m e n foram fixados arbitrariamente, $(m+n)p = mp + np$ é válido para quaisquer m, n e p naturais. \square

Proposição 5.2.43 (distributividade da multiplicação em relação à adição nos inteiros). *Sejam $\alpha = \overline{(a, b)}$, $\beta = \overline{(c, d)}$ e $\gamma = \overline{(e, f)}$ inteiros. A multiplicação em \mathbb{Z} é distributiva em relação à adição.*

Demonstração. Deseja-se demonstrar que: $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ e $(\beta + \gamma) \cdot \alpha = \beta \cdot \alpha + \gamma \cdot \alpha$. De fato,

(i)

$$\begin{aligned}
 \alpha \cdot (\beta + \gamma) &= \overline{(a, b)} \cdot \overline{(\overline{(c, d)} + \overline{(e, f)})} \\
 &= \overline{(a, b)} \cdot \overline{(c + e, d + f)} \\
 &= \overline{(a \cdot (c + e) + b \cdot (d + f), a(d + f) + b \cdot (c + e))} \\
 &= \overline{(ac + ae + bd + bf, ad + af + bc + be)} \\
 &= \overline{(ac + bd + ae + bf, ad + bc + af + be)} \\
 &= \overline{(ac + bd, ad + bc)} + \overline{(ae + bf, af + be)} \\
 &= \alpha \cdot \beta + \alpha \cdot \gamma
 \end{aligned}$$

(ii)

$$\begin{aligned}
(\beta + \gamma) \cdot \alpha &= \overline{((c, d) + (e, f))} \cdot \overline{(a, b)} \\
&= \overline{(c + e, d + f)} \cdot \overline{(a, b)} \\
&= \overline{((c + e) \cdot a + (d + f) \cdot b, (d + f)a + (c + e)b)} \\
&= \overline{(ca + db + ea + fb, cb + da + eb + fa)} \\
&= \overline{(ca + db, cb + da)} + \overline{(ea + fb, eb + fa)} \\
&= \beta \cdot \alpha + \gamma \cdot \alpha
\end{aligned}$$

□

Proposição 5.2.44 (distributividade da multiplicação em relação à adição nos racionais).
 Sejam $r = \frac{a}{b}$, $s = \frac{c}{d}$ e $t = \frac{e}{f}$ racionais. A multiplicação em \mathbb{Q} é distributiva em relação a adição.

Demonstração. De fato, $r(s+t) = \frac{a}{b} \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} \left(\frac{cf + de}{df} \right) = \frac{a(cf + de)}{bdf} = \frac{acf + ade}{bdf} =$
 $\frac{acf + ade}{bdf} \frac{1}{1} = \frac{acf + ade}{bdf} \frac{b}{b} = \frac{acfb + adeb}{bdfb} = \frac{acbf + bdae}{bdbf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{ac}{bd} + \frac{ae}{bf} =$
 $rs + rt.$

Além disso, $(s + t)r = sr + tr$. A demonstração é análoga. □

Proposição 5.2.45 (distributividade da multiplicação em relação à adição nos reais).
 Sejam $\alpha, \beta, \gamma \in \mathbb{R}$ então $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Demonstração. A demonstração desta proposição pode ser encontrada em [10] (p. 97). □

Proposição 5.2.46 (distributividade da multiplicação em relação à adição nos complexos).
 Sejam $(a, b), (c, d), (e, f) \in \mathbb{C}$. A multiplicação é distributiva em relação a adição, ou seja, $(a, b) \cdot [(c, d) + (e, f)] = (a, b) \cdot (c, d) + (a, b) \cdot (e, f)$.

Demonstração. De fato, $(a, b) \cdot [(c, d) + (e, f)] = (a, b) \cdot (c + e, d + f) = (a(c + e) - b(d + f), a(d + f) + b(c + e)) = (ac + ae - bd - bf, ad + af + bc + be) = (ac - bd + ae - bf, ad + bc + af + be) = (ac - bd, ad + bc) + (ae - bf, af + be) = (a, b) \cdot (c, d) + (a, b) \cdot (e, f). \quad \square$

Observação 5.2.47. Analogamente aos complexos, verifica-se que a distributividade da multiplicação para a adição é válida para os quatérnios e octônios.

Definição 5.2.48. Um anel A é um conjunto não vazio munido de duas operações binárias, denotadas por $+$ (adição) e \cdot (multiplicação) tais que, para todos $a, b, c \in A$ verificam-se as seguintes propriedades:

(i) $(a + b) + c = a + (b + c)$ (associatividade da adição);

- (ii) Existe elemento $0 \in A$ tal que, para todo $a \in A$, $a + 0 = a = 0 + a$ (existência de elemento neutro aditivo);
- (iii) Para todo $a \in A$, existe elemento $-a \in A$ tal que, $a + (-a) = 0 = (-a) + a$ (existência de elemento simétrico aditivo);
- (iv) $a + b = b + a$ (comutatividade da adição);
- (v) $(ab)c = a(bc)$ (associatividade da multiplicação);
- (vi) $(a + b)c = ac + bc$ (distributividade da multiplicação em relação à adição).

Observação 5.2.49. Um anel também pode ser caracterizado como um conjunto A não vazio munido de duas operações binárias, denotadas por $+$ (adição) e \cdot (multiplicação) tais que, $(A, +)$ é um grupo abeliano, (A, \cdot) é um semigrupo e é válida a propriedade (vi).

Definição 5.2.50. Seja A um anel. Diremos que A é um anel com unidade, se existe um elemento $1 \in A$ tal que, para todo $a \in A$, $a \cdot 1 = a = 1 \cdot a$ e, neste caso, diremos que existe um elemento neutro multiplicativo.

Os anéis utilizados neste trabalho são de forma indistinta anéis com unidade, portanto a nomenclatura anel será usada invariavelmente para indicar anéis com unidade. A notação utilizada para um anel A , dotado das operações de $+$ (adição) e \cdot (multiplicação) será $(A, +, \cdot)$.

Definição 5.2.51. Seja A um anel. Dados $a, b, c \in A$, define-se o comutador de a e b por $[a, b] = ab - ba$ e o associador de a e b por $A(a, b, c) = (ab)c - a(bc)$. Diz-se que um anel é comutativo se $[a, b] = 0$ e associativo, caso, $A(a, b, c) = 0$, para todo $a, b, c \in A$.

Observação 5.2.52. Note que todo Anel é Anel associativo.

Exemplos 5.2.53. Tomando como base as definições acima, segue a análise dos “conjuntos clássicos” quanto a caracterização como anel e anel comutativo.

- São anéis: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ e $(\mathbb{H}, +, \cdot)$.
- São anéis comutativos: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.
- Note que o anel das matrizes $(M_n(\mathbb{R}), +, \cdot)$, com $+$ e \cdot , sendo as operações usuais entre matrizes, e o anel dos quatérnios $(\mathbb{H}, +, \cdot)$, sendo $+$ e \cdot as operações entre quatérnios definidas por Hamilton, não são anéis comutativos. É fácil perceber que, dadas duas matrizes A e B , o produto $AB \neq BA$ e já foi mostrado neste trabalho que a multiplicação de quatérnios não é comutativa. Além disso, o anel dos quatérnios é o primeiro exemplo de anel não comutativo.

Observação 5.2.54. *O conjunto dos naturais associado às operações de adição e multiplicação usuais não se caracteriza como anel, uma vez que não atende a propriedade (iii) da definição de anel. Além disso, não é grupo abeliano, tampouco grupo.*

5.2.7 Domínios de Integridade

Definição 5.2.55. *Sejam A um anel comutativo e $a, b \in A$. Se $ab = 0$, implica que $a = 0$ ou $b = 0$, diremos que A é um domínio de integridade, ou simplesmente um domínio.*

Definição 5.2.56. *Sejam $a, b \in A$ com $a, b \neq 0$, tais que $ab = 0$, diz-se que a e b são divisores de 0.*

Dessa forma, pode-se definir domínio de integridade de outra maneira.

Definição 5.2.57. *Um domínio é um anel comutativo sem divisores de zero.*

Exemplo 5.2.58. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são domínio de integridade.

Exemplo 5.2.59. *Note que $(\mathbb{H}, +, \cdot)$ não é domínio de integridade. Apesar de $(\mathbb{H}, +, \cdot)$ ser anel, o mesmo não é anel comutativo.*

5.2.8 Corpos

Definição 5.2.60. *Seja A um anel. Um elemento $a \in A$ é invertível se existe um outro elemento $b \in A$ tal que $ab = 1 = ba$. Neste caso, b é dito inverso de a e usualmente indicado por a^{-1} .*

Observação 5.2.61. *Note que a definição de invertível acima se refere à operação multiplicativa. A análise da existência do elemento inverso quanto à multiplicação já foi feita em 5.2.4, o que facilitará a classificação dos “conjuntos clássicos” quanto à definição de Corpo.*

Definição 5.2.62. *Um anel A é dito de divisão, se todos os seus elementos não-nulos são invertíveis.*

Exemplo 5.2.63. *São anéis de divisão: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ e $(\mathbb{H}, +, \cdot)$.*

Definição 5.2.64. *Um corpo é, por definição, um anel de divisão comutativo.*

Exemplo 5.2.65. *São corpos: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.*

Observação 5.2.66. *O anel de divisão dos quatérnios não é um corpo já que a respectiva multiplicação não é comutativa.*

Proposição 5.2.67. *Todo corpo é domínio de integridade.*

Demonstração. Com efeito, seja R um corpo e $x \neq 0 \in R$. Supondo que $xy = 0$, então $0 = x^{-1} \cdot 0 = x^{-1}xy = y$, analogamente, se $y \neq 0 \in R$, conclui-se que $x = 0$. Assim, R não possui divisores de zero, ou seja, R é domínio de integridade. \square

Entretanto, nem todo domínio de integridade é corpo: basta notar que \mathbb{Z} é um domínio de integridade, mas não é corpo, pois seus únicos elementos inversíveis são 1 e -1 .

5.2.9 Espaço vetorial

Definição 5.2.68. *Seja um conjunto A não vazio. Diremos que A é um espaço vetorial sobre \mathbb{R} se, para todos os elementos $a, b, c \in A$ e $\forall \alpha \in \mathbb{R}$, estão definidas as operações de adição e produto por escalar, satisfazendo as seguintes condições:*

- (1) $a + (b + c) = (a + b) + c$;
- (2) $a + b = b + a$;
- (3) existe $0 \in A$ tal que $a + 0 = 0 + a = a$;
- (4) existe $(-a) \in A$ tal que $a + (-a) = 0$;
- (5) $\alpha(\beta a) = (\alpha\beta)a$;
- (6) $(\alpha + \beta)a = \alpha a + \beta a$;
- (7) $\alpha(a + b) = \alpha a + \alpha b$;
- (8) $\exists 1 \in K$ tal que $1 \cdot a = a$.

Exemplo 5.2.69. \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{H} e \mathbb{O} são espaços vetoriais sobre o corpo \mathbb{R} .

5.2.10 Álgebra

Neste ponto é conveniente introduzir a definição de álgebra (associativa) sobre um corpo, ao qual neste trabalho, iremos considerar, por conveniência como o corpo dos números reais. De maneira mais específica iremos tratar de álgebras de dimensão finita.

Definição 5.2.70. *Sejam \mathbb{R} o corpo dos números reais e A um conjunto não-vazio. Diz-se que A é uma \mathbb{R} -álgebra (álgebra sobre o corpo \mathbb{R}), se em A estiverem definidas as operações de adição e o produto por escalar:*

$$\begin{aligned} A \times A &\rightarrow A & \mathbb{R} \times A &\rightarrow A \\ (a, b) &\mapsto a + b & (\alpha, a) &\mapsto \alpha a \end{aligned}$$

de tal modo que A seja um espaço vetorial sobre o corpo \mathbb{R} . Além disso, que a operação de multiplicação:

$$\begin{aligned} A \times A &\rightarrow A \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

satisfaça as seguintes condições:

- (i) $\alpha(ab) = (\alpha a)b = a(\alpha b)$;
- (ii) $(a + \alpha b)c = ac + \alpha bc$ e $a(b + \alpha c) = ab + \alpha(ac)$,

todas as condições acima, valendo para todos $a, b, c \in A$ e $\alpha \in \mathbb{R}$.

Definição 5.2.71. *Sejam $a, b, c \in A$ e a \mathbb{R} -álgebra definida acima. Diz-se que:*

- Uma \mathbb{R} -álgebra é comutativa se $[a, b] = 0$;
- Uma \mathbb{R} -álgebra é associativa se $A(a, b, c) = 0$;
- Uma \mathbb{R} -álgebra é álgebra com unidade, se existe $e \in A$ tal que $ae = ea = a$.
- Uma \mathbb{R} -álgebra é álgebra alternativa, se $A(a, a, b) = A(a, b, b) = 0$, ou seja, $a(ab) = a^2b$ e $(ba)a = ba^2$.

Decorre imediatamente que se A é uma \mathbb{R} -álgebra associativa, então A é também \mathbb{R} -álgebra alternativa.

Exemplo 5.2.72. *Note que $M_2(\mathbb{R})$ é uma \mathbb{R} -álgebra sendo as operações: a multiplicação por escalar, a soma de matrizes e a multiplicação de matrizes. $M_2(\mathbb{R})$ é uma álgebra associativa e com unidade.*

Definição 5.2.73. *Seja A uma \mathbb{R} -álgebra, com unidade denotada por e . Dado $x \in A$, se existe $y \in A$ tal que $xy = yx = e$, diz-se que y é o elemento inverso de x , sendo que y é único e denotado por x^{-1} .*

Definição 5.2.74. *Seja A uma \mathbb{R} -álgebra com unidade. Diremos que A é uma álgebra de divisão¹, se todo elemento $x \neq 0$ de A possuir um elemento inverso.*

Exemplo 5.2.75. *Seguem alguns exemplos de álgebras de divisão:*

- O conjunto dos números reais (\mathbb{R}) é uma \mathbb{R} -álgebra de divisão comutativa com a adição, multiplicação e produto por escalar usuais dos números reais;

¹O primeiro exemplo conhecido de álgebra de divisão são os números reais. Somente, por volta de 1572, o matemático italiano *Rafael Bombelli* formalizou a aritmética dos números complexos dando-lhes também a estrutura de álgebra de divisão e os utilizou em seu livro *L'Algebra* para resolver equações.

- O conjunto dos números complexos (\mathbb{C}) é uma \mathbb{R} -álgebra de divisão comutativa com a adição, multiplicação e produto por escalar usuais dos números complexos;
- O conjunto dos quatérnios (\mathbb{H}) é uma \mathbb{R} -álgebra de divisão não-comutativa com a adição, multiplicação e produto por escalar dos números quatérnios;
- O conjunto dos octônios (\mathbb{O}) é uma \mathbb{R} -álgebra de divisão não-comutativa e não associativa com a adição, multiplicação e produto por escalar dos octônios.

Observação 5.2.76. O conceito de dimensão de uma \mathbb{R} -álgebra é análogo ao conceito de dimensão visto em álgebra linear para o caso de um espaço vetorial, uma vez que \mathbb{R} -álgebra é, de fato, um espaço vetorial sobre o conjunto dos números reais. Para detalhes veja, por exemplo, [9]. Nosso interesse é por \mathbb{R} -álgebra de dimensão finita.

Abaixo a definição de isomorfismo \mathbb{R} -álgebras.

Definição 5.2.77. Sejam A e A' duas \mathbb{R} -álgebras. Diz-se que A e A' são isomorfas ou equivalentes quando existe uma correspondência biunívoca $a \rightarrow a'$ entre A e A' de forma que,

$$\begin{aligned}(a + b)' &= a' + b' \\ (\alpha a)' &= \alpha a' \\ (ab)' &= a'b',\end{aligned}$$

em que $a, b \in A$, $a', b' \in A'$ e $\alpha \in \mathbb{R}$.

Capítulo 6

A questão proposta por Hamilton

6.1 A questão proposta por Hamilton: Quais esferas são paralelizáveis?

Para respondermos a questão 1 introduziremos algumas ferramentas geométricas. Aqui ressaltamos que, para além de responder a questão proposta pelo Hamilton, esta breve discussão estabelecerá relações entre a estrutura algébrica dos conjuntos e sua geometria, a partir do conceito de paralelizável, no caso de esferas n -dimensionais.

Antes de definir esferas paralelizáveis, lembremos o conceito de uma esfera n -dimensional no espaço euclidiano \mathbb{R}^n .

Definição 6.1.1. *Seja $n > -1$ e seja $\| - \|$ a norma euclidiana sobre \mathbb{R}^n . A n -esfera é o sub-espaço topológico $S^n := \{a \in \mathbb{R}^{n+1}; \|a\| = 1\} \subset \mathbb{R}^{n+1}$.*

Definição 6.1.2. *A esfera n -dimensional S^n é, por definição, o seguinte subconjunto $S^n = \{x \in \mathbb{R}^{n+1}; \|x\| = 1\}$.*

Exemplo 6.1.3. *A esfera $S^1 = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 = 1\}$ e a esfera $S^2 = \{(x, y, z) \in \mathbb{R}^3; x^2 + y^2 + z^2 = 1\}$.*

O conceito de paralelizável, a seguir, é relevante para a existência de álgebras de divisão, conforme estabelece a proposição 6.1.5, a qual apresentamos sem demonstração. Para maiores detalhes, sobre esta discussão, veja, por exemplo, [13, 3, 14, 9].

Definição 6.1.4. *A n -esfera é dita ser paralelizável, se existem $n+1$ aplicações contínuas $\phi_0, \phi_1, \dots, \phi_n : S^n \rightarrow S^n$, com $\phi_0 = Id_{S^n}$ e tal que para todo $a \in S^n$, as imagens $\phi_0(a), \phi_1(a), \dots, \phi_n(a)$ são linearmente independentes em \mathbb{R}^{n+1} .*

Proposição 6.1.5. *Suponha que para todo $n \geq 0$, existe uma n -dimensional A -álgebra de divisão sobre \mathbb{R} , então a $(n-1)$ -esfera é paralelizável.*

Assim, de acordo com a proposição 6.1.5, para mostrarmos que não existe uma álgebra de divisão sobre \mathbb{R} de dimensão 3 é suficiente mostrarmos que a 2-esfera não é paralelizável. No entanto, é possível mostrar um resultado mais geral, como a seguir.

Proposição 6.1.6. *Seja $n \in \mathbb{N}$ par. Então a n -esfera não é paralelizável.*

Para provar o resultado anterior, precisamos das seguintes definições.

Definição 6.1.7. *Sejam S^n uma n -esfera e as funções contínuas $f, g : S^n \rightarrow S^n$. Diremos que f é **homotópica a g** e escrevemos $f \simeq g$ se existe uma função contínua*

$$F : \begin{cases} S^n \times I & \rightarrow S^n \\ (x, t) & \mapsto F(x, t) \end{cases}$$

tal que:

$$(a) \quad F(x, 0) = f(x);$$

$$(b) \quad F(x, 1) = g(x), \quad \forall x \in S^n,$$

em que $I = [0, 1]$.

Proposição 6.1.8. *Sejam $f, g : S^n \rightarrow S^n$ contínuas tal que $f(x) \neq -g(x)$, $\forall x \in S^n$, então f é homotópica a g .*

Demonstração. Se $f(x) \neq -g(x)$, $\forall x \in S^n$ (hipótese), então o segmento de reta

$$tf(x) + (1-t)g(x), \quad 0 \leq t \leq 1,$$

não passa pela origem de \mathbb{R}^{n+1} . Assim, podemos considerar a aplicação

$$F : S^n \times I \rightarrow S^n \subset \mathbb{R}^{n+1} \\ (x, t) \mapsto F(x, t) := \frac{tf(x) + (1-t)g(x)}{|tf(x) + (1-t)g(x)|}$$

Note que F está bem definida, desde que $tf(x) + (1-t)g(x) \neq 0$ e é contínua, pois f, g são contínuas (hipótese). Além disso,

$$F(x, 0) = \frac{g(x)}{|g(x)|} = g(x), \quad \text{pois } |g(x)| = 1, \quad \text{pois } g : S^n \rightarrow S^n$$

e

$$F(x, 1) = \frac{f(x)}{|f(x)|} = f(x), \quad \text{pois } |f(x)| = 1, \quad \text{pois } f : S^n \rightarrow S^n$$

Portanto, $f \simeq g$, como queríamos mostrar. □

Decorre imediatamente proposição anterior o seguinte resultado.

Lema 6.1.9. *Seja $f : S^n \rightarrow S^n$ uma aplicação contínua, $n \geq 1$.*

(a) *Se $f(x) \neq -x$, então $f \simeq Id_{S^n}$ ($Id_{S^n}(x) = x$ é a função identidade).*

(b) *Se $f(x) \neq x$, então $f \simeq -Id_{S^n}$ ($-Id_{S^n}(x)$ é chamada aplicação antipodal).*

Para completarmos os ingredientes necessários para a demonstração da proposição 6.1.6, vamos assumir a existência de uma função φ_* que cumpre as seguintes propriedades.

Observação 6.1.10. *Sejam $n \geq 1$ e $f, g : S^n \rightarrow S^n$ aplicações contínuas. É possível mostrar que existe uma função φ_* , satisfazendo as seguintes propriedades.*

(a) $\varphi_*(Id_{S^n}) = 1$;

(b) $\varphi_*(Id_{S^n}) = (-1)^{n+1}$.

Para detalhes sobre a função φ_* e suas propriedades, consulte por exemplo, [14], no tópico sobre grau de Browner de uma aplicação.

Agora, podemos provar a proposição 6.1.6.

Demonstração. [da proposição 6.1.6]. Suponhamos que uma n -esfera seja paralelizável. Então, existe uma aplicação $\phi : S^n \rightarrow S^n$ tal que para todo $a \in S^n$, os vetores a e $\phi(a)$ são linearmente independentes, o que é equivalente a afirmar que $\phi(a) \neq a$ e $\phi(a) \neq -a$. Daí, de acordo com o lema 6.1.9, temos que $\phi \simeq Id_{S^n}$ e $\phi \simeq -Id_{S^n}$, e, portanto, pela observação 6.1.10, segue que

$$1 = \varphi_*(Id_{S^n}) = \varphi_*(-Id_{S^n}) = (-1)^{n+1},$$

o que para n par não é verdadeiro. O que completa a prova da proposição 6.1.6. \square

Face ao exposto já é possível provar o seguinte resultado.

Teorema 6.1.11. *Não existe álgebra de divisão sobre \mathbb{R} de dimensão ímpar maior do que 1. Em particular, não existe uma álgebra de divisão sobre \mathbb{R} de dimensão 3.*

Demonstração. Para $n \geq 1$, decorre da proposição anterior que, sendo n um número par, então a n -esfera não é paralelizável. Sendo assim, o resultado segue da proposição 6.1.5. \square

6.2 A questão proposta por Hamilton: Quais esferas são grupos?

Nesta seção discutiremos uma outra abordagem para solucionar a questão 1. De fato, veremos que esta questão surge, naturalmente, na discussão sobre quais esferas n -dimensionais são grupos (questão 5, abaixo). Para detalhes sobre as demonstrações dos resultados e sobre as demais discussões desta seção, veja, por exemplo, [3, 9, 13].

Para introduzir a discussão lembre-se que a esfera $S^n := \{a \in \mathbb{R}^{n+1} : \|a\| = 1\} \subset \mathbb{R}^{n+1}$. Temos que para $n = 0$, a esfera $S^0 = \{-1, 1\} \subset \mathbb{R}$. Ademais, usando o isomorfismo existente entre \mathbb{R}^2 e \mathbb{C} , podemos escrever a esfera S^1 como o subconjunto $S^1 = \{e^{i\theta}, \theta \in [0, 2\pi)\}$ de \mathbb{C} . Observemos que tanto S^0 quanto S^1 são grupos, com respeito à operação de multiplicação. A partir desta discussão, cabe a seguinte pergunta:

Questão 5. *A n -esfera S^n é um grupo, para qualquer $n \in \mathbb{N}$? Se não, quais esferas são grupos?*

Antes de responder a questão acima, observe o seguinte.

- (a) A esfera S^0 é um subconjunto de \mathbb{R} cujos elementos têm norma unitária. Além disso, para qualquer $t, s \in \mathbb{R}$, temos que $\|ts\| = \|t\|\|s\|$.
- (b) A esfera S^1 é um subconjunto de \mathbb{C} cujos elementos têm norma unitária. Além disso, para quaisquer $z, w \in \mathbb{C}$, temos que $\|zw\| = \|z\|\|w\|$.

A discussão acima, motiva a seguinte definição.

Definição 6.2.1. *(álgebra de divisão normada) O conjunto A é uma álgebra real de divisão normada de dimensão n , se A satisfaz as seguintes condições:*

- (a) *A é um espaço vetorial de dimensão n , com uma norma: $\|\cdot\|$.*
- (b) *A tem uma estrutura de anel com identidade, e qualquer elemento não-nulo é invertível.*
- (c) *A norma e a multiplicação são compatíveis, no seguinte sentido:*

$$\|ab\| = \|a\|\|b\|, \quad \forall a, b \in A.$$

Decorre imediatamente da definição que toda álgebra de divisão normada é uma álgebra de divisão. Além disso, sendo $A = \mathbb{R}$, temos que $S_{\mathbb{R}} = S^0$, e sendo, $A = \mathbb{C}$, temos que $S_{\mathbb{C}} = S^1$, são grupos, com já vimos. Sendo $A = \mathbb{H}$, é possível mostrar que a esfera unitária $S_{\mathbb{H}} = S^3$ é também um grupo.

De modo geral, é possível mostrar o seguinte resultado, o qual responde a questão 1.

“Quando A é uma álgebra associativa, a esfera unitária $S_n = \{a \in S^n; |a| = 1\}$ é uma $(n - 1)$ esfera que também é um grupo.”

De fato, vale também a recíproca, ou seja, se S^{n-1} é um grupo, então esta induz uma estrutura de uma álgebra real de divisão associativa normada em \mathbb{R}^n . Portanto, se S^2 é um grupo, então deve existir uma estrutura de álgebra real de divisão normada associativa em \mathbb{R}^3 . Mas, é possível mostrar que não existe uma tal estrutura, logo S^2 não pode ser um grupo.

A partir destas discussões recuperamos de um outro ponto de vista, ou melhor, de um outro ponto de partida, uma resposta para o questionamento do Hamilton (questão 1), uma vez que S^2 não sendo um grupo, implica, em particular, a não existência de uma estrutura de álgebra real de divisão associativa em \mathbb{R}^3 . Mais ainda, as únicas esferas que são grupos são S^0 , S^1 e S^3 .

6.3 O Teorema de Frobenius para \mathbb{R} -álgebras de divisão associativas de dimensão finita

Nesta seção, uma classificação das \mathbb{R} -álgebras de divisão, associativas e de dimensão finita (teorema 6.3.8) é apresentada. A principal referência utilizada foi [24]. Outros detalhes também podem ser vistos em [9, 13, 14, 17, 30].

Antes, porém, serão necessárias algumas definições e resultados que apresentaremos a seguir.

Proposição 6.3.1. *Seja A uma álgebra de divisão associativa de dimensão finita sobre o corpo \mathbb{R} . Se $x \in A$, então $x^2 \in \mathbb{R} + \mathbb{R}x$.*

Demonstração. O conjunto de potências $1, x, x^2, \dots$ de um elemento $x \in A$ é linearmente dependente. Então, existem a_0, \dots, a_m não todos nulos, tais que $p(x) = a_0 + \dots + a_m x^m = 0$. Como todo polinômio em $\mathbb{R}[X]$ pode se fatorado com fatores de grau no máximo 2, segue que $p(x) = b_0(x - b_1) \cdots (x - b_k) \cdots (x^2 + c_1x + d_1)$. Como A não possui divisores de zero, existe um certo índice, digamos k , tal que $x - b_k = 0$ ou $x^2 + c_kx + d_k = 0$, logo, $x^2 \in \mathbb{R} + \mathbb{R}x$. \square

Proposição 6.3.2. *Se $A \neq \mathbb{R}$, então:*

- (a) *Existe um elemento $i \in A$ tal que $i^2 = -1$.*
- (b) *$C = \mathbb{R} + \mathbb{R}i$ é um corpo isomorfo ao conjunto dos números complexos e $C := \{x \in A : xi = ix\}$.*

Demonstração. Inicialmente, observe que se $A \neq \mathbb{R}$, então, existe um elemento $x \in A$, tal que $x \notin \mathbb{R}$. Pela proposição 6.3.1, vale que $x^2 \in \mathbb{R} + \mathbb{R}x$, ou seja, existem a e b em \mathbb{R} , tal que $x^2 = ax + b$, equivalentemente,

$$x^2 - ax = b \Leftrightarrow \left(x - \frac{a}{2}\right)^2 = b + \frac{a^2}{4}. \quad (6.1)$$

Afirmção 6.3.3. *Se $b - \frac{a^2}{4} \geq 0$, então $x \in \mathbb{R}$.*

Demonstração. De fato, da equação 6.1 e da hipótese, segue que

$$\left(x - \frac{a}{2}\right)^2 - \left(b + \frac{a^2}{4}\right) = 0 \quad (6.2)$$

Reescrevendo $\left(b + \frac{a^2}{4}\right) = \left((b + \frac{a^2}{4})^{\frac{1}{2}}\right)^2$. A equação 6.2 pode ser reescrita da seguinte forma:

$$\left(x - \frac{a}{2}\right)^2 - \left((b + \frac{a^2}{4})^{\frac{1}{2}}\right)^2 = 0 \quad (6.3)$$

E, portanto,

$$x = \pm \sqrt{\left((b + \frac{a^2}{4})^{\frac{1}{2}}\right)^2} + \frac{a}{2}.$$

Logo, $x \in \mathbb{R}$, desde que $a, b \in \mathbb{R}$ e $b + \frac{a^2}{4} \geq 0$, o que conclui a prova da afirmação 6.3.3. \square

Decorre da afirmação 6.3.3 que se $x \notin \mathbb{R}$, então $b + \frac{a^2}{4} < 0$ e, portanto, existe um $c \in \mathbb{R}$ tal que $c > 0$ de tal sorte que podemos escrever $b + \frac{a^2}{4} = -c^2$.

Demonstração. (Prova do item [(a)]). De fato, do exposto acima, se x é um elemento de A , tal que $x \notin \mathbb{R}$, então, existem a e b em \mathbb{R} , tal que

$$\left(x - \frac{a}{2}\right)^2 = -c^2, \quad (6.4)$$

o que implica que

$$\frac{\left(x - \frac{a}{2}\right)^2}{c^2} = -1. \quad (6.5)$$

Faça $i^2 = -1$. Assim, temos que

$$\frac{\left(x - \frac{a}{2}\right)^2}{c^2} = i^2. \quad (6.6)$$

Agora, note que, $\frac{\left(x - \frac{a}{2}\right)^2}{c^2} \in \mathbb{R}$, desde que $\left(x - \frac{a}{2}\right)^2 = b + \frac{a^2}{4} \in \mathbb{R}$, pois $a, b, c \in \mathbb{R}$. E, portanto, para concluir a prova do item [(a)], basta tomar $i = \frac{2x - a}{2c}$, na equação 6.6. \square

Demonstração. (Prova do item [(b)]). Vamos mostrar que $x \in \mathbb{R} + \mathbb{R}i$. De fato, usando o fato que x é um elemento qualquer de A que comuta com o elemento i e que $i^2 = -1$, podemos escrever:

$$\begin{aligned} \left(x - \frac{a}{2}\right)^2 &= -c^2 \\ &= i^2 c^2 \\ &= i^2 c^2 \\ &= (ic)^2 \end{aligned}$$

Donde segue que

$$\begin{aligned} 0 &= \left(x - \frac{a}{2}\right)^2 - (ic)^2 \\ &= \left(x - \frac{a}{2} + ic\right) \left(x - \frac{a}{2} - ic\right) \end{aligned}$$

E, portanto, $\left(x - \frac{a}{2} + ic\right) = 0$ ou $\left(x - \frac{a}{2} - ic\right) = 0$. Ou seja, $x = \frac{a}{2} - ic \in \mathbb{R} + \mathbb{R}i$ ou $x = \frac{a}{2} + ic \in \mathbb{R} + \mathbb{R}i$, como queríamos mostrar. \square

Claramente, $C = \mathbb{R} + \mathbb{R}i$ é um corpo. O que conclui a prova da proposição 6.3.2. \square

Proposição 6.3.4. *Seja $C^- := \{x \in A; xi = -ix\}$, então C^- é um subespaço vetorial de A tal que $C \cap C^- = \{0\}$ e $A = C \oplus C^-$.*

Demonstração. Note que $0 \in C^-$. Além disso, se $x, y \in C^-$ e $a, b \in \mathbb{R}$, então $(ax + by)i = axi + byi = -aix - biy = -i(ax + by)$. E, portanto, $ax + by \in C^-$. Se $x \in C \cap C^-$, segue que $ix = xi = -ix$, o que implica que $(x = 0$ ou $1 = -1) \Rightarrow x = 0$. Para mostrarmos que $A = C + C^-$, inicialmente, mostremos a seguinte afirmação.

Afirmção 6.3.5. $\frac{1}{2}(x - ixi) \in C$ e $\frac{1}{2}(x + ixi) \in C^-$.

Demonstração. (Prova da afirmação) De fato, decorre da comutatividade e da associatividade em A , que:

$$\begin{aligned} (x - ixi)i &= xi - (ixi)i \\ &= -(i^2)(xi) - [(ix)i]i \\ &= -i[i(xi)] - (ix)(i^2) \\ &= -i(ixi) + ix \\ &= i(x - ixi) \end{aligned}$$

e

$$\begin{aligned}
 (x + ixi)i &= xi + (ixi)i \\
 &= -(i^2)(xi) + [(ix)i]i \\
 &= -i[i(xi)] + (ix)(i^2) \\
 &= -i(ixi) - ix \\
 &= -i(x + ixi)
 \end{aligned}$$

Logo, $\frac{1}{2}(x - ixi) \in C$ e $\frac{1}{2}(x + ixi) \in C^-$. □

Como $x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi)$, segue que $A = C + C^-$, como queríamos mostrar. □

Proposição 6.3.6. *Se $x, u \in A$ anticomutam, então x^2 e u comutam.*

Demonstração. Decorre da comutatividade e da associatividade em A . □

A demonstração do próximo resultado segue a mesma ideia da proposição 6.3.4, por isso, omitiremos esta demonstração. O leitor interessado poderá consultar, por exemplo, [24].

Proposição 6.3.7. *Se $A \not\subseteq C$, então:*

- (a) *Existe $j \in C^-$ tal que $j^2 = -1$.*
- (b) *O subespaço 4-dimensional $C + Cj$ é uma álgebra de divisão associativa sobre \mathbb{R} isomorfa aos quatérnios de Hamilton.*

Com isto, prova-se o Teorema de Frobenius:

Teorema 6.3.8 (Teorema de Frobenius). *Se A é uma \mathbb{R} -álgebra de divisão associativa, com dimensão finita, então A é isomorfa a \mathbb{R} , ou a \mathbb{C} , ou a \mathbb{H} .*

Uma continuação natural do Teorema de Frobenius consiste em enfraquecer a hipótese da associatividade, por exemplo, substituindo-a pela condição de que a álgebra de divisão é alternativa, a qual é condição necessária para a associatividade. Nesta direção, temos o Teorema de Hurwitz (Ver, por exemplo, [24]), o qual garante que, a menos de isomorfismo, existem apenas as seguintes \mathbb{R} -álgebras de divisão alternativas: \mathbb{R} , \mathbb{C} , \mathbb{H} ou \mathbb{O} . Note que os octônios tem dimensão 8 é não-associativo e é não-comutativo.

Face ao exposto questiona-se, imediatamente, se extensões em dimensões mais altas existem? De fato, é possível mostrar que, preservando a estrutura de álgebra de divisão, estes são as únicas possibilidades, conforme provado em [3].

Finalmente, espera-se que este trabalho tenha evidenciado a riqueza de abordagens e técnicas presentes nas discussões em torno do conhecido Teorema de Frobenius.

Apêndice A

<p>Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)</p> <p>O presente instrumento objetiva consubstanciar dados para o desenvolvimento da pesquisa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade Federal do Recôncavo da Bahia (UFRB).</p> <p>Na primeira parte, solicitamos alguns dados de identificação com o intuito de classificar os grupos pesquisados. Na segunda parte, apresentamos questões específicas, visando melhor compressão do objeto da pesquisa.</p> <p>Apesar de solicitar a identificação no presente formulário, a mesma não será divulgada dentro da pesquisa, sendo meramente elemento prático para a distinção na análise dos dados. A pesquisa terá caráter confidencial no que diz respeito às informações apresentadas no presente instrumento.</p> <p>Sua colaboração é de fundamental importância. Antecipo meus agradecimentos pela sua valorosa colaboração.</p> <p style="text-align: right;">José Carlos Leal do Valle Júnior Estudante de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)</p>	
---	--

PRIMEIRA PARTE <i>(DADOS DE IDENTIFICAÇÃO)</i>
Nome:
Idade:
Instituição de Ensino:
Série/Ano:

Figura 6.1: Questionário aplicado aos alunos - p.1

SEGUNDA PARTE
(QUESTÕES ESPECÍFICAS)

1) Sendo $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e \mathbb{C} os conjuntos dos naturais, inteiros, racionais, reais e complexos, respectivamente. Supondo que as caixas abaixo representam tais conjuntos e que os seus elementos devem estar inseridos nas mesmas, direcione os elementos abaixo, posicionando-os na(s) caixa(s) corretas.

0	1	$1 + i$	$\frac{2}{1}$	$\frac{3}{4}$	i	1000	0,353535...	π	-2
---	---	---------	---------------	---------------	-----	------	-------------	-------	----

N

Z

Q

R

C

2) Resumidamente, as equações visam determinar através de processos matemáticos, determinados valores desconhecidos. Através dos seus conhecimentos matemáticos responda os itens abaixo sobre a equação:
$$x^2 + 1 = 0$$

a) Resolva a equação acima descrevendo abaixo o método utilizado para tal.

b) Assinale abaixo as caixas que contém a solução da equação acima.

N

Z

Q

R

C

3) Quando um conjunto A possui todos os elementos de outro conjunto, por exemplo, B, dizemos que o conjunto A contém o conjunto B; ou que o conjunto B está contido no conjunto A. Denota-se este fato como $A \supset B$ (A contém B) ou $B \subset A$ (B está contido em A). Tomando como base a notação apresentada acima, complete os espaços vazios com as respectivas inclusões entre os conjuntos numéricos.

N ___ Z	Q ___ Z	Z ___ Q	R ___ Q	R ___ C
---------	---------	---------	---------	---------

Figura 6.2: Questionário aplicado aos alunos - p.2

<p>Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)</p> 
<p>O presente instrumento objetiva consubstanciar dados para o desenvolvimento da pesquisa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade Federal do Recôncavo da Bahia (UFRB).</p> <p>Na primeira parte, solicitamos alguns dados de identificação com o intuito de classificar os grupos pesquisados. Na segunda parte, apresentamos questões específicas, visando melhor compressão do objeto da pesquisa.</p> <p>Apesar de solicitar a identificação no presente formulário, a mesma não será divulgada dentro da pesquisa, sendo meramente elemento prático para a distinção na análise dos dados. A pesquisa terá caráter confidencial no que diz respeito às informações apresentadas no presente instrumento.</p> <p>Sua colaboração é de fundamental importância. Antecipo meus agradecimentos pela sua valorosa colaboração.</p> <p style="text-align: right;">José Carlos Leal do Valle Júnior Estudante de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)</p>

<p>PRIMEIRA PARTE (DADOS DE IDENTIFICAÇÃO)</p>
<p>Nome: _____</p>
<p>Idade: _____</p>
<p>Instituição de Ensino: _____</p>
<p>Formação:</p> <p>(1) _____</p> <p>(2) _____</p> <p>(3) _____</p> <p>(4) _____</p>

Figura 6.3: Questionário aplicado aos professores - p.1

SEGUNDA PARTE <i>(QUESTÕES ESPECÍFICAS)</i>	
<p>1) Nas suas experiências como docente de matemática, os alunos apresentam motivação para o estudo dos números complexos?</p> <p>a) Sim b) Não c) Raramente</p>	
<p>2) Os alunos conseguem identificar alguma aplicação dos números complexos associada à realidade?</p> <p>a) Sim b) Não c) Raramente</p> <p>Se sim, qual (is)?</p> <p>_____</p> <p>_____</p> <p>_____</p>	
<p>3) Sendo $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e \mathbb{C} os conjuntos dos naturais, inteiros, racionais, reais e complexos, respectivamente e motivado pela sucessão de inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, você acredita que existe um conjunto X tal que $\mathbb{C} \subset X$?</p> <p>a) Sim b) Não</p>	
<p>4) Caso tenha respondido sim na questão anterior, você acredita que existe um conjunto Y tal que $X \subset Y$?</p> <p>a) Sim b) Não</p>	
<p>5) Caso tenha respondido sim na questão anterior, você julga a sucessão $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset X \subset Y$ é:</p> <p>a) finita b) infinita</p>	

Figura 6.4: Questionário aplicado aos professores - p.2

Referências Bibliográficas

- [1] ARAÚJO, N. B. F. Números complexos: uma proposta de mudança metodológica para uma aprendizagem significativa no ensino médio. Master's thesis, Universidade Federal do Rio Grande do Norte, 2006.
- [2] BATISTA, ELIEZER E DOS SANTOS, M. V. Rotações, quatérnions e álgebras de clifford.
- [3] BOTT, R. MILNOR, J. On the parallelizability of the spheres. *University of Michigan and Oxford University* (1958), 87–89.
- [4] CEZAR, M. S. Concepções acerca do conceito de números reais: Uma breve reflexão sobre seu ensino na educação básica. Master's thesis, Departamento de Educação e Ciências Humanas. UFES/CEUNES. São Mateus, ES, 2011.
- [5] CONWAY, JOHN H E GUY, R. *The book of numbers*. Springer Science & Business Media, 2012.
- [6] DE BIASI, SERGIO COUTINHO E GATTASS, M. Utilização de quatérnions para representação de rotações em 3d. *Relatório técnico, TecGraf–Pontifícia Universidade Católica do Rio de Janeiro, PUCRIO. Disponível em <http://www.tecgraf.pucrio.br/~mgattass>* (2007).
- [7] DEVLIN, K. J. *O instinto matemático*. Record, 2009.
- [8] DO JÚRI, C. *Os quatérnions e suas aplicações*. PhD thesis, UNIVERSIDADE LUSÍADA DE LISBOA, 2012.
- [9] FELZENSZWALB, B. *Álgebras de Dimensão Finitas*. Instituto de Matemática Pura e Aplicada-IMPA, 1979.
- [10] FERREIRA, J. *A construção dos números*. Sociedade Brasileira de Matemática, 2011.
- [11] FREITAS, J. R. Equações algébricas nos quatérnions de hamilton.

- [12] GASPAR, A. D. J. Um estudo sobre quatérnios e sua aplicação em robótica theldo cruz franqueira.
- [13] GRUNDHOFER, THEO E HAHN, H. Fibration of spheres by great spheres over division algebras and their differentiability. *J.Differential Geometry* (1990), 357–363.
- [14] HATCHER, A. *Algebraic Topology*. 2002.
- [15] HERSTEIN, I. *Topics in Algebra*. John Wiley and Sons, 1964.
- [16] HOHENWARTER, MARKUS E HOHENWARTER, J. Ajuda geogebra: Manual oficial da versão 3.2. *Sl:sn* (2009).
- [17] LENZ, O. U. Some results on the existence of division algebras over \mathbb{R} .
- [18] LIMA, E. L. *Exame de textos: Análise de Livros didáticos para o Ensino Médio*. Rio de Janeiro, 2001.
- [19] LINGUAGENS, C. Orientações curriculares para o ensino médio, 2006.
- [20] MARÃO, J. A. P. F. Hipercomplexos: um estudo da analicidade e da hiperperiodicidade de funções octoniônicas.
- [21] MÉDIO, P. C. N. D. E. Ciências da natureza, matemática e suas tecnologias. *Brasília: MEC/SEB* (2006).
- [22] MILIES, C. P. Breve história da álgebra abstrata. *II Bienal da Sociedade Brasileira de Matemática (www.bienasbm.ufba.br/M18.pdf)* (2004).
- [23] NEVES, R. C., AND GRIMBERG, G. E. *Os quatérnios de Hamilton e o Espaço*. PhD thesis, Dissertação de, 2008.
- [24] ONETO, A. *Alternative real division algebras of finite dimension*, vol. 10. 2002.
- [25] RIBEIRO, S. M. Parametrização e animação de rotações no espaço por quatérnios.
- [26] RODRÍGUEZ BOUZA, V. Sobre los cuaterniones, álgebras de lie, y matrices de pauli. teoría básica y aplicaciones físicas.
- [27] SANTIAGO, P. R. P. Rotações tridimensionais em biomecânica via quatérnios: aplicações na análise dos movimentos esportivos.
- [28] SANTOS, D. J. D. E. O. A álgebra dos complexos/quatérnios/octônios e a construção de cayley-dickson.

-
- [29] SANTOS, M. A. D. Dos números complexos aos quatérnions: desenvolvimento algébrico, interpretação geométrica e aplicações. Master's thesis, Universidade Tecnológica Federal do Paraná, 2013.
- [30] SCHAFER, R. D. *An introduction to nonassociative algebras*, vol. 22. Courier Corporation, 1966.
- [31] WAGNER, EDUARDO E MORGADO, A. C. D. O. E. C. M. P. D. Trigonometria e números complexos. *Editora SBM* (2005).

Universidade Federal do Recôncavo da Bahia - UFRB
Centro de Ciências Exatas e Tecnológicas / Colegiado do Programa de Mestrado
Profissional em Matemática em Rede Nacional

Rua Rui Barbosa, 710, Centro, *Campus* Universitário de Cruz das Almas, Cruz das
Almas – BA
CEP: 44380-000
<<http://www.ufrb.edu.br/profmat/>>