Universidade Federal de Sergipe

Centro de Ciências Exatas e Tecnologia

Departamento de Matemática

Pós-Graduação em Matemática

A Construção Ortodoxa dos Números: Dos Números Naturais aos Complexos

São Cristóvão – SE
Abril de 2017

Universidade Federal de Sergipe

Centro de Ciências Exatas e Tecnologia

Departamento de Matemática

Pós-Graduação em Matemática

A Construção Ortodoxa dos Números: Dos Números Naturais aos Complexos

por

WESLEY SIDNEY SANTOS OLIVEIRA

sob a orientação do

Prof. Dr. Gerson Cruz Araujo

São Cristóvão – SE
Abril de 2017

A Construção Ortodoxa dos Números: Dos Números Naturais aos Complexos

por
WESLEY SIDNEY SANTOS OLIVEIRA

Dissertação apresentada ao Corpo Docente da Pós-Graduação em Matemática da Universidade Federal de Sergipe como requisito parcial para a obtenção do título de Mestrado profissional em Matemática.

Área de Concentração: Álgebra

Aprovada em 20 de Abril de 2017.

Banca Examinadora:

Prof. Dr. Gerson Cruz Araujo – UFS
(Orientador)

Prof. Dr. Naldisson dos Santos - UFS
(Examinador Interno)

Prof. Dr. Lucas Rezende Valeriano - UFS
(Examinador Externo)

Pai é... Um homem comum
dando o melhor de si
para cumprir a funao de
Super-Homem!!

Agradecimentos

• Gostaria primeiramente de agradecer a Deus por me conceder essa vitória e aos meus familiares e amigos mais próximos que sempre acreditaram em meu potencial. Em especial, agradeço a esses dois anjos presentes em minha vida que é: minha mãe, Neildes, que sempre insistiu para que eu realizasse esse sonho depositando total confiança em mim e a minha esposa Marianny, que sempre esteve ao meu lado torcendo por mim em noites de estudos sem dormir, com toda dificuldade, mas nunca largou minha mão e me acompanhou nessa jornada.

• Agradeço e dedico essa vitória a toda minha família: Minha irmã Deny, meu pai Adailton, meus irmãos Neilton, Adeilton (em vários momentos de minha vida tornou-se minha refência) e Adenilton, como também minhas cunhadas Edlaine e Rosivânia.

• Seria injusto não citar e agradecer a minha sogra, Cleide, que sempre foi uma segunda mãe, me apoiando e incentivando as minhas conquistas. Agradeço também aos colegas de classe que foram cruciais para minha formação: Lázaro (extremamente detalhista e persistente), Sóstenes (completamente assíduo), Glauber (um gênio geométrico), Edson (sempre buscando clareza), Ruan (simplismente impressionante) e Alexandre, em especial, ao meu parceiro de todas as horas e estudos Deusdete.

• Todos os professores que contribuíram de forma direta para essa conquista, então agradeço formalmente à: Giovana, Almir, André, Zaqueu, Evílson, Bruno, Kalasas, Fábio, Débora e ao meu orientador Gerson. Concluo, com meus sinceros agradecimentos ao meu amigo e colega de trabalho, além de excelente profissional, Msc. Hélio Jr que me aconselhou e torceu para meu ingresso no curso e também à Marcone Borges pela pessoa que é, excelente profissional, flamenguista, fera da matemática que me ajudou ao extremo na minha jornada acadêmica.

• Dedico essa conquista, do fundo do coração, ao meu filho, Enzo Lucca, pois foi nele que sempre encontrei inspiração e forças para continuar naqueles momentos mais difíceis, que foram muitos, ao ver mais da metade da turma desistir, enfrentando minha jornada árdua de trabalho. Enfim, quanto maior a dificuldade, mais valorizada é a conquista.

Resumo

No presente trabalho, investigamos, cuidadosamente, a construção dos números naturais, inteiros, racionais, reais e números complexos. Sendo que, o conjunto dos números reais foi obtido através dos conhecidos métodos: Cortes de Dedekind e Classe de Equivalência por Sequências de Cauchy. O estudo consistiu em utilizar os famosos Axiomas de Peano, os quais estão relacionados aos números naturais, em ordem a obter as bem conhecidas propriedades elementares satisfeitas por todos estes números. E, a partir deste conhecimento, encontramos rigorosamente as provas dos resultados básicos envolvendo os números reais. Este processo em questão foi desenvolvido de maneira construtiva através dos números inteiros e racionais. Em seguida, mostramos que é possível estabelecer a existência dos números complexos, juntamente com suas propriedades aritméticas mais usuais. Por fim, terminamos cada capítulo do nosso trabalho mostrando algumas possíveis aplicações em cada conjunto trabalhado.

Palavras-chave: Axiomas de Peano; Números Reais; Números Complexos;

Abstract

In this work, we investigated the construction of natural, integer, rational, real, complex, quaternion and Octonion numbers. More precisely, the set of real numbers was achieved by applying two methods: Dedekind Cuts and Equivalence Classes of Cauchy Sequences. Our study is only based on using Peano Axioms, which are directly related to the natural numbers, in order to get the basic properties satisfied by these numbers. In addition, we carefully proved the elementary results involving real numbers. This process in question was developed constructively throughout of the concepts of the integer and rational numbers. Next, we show that it is possible to establish the existence of complex numbers along with their more usual arithmetic properties. Finally, we finish each chapter of our work showing some possible applications in each set worked.

Keywords: Peano Axioms; Real Numbers; Complex Numbers.

Sumário

Introdução

Notoriamente, a Teoria dos Números foi de suma importância para o desenvolvimento científico da civilização, e apesar de ser uma área de estudos milenar, é de certa forma surpreendente, que a Teoria dos Números, seja atualmente, uma das áreas de pesquisa mais efervescentes da Matemática e que mais do que nunca, continue a fascinar as atuais gerações de Matemáticos. Evidente que, ao longo do tempo, esta Teoria passou por algumas transformações e quebras de paradigmas. Nos primordios da sociedade sedentária, por exemplo, a maneira de trabalhar com contagem foi aprimorada ao longo dos séculos, de acordo com as problemáticas do cotidiano de antigas civilizações. O homem criava situações interessantes na contagem de seus objetos, animais e etc. Por exemplo, ao levar seu rebanho para a pastagem ele relacionava uma pedra para cada animal, no momento em que ele recolhia os animais fazia a relação inversa, no caso de sobrar alguma pedra poderia verificar a falta de algum animal.

Conceda-nos apresentar da forma mais natural possível, um pouco da história desta fascinante teoria, tentando ao máximo, seguir uma ordem cronológica da formulação de cada elemento que forma tal área, a saber, os números Naturais, números Inteiros, números Racionais, Reais e Complexos.

Evidentemente começaremos com os números Naturais. Tais números tiveram suas origens com os egípcios, por volta de 1650 a.C., partindo da necessidade de se efetuar cálculos rápidos e precisos (já que estavam acontecendo muitos progressos, como a construção das pirâmides, os quais marcaram o fim da Pré-História), pois com a contagem concreta (usando pedras, nós ou riscos em ossos) não estava sendo prático. Foi quando surgiram as representações da quantidade de objetos através de desenhos: os símbolos. Os egípcios baseavam seu sistema de numeração em sete números-chave e todos os outros números eram escritos combinando os números-chave. Para os egípcios, a ordem dos símbolos não alterava o número em questão. Outros povos (Babilônicos, Romanos, Gregos, Hindus, Árabes) também criaram o seu próprio sistema de numeração, mas foram os romanos que criaram um sistema de numeração bem mais prático e eficiente. Os romanos

aperfeiçoaram a representação do número, mas não usaram símbolos novos para representar os números, usaram as próprias letras do alfabeto.

Os romanos baseavam seu sistema de numeração em sete números-chave (I,V,X,L,C,D,M). Os cálculos que os romanos utilizavam eram baseados na adição e na subtração, dependendo da ordem em que os números-chave apareciam. Este sistema foi adotado por muitos povos, mas ainda era difícil efetuar cálculos com o mesmo. Foi quando aconteceu no norte da Índia, por volta do século V da era cristã, uma das mais notáveis invenções de toda a história da Matemática: O sistema de numeração decimal. Isto aconteceu após o aperfeiçoamento dos símbolos utilizados pelos hindus, quando houve a ideia de introduzir uma notação para uma posição vazia − o zero. Foi quando os dez símbolos que conhecemos hoje em dia foram criados. Hoje, estes símbolos são chamados de algarismos indo-arábicos. Mas foram os árabes, a partir da metade do século IX, que divulgaram ao mundo os números hindus, após traduções de livros vindos da Índia. Os árabes compreenderam o tesouro que os matemáticos hindus haviam descoberto. Isto permitiu o desenvolvimento de sistemas para o armazenamento de grandes números. Por isso, o nosso sistema de numeração decimal é conhecido como indo-arábico. Com este sistema de numeração ficou mais viável escrever qualquer número, por maior que ele fosse, e como estes números foram criados para tornar mais prático contar as coisas da natureza, eles foram chamados de números naturais. Com o início do Renascimento (Século XV) surgiu a expansão comercial, que aumentou a circulação de dinheiro, obrigando os comerciantes a expressarem situações envolvendo lucros e prejuízos. A maneira que eles encontraram de resolver tais situações problemas consistia no uso dos símbolos + e −.

Para suprir a deficiência dos Números Naturais em resolver operações do tipo $a - b$, com $a < b$, é que foi ampliado o conjunto dos naturais formando o conjunto dos números inteiros $\{..., -2, -1, 0, 1, 2, 3, ...\}$ denotado pelo símbolo $\mathbb{Z}$ (da palavra alemã Zahl, que significa número). Na Índia, a necessidade de realizar com maior rapidez os cálculos oriundos da astronomia fez com que os sábios hindus se preocupassem em idealizar formas de representação numérica que simplificassem esses cálculos. Os matemáticos hindus se mostraram virtuosos no cálculo aritmético e manipulações algébricas que permitiram conceber um novo tipo de símbolo para representar dívidas que posteriormente o Ocidente chamaria de negativo. A primeira vez que explicitamente as regras que regem a aritmética com os números negativos apareceram em uma obra foi na obra de *Brahmagupta*, que data do ano 628 d.C. Esse matemático indiano não só utilizou os negativos em seus cálculos como os considerou entidades separadas e os dotou de uma aritmética concordante com a dos naturais. Muitos séculos se passaram para que o interesse pelos números negativos fosse retomado. Alguns historiadores escreveram que foram problemas com dinheiro que interpretaram o número negativo como perda. Negativo − esta palavra pode ter vindo desta época que eram os va-

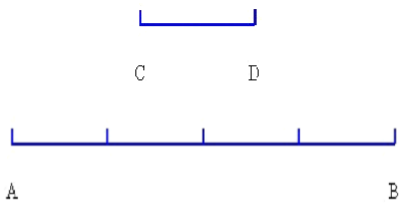
lores negados quando se obtinha raízes negativas de uma equação. O filósofo Diofanto, (século III) em seus estudos, encontrou muitas vezes com os números negativos. Eles apareciam constantemente em cálculos intermediários em muitos problemas de seus Ensaios, denominados de *Aritmetika*. No entanto, havia certos problemas para o qual as soluções eram valores inteiros negativos como, por exemplo, $4 = 4x + 20$. Nestas situações Diofanto limitava-se a classificar o problema de absurdo. Nos séculos XVI e XVII, muitos matemáticos europeus não apreciavam os números negativos e, se esses números apareciam nos seus cálculos, eles consideravam-nos falsos ou impossíveis. Exemplo deste fato foi nos estudos desenvolvidos por Michael Stifel (1487−1567) que se recusou a admitir números negativos como raízes de uma equação, chamando-lhes de *numeri absurdi*.

A situação mudou (a partir do século XVI) quando foi descoberta uma interpretação geométrica dos números positivos e negativos como sendo segmentos de direções opostas. Foi no Renascimento que apareceu um número negativo ligado a uma equação algébrica, na obra do matemático francês Nicolás Chuquet (1445−1500). Trata-se de seu tratado *Triparty*, escrita em 1484, que contém uma expressão que poderíamos escrever hoje como $4x = -2$. Na época, ainda não eram usados os simbolos $x, =$ e $-$. Simon Stevin (1548−1620) aceita os números negativos como raízes e coeficientes de equações. Admite a adição de $x + (-y)$ em lugar de considerá-la como subtração de y á x. Também tratou de justificar geometricamente a regra de sinais fazendo uso da identidade algébrica: $(a - b)(c - d) = ac - bc - ad + bd$. O matemático Albert Girard (1590 −1639) foi o primeiro a reconhecer, explicitamente, a utilidade algébrica de admitir as raízes negativas e imaginárias como soluções formais das equações, porque ele permitia uma regra geral de resolução na construção de equações através de suas raízes. A legitimidade dos números negativos deu-se definitivamente por Hermann Hankel (1839−1873) em sua obra *Teoria do Sistema dos números Complexos*, publicada em 1867. Hankel formulou o princípio de permanência e das leis formais que estabelece um critério geral de algumas aplicações do conceito de número.

Seguindo a linha logica dos nossos estudos, os números fracionários foram intuitivamente descobretos na antiguidade, mas, na falta de numerações bem constituídas, suas notações foram, durante muito tempo, mal fixadas e inadaptadas às aplicações práticas. Não foram consideradas desde sua origem como números nem se concebia a noção de fração geral $\frac{m}{n}$ como m vezes o inverso de n. Os egípcios, por exemplo, só conheciam as frações denominadas *unitárias* (as de numerador igual a 1) e só exprimiam as frações ordinárias através de somas de frações desse tipo (mostraremos ao longo do trabalho) (por exemplo: $\frac{7}{12} = \frac{1}{3} + \frac{1}{4}$). Com o passar do tempo, ficou claro que as frações se submetiam às mesmas regras que os inteiros e que eram, portanto, assimiláveis aos números (sendo um inteiro uma fração de denominador igual a 1). Graças a esta extensão, os números, que outrora serviam apenas para recenseamento, tornaram-se *marcas* adaptadas a inúmeros usos. Daí

em diante, não só foi possível comparar duas grandezas *por estimação*, mas também dividi-las em parcelas ou pelo menos supô-las divididas em partes iguais de uma grandeza da mesma espécie escolhida como padrão. Mas, apesar desse progresso, por causa de suas notações imperfeitas os antigos não foram capazes nem de unificar a notação de fração, nem de construir um sistema coerente para suas unidades de medida. Assim como os números naturais surgiram da necessidade de contar, os números racionais, que são expressos pela razão entre dois inteiros, surgiram da necessidade de medir. Medir e comparar. Para isso foi necessário estabelecer um padrão de comparação para todas as grandezas da mesma espécie, por exemplo, 1 cm para comprimentos, 1 segundo para tempo, etc. Este padrão estabelece uma unidade de medida da grandeza (comprimentos, áreas, tempo, etc). Medir, portanto, é determinar quantas vezes a unidade estabelecida cabe, por exemplo, no comprimento que se quer medir. O resultado desta comparação, que é a medida da grandeza em relação à unidade considerada, deve ser expresso por um número. Na figura abaixo, se considerarmos o segmento CD como a unidade de medida, teremos que o segmento AB mede 4 unidades. Tomando-se CE como unidade, a medida deste mesmo segmento será de 8 unidades.

Só em casos muito especiais a grandeza a ser medida contém um número inteiro de vezes a unidade de medida. O caso mais frequente é o caso da figura abaixo onde, tomando-se a medida u do segmento CD como unidade, a medida de AB é maior que 3 u e menor que 4 u .



É claro que neste exemplo, podemos subdividir a unidade em partes menores para que cada uma delas caiba um número inteiro de vezes na grandeza a medir, mas o que se pode dizer da medida de AB em relação à CD? A dificuldade surge porque, neste caso, a medida m de AB não é divisível pela medida u de CD. No conjunto dos números inteiros existe a impossibilidade da divisão, isto é, neste conjunto nem sempre é possível expressar o resultado de uma medição ou de uma razão. Para resolver esse problema criou-se um novo conjunto de números, chamado conjunto dos números racionais e denotado pelo símbolo $\mathbb{Q}$ (de quociente). Um número racional p é, portanto, aquele que pode ser escrito na forma $p = \frac{m}{n}$, onde m e n são inteiros e $n \neq 0$. (Lembre-se que a divisão por zero não tem sentido, pois não existe nenhum número que multiplicado por zero seja diferente de 0 e, portanto, expressões do tipo $\frac{3}{0}$ não estão definidas e expressões do tipo $\frac{0}{0}$ são indeterminadas). Os

babilônios, através de sua numeração de posição com base sessenta, foram os primeiros a atribuir às frações uma notação racional, convertendo-as em frações sexagesimais (cujo denominador é igual a uma potência de 60) e exprimindo-as mais ou menos como se exprimem as frações de horas em minutos e segundos:

$$33 \text{ min } 45\text{s} = \tfrac{33}{60}h + \tfrac{45}{3600}h.$$

Mas os babilônios não chegaram ao uso da *vírgula* para diferenciar os inteiros das frações sexagesimais da unidade. A expressão (33;45) tanto podia significar 33h 45 min quanto 0h 33 min 45s. O entendimento ficava estabelecido pelo contexto. Depois deles, os gregos tentaram atribuir uma notação geral às frações ordinárias, mas sua numeração alfabética complicou muito a simbolização, o que os levou a desistir de adotar a notação sexagesimal de origem babilônica em seus cálculos com frações. A notação moderna das frações ordinárias se deve aos hindus, que, devido a sua numeração decimal posicional chegaram a simbolizar frações mais ou menos como fazemos hoje. Esta notação foi depois adotada e aperfeiçoada pelos árabes, que inventaram a famosa barra horizontal. Em seguida, graças à descoberta das frações *decimais* (aquelas cujo denominador é uma potência de 10) foi pouco a pouco transparecendo o interesse em prolongar a numeração decimal de posição no outro sentido, isto é, em termos modernos, na representação de números *depois da vírgula*. O que permitiu a notação sem nenhuma dificuldade de todas as frações, além de mostrar nitidamente os inteiros como frações particulares: aquelas cuja representação não comporta nenhum algarismo depois da vírgula.

As conseqüências desta racionalização da noção e da representação das frações foram incalculáveis em todos os domínios, a começar pela invenção do sistema métrico. Sistema metrológico fundado sobre a base dez, coerente e perfeitamente adaptado ao cálculo numérico. Desenvolvido na Revolução Francesa (1792) em substituição aos velhos sistemas de unidades arbitrárias incoerentes e variáveis.

A numeração decimal de posição introduziu também a infinita complexidade do universo dos números, e levou os matemáticos a um avanço prodigioso. Desde o século VI a.C., os matemáticos gregos, a começar pela escola Pitágorica, já tinham descoberto que a diagonal de um quadrado *não tem medida comum* com o seu lado. De fato, tanto pela medida quanto pelo raciocínio, o comprimento de sua diagonal não corresponde a um número inteiro de metros. Ou seja, uma vez que tal é o seu comprimento matemático, a $\sqrt{2}$ é um número *incomensurável*. Foi a descoberta do que hoje denominamos *números irracionais*, os que não são nem inteiros nem frações. Esta descoberta provocou uma grande consternação entre os Pitagóricos, que pensavam até então que *os*

números regem o Universo, isto é, os inteiros naturais e suas combinações mais simples, as frações ordinárias positivas. O próprio nome destas grandezas é uma prova desde que foram denominadas *inexprimíveis*. A categoria dos números irracionais ficou ainda pouco precisa durante séculos por causa das notações imperfeitas de outrora, que não permitiam a representação destes números de um modo coerente, já que eles eram designados por palavras e valores aproximados aparentemente sem nenhuma relação uns com os outros. Como não era possível defini-los corretamente, constatou-se simplesmente a sua existência, sem poder implicá-los num raciocínio geral. Beneficiados por uma notação numérica muito eficaz e por uma ciência cada vez mais avançada, os matemáticos europeus dos tempos modernos conseguiram ter sucesso onde seus antecessores tinham falhado. Eles descobriram que estes números eram identificáveis a números decimais sem fim, cujos algarismos após a vírgula nunca se reproduzem na mesma ordem. Descoberta fundamental que permitiu uma melhor compreensão desta categoria de números, já que eles têm por característica esta propriedade. Se o número é irracional a parte decimal não segue um padrão, isto é, não se repete nunca! Com o auxílio de um computador, podemos calcular a representação decimal de $\sqrt{2}$ e de π com muitas casas decimais para nos convencer deste fato. Embora estes números com suas aproximações vistas em computador com até bilhões de casas decimais sejam convincentes, isto não basta como uma prova matemática. É possível demonstrar logicamente que $\sqrt{2}$ é irracional (faremos a prova ao longo deste trabalho) e também que os números π e e são irracionais.

No entanto, a extensão destes sistemas ainda era necessária, com o objetivo de obter um quadro claro da relação entre números e pontos de uma reta, desenvolvendo a noção de completude, propriedade que o sistema dos racionais não tem. Construir a reta numerada completa implica construir um novo sistema numérico que inclui os racionais, como subsistema. O sistema inclui todas as razões entre quantidades geométricas − todos os valores que resultam de medidas − e muitos desses valores não são números racionais. À união dos números racionais com os irracionais, denominamos Conjunto dos Números Reais. O conceito do conjunto dos números reais passou pelo matemático Eudoxo, no século IV a.C., o qual tem sua teoria das proporções registrada no famoso livro Elementos de Euclides. Durante a segunda metade do século XIX um crescente número de artigos e livros foram publicados, dedicados a um único assunto: a definição precisa de número real e a investigação de funções reais baseada nessa definição. Podemos destacar três campos distintos de construção da definição de número real.

− Heine (1821 - 1881), Thomae (1840 - 1921) e Hilbert (1862 - 1943) defenderam que os conceitos fundamentais da Análise poderiam, e deveriam, ser construídos simplesmente de uma maneira formal, desprezando, tanto quanto possível, os assuntos de ordem filosófica.

– Hankel (1839 - 1873) e Frege (1848 - 1925) defenderam a ideia tradicional de que a Análise deveria ser fundada na noção de quantidade contínua.

Hankel estudou com Riemann (1826 - 1866) bem como com Weierstrass e Kronecker (1823 - 1891). Em 1867 publicou o livro Theorie der Complexen Zahlensysteme, insbesondere der gemeinen imaginären Zahlen und der Hamiltonschen Quaternionen onde tratou um dos assuntos que caracterizou o fim da ciência da quantidade. Para Hankel o número não é um objeto, é uma substância que existe fora do sujeito e do objeto que lhe deu origem, é um princípio independente, tal como foi visto pelos Pitagóricos.

– Dedekind, Weierstrass (1815 - 1897) e Cantor defenderam que a noção de quantidade deveria ser substituída por uma rigorosa construção aritmética dos números reais, isto é, uma construção baseada na noção de números naturais ou racionais, que assumiu-se ser menos problemática do que a noção de quantidade contínua. O conceito só foi concretizado no século XIX, através dos matemáticos alemães Cantor e Dedekind, estes construíram os números reais a partir do conjunto dos racionais: Cantor pelo método conhecido por Classe de Equivalência de Sequências de Cauchy e Dedekind por Cortes de Dedekind. Abordaremos os dois tipos de obtenção dos reais nesta dissertação.

Apesar do conjunto dos números reais ser completo, havia uma problemática desde o surgimento da fórmula de Baskara no século XI. Dependendo da equação quadrática, poderia ocorrer do número delta ser negativo. Entretanto isso não pertubava muito os matemáticos da época. Neste caso eles simplesmente diziam que o problema não tinha solução. O interesse pelo estudo da Matemática ressurgiu na Europa, mais especificamente na Itália, no século XVI. Lá, e no meio da disputa entre Cardano e Tartaglia pela resolução da equação do 3^{o}grau, é que se percebeu que os números reais não eram suficientes e as primeiras ideias da criação do conjunto dos números complexos surgiram. Questões realmente perturbadoras surgiram e não podiam ser ignoradas. Além da extração de raízes quadradas de números negativos, também nos deparamos com uma extração de raizes cúbicas de números de natureza desconhecidas. Quando, nas equações de grau 2 a fórmula de Baskara levava à raiz quadrada de números negativos, era fácil dizer que aquilo indicava a não existência de soluções. Agora, entretanto, nota-se que há equações de grau 3 com soluções reais conhecidas, mas cuja determinação passava pela extração de raízes quadradas de números negativos.

Não havia como negar que os números reais eram insuficientes para se tratar de equações algébricas. O que estava acontecendo no século XVI era semelhante ao que ocorreu no tempo dos gregos antigos, quando se verificou a insuficiência dos números racionais com a construção

do número $\sqrt{2}$, que não era racional: o conceito de número precisava ser estendido. Foi Rafael Bombelli, engenheiro hidráulico nascido em Bolonha, Itália, em 1530, quem conseguiu atravessar a barreira e chegar aos novos números. A partir da ideia pioneira de Bombelli, ainda se demorou mais de dois séculos para que se conseguisse, através de Euler, saber como extrair raízes de números complexos.

Entretanto, foi na primeira metade do século XVII que os geniais matemáticos franceses Pierre de Fermat e René Descartes inventaram, independentemente e quase simultaneamente, o que hoje conhecemos por Geometria Analítica. Com o domínio da geometria Analítica Descartes estudou, entre outras coisas, as equações algébricas. Em uma passagem do Discurso do Método Descartes escreveu a seguinte frase: *Nem sempre as raízes verdadeiras (positivas) ou falsas (negativas) de uma equação são reais. Ás vezes elas são imaginárias.* Por esse motivo, até hoje o número que denominamos de raiz de -1 é chamado de número imaginário, termo que se consagrou juntamente com a expressão *número complexo*. Infelizmente, são designações um tanto inadequadas e subjetivas para objetos matemáticos.

Depois de Bombelli, em 1530, outros personagens importantes da História da Matemática deram contribuições ao desenvolvimento da teoria dos números complexos, dentre os quais o matemático francês Abraham de Moivre, amigo de Isaac Newton, e também os irmãos Jacques e Jean Bernoulli. Mas quem fez o trabalho mais importante e decisivo sobre o assunto foi Euler. Dentre as inúmeras contribuições de Euler foi notável seu empenho na melhoria da simbologia. Muitas das notações que utilizamos hoje foram introduzidas por ele. Dentre as representações propostas por Euler destacamos o i substituindo $\sqrt{-1}$. Euler passou a estudar números da forma $z = a + bi$ onde a e b são números reais e $i^2 = -1$. Esses números são chamados de números complexos.

Em resumo, até o século XIX, os números naturais eram vistos como coleções de unidades; frações eram razões entre quantidades; números reais eram comprimentos de segmentos e números complexos eram pontos do plano. Mas os matemáticos não estavam satisfeitos com os resultados baseados nestas noções intuitivas. Era preciso construir uma teoria dos números. Nessa perspectiva, foi formulado um princípio geral para direcionar qualquer generalização do conceito de número: o princípio da permanência das leis do cálculo. Para construir um novo sistema numérico, como extensão de um sistema dado, as operações devem ser definidas de tal modo que as leis existentes permaneçam. A partir da definição axiomática do sistema dos números naturais, foi construída a teoria dos inteiros, como pares de números naturais (cuja diferença m-n vai resultar num número inteiro positivo ou negativo); a teoria dos números racionais como pares de números inteiros (cujo quociente m:n vai resultar num número racional); e a teoria dos números reais como seqüências

de racionais (cujo limite vai resultar num número real). Sabemos que grande parte das disciplinas ministradas nos cursos de Matemática apresenta muito discretamente a origem dos números reais e imaginários (inclusive Fundamentos da Matemática). Além disso, em disciplinas como Análise Real, os conjuntos constituídos por esses números são adotados existentes por razões de falta de tempo hábil para o cumprimento da ementa. Assim sendo, nosso interesse neste trabalho é a construção detalhada dos conjuntos de números tais como: naturais, inteiros, racionais, reais e complexos.

Enfim, descreveremos resumidamente o que será feito em todos os capítulos listados neste texto: No primeiro capítulo formalizaremos o conceito de número natural e apresentaremos suas propriedades através dos conhecidos Axiomas de Peano, além disso, apresentaremos uma aplicação lúdica no jogo Torre de Hanói. No capítulo seguinte, veremos a construção do conjunto dos números inteiros utilizando conceitos como relações de equivalência e noções de Teoria dos Conjuntos e da estrutura do conjunto anteriormente construído, e ao fim do capítulo, apresentaremos um exemplo na Astronomia. Por conseguinte, notaremos que a construção do conjunto dos números racionais é feita de maneira análoga a dos inteiros − neste capítulo daremos ênfase à aplicação dos racionais apresentando ao leitor o Método de Sylvester - . Já no quarto capítulo, faremos a construção do conjunto dos números reais aplicando os métodos descritos acima: Cortes de Dedekind e Sequências de Cauchy. Neste capítulo, faremos duas aplicações notaveis: A sequência de Fibonacci e o Conjunto de Cantor (Carpete de Sierpinsk). Por fim, no último capítulo, faremos a construção e aritmetização dos números imaginários (complexos) e como aplicação, daremos ênfase à equação da onda, mais conhecida como equação de Schrödinger.

É importante ressaltar que toda a dissertação visa os aspectos aritméticos da construção dos conjuntos de números citados acima. Portanto, nenhum tipo de aplicação, fora do ambiente da Matemática, será abordado neste texto. Em contra ponto, trabalharemos em um caminho que este estudo seja, com exceções das definições de conjunto e função[1], autoconsistente e com uma grande riqueza de detalhes. Vale também destacar que, [3], e [9] são usadas como referências principais neste trabalho.

Em todo o trabalho usaremos a notação ($\Rightarrow$) para denotar que estamos interessados em provar a implicação direta exposta no resultado em questão. Já ($\Leftarrow$) significará que iremos provar a recíproca da afirmação estabelecida previamente. O símbolo $:=$ será usado com o sentido de "igual por definição". Para concluir, **a**)$\Rightarrow$**b**) nos dirá que utilizaremos as informações dadas no item **a**) para obter o que estará estabelecido em **b**).

[1]Os conceitos básicos envolvendo conjuntos e funções podem ser encontrados com mais detalhes em [7].

Capítulo 1

Construção dos Números Naturais

1.1 Os Axiomas de Peano

Nesta seção, estabeleceremos os Axiomas de Peano [1], os quais são apresentados em forma de postulado (ver Axioma 1.1 abaixo) e comprovam rigorosamente nossas ideias intuitivas sobre o conjunto dos números naturais. Em ordem a entendermos por completo o enunciado deste axioma, dado logo abaixo, precisamos de alguns conceitos matemáticos básicos como, por exemplo, os de conjuntos e funções.

Axioma 1.1 (Axiomas de Peano)**.** Existem um conjunto $\mathbb{N}$ (denominado conjunto dos Números Naturais) e uma função $s : \mathbb{N} \to \mathbb{N}$ que satisfazem os seguintes postulados:

A1) s é injetiva[2];

A2) Existe um elemento $0 \in \mathbb{N}$ tal que $0 \notin \mathrm{Im}(s)$ (aqui $\mathrm{Im}(s)$ é a imagem da aplicação s);

A3) [Princípio da Indução] Assuma que $X \subset \mathbb{N}$ satisfaz as afirmações abaixo:

i) $0 \in X$;

ii) $k \in X \Rightarrow s(k) \in X$.

Então, $X = \mathbb{N}$.

A aplicação s considerada no Axioma 1.1 tem sua origem na palavra sucessor. Mais precisamente, temos a seguinte definição.

[1] Outra referência clássica para construção dos números naturais é via Teoria dos Conjuntos, no qual pode ser vista detalhadamente em [5] e [10].

[2] Uma função $f : A \to B$ é chamada injetiva se $f(x) = f(y)$, com $x, y \in A$, implicar $x = y$.

Definição 1.1. A função s, dada acima, é denominada função (ou aplicação) sucessor. Além disso, chamamos $s(x) \in \text{Im}(s) \subset \mathbb{N}$ sucessor de x, onde $x \in \mathbb{N}$.

É importante ressaltar que, o axioma **A3**) acima dado é conhecido na literatura como o Princípio da Indução Finita (ou Princípio da Indução Matemática, ou simplesmente Princípio da Indução). Além disso, **A2**), estabelecido acima, garante que $\mathbb{N} \neq \emptyset$ (pois $0 \in \mathbb{N}$) e também que $s(0) \neq 0$ (desde que $0 \notin \text{Im}(s)$ e $s(0) \in \text{Im}(s)$). Portanto, $\mathbb{N}$ contém, pelo menos, os elementos distintos 0 e $s(0)$. Consequentemente, como s é injetora (ver **A1**)), obtemos que $s(0) \neq s(s(0))$. Este fato acrescenta mais um elemento em $\mathbb{N}$, $s(s(0))$, o qual é diferente de 0 (através da simples justificativa: $0 \notin \text{Im}(s)$ e $s(s(0)) \in \text{Im}(s)$).

Seguindo o processo acima, tomando sucessores de forma iterada, parece que cada elemento encontrado é diferente de todos aqueles anteriormente obtidos. Devido a esse fato, somos levados a considerar que $\mathbb{N}$ é um conjunto infinito (esta afirmação ficará mais clara ao decorrer deste capítulo). A partir disto, podemos definir quando um conjunto qualquer é infinito da seguinte forma:

Definição 1.2. Um conjunto X é denominado infinito quando existe uma função injetora $f : \mathbb{N} \to X$. Caso contrário, X é chamado finito.

Note que a Definição 1.2 nos garante que um conjunto infinito X está em bijeção[3] com $f(\mathbb{N}) \subset X$. Reciprocamente, se existir uma bijeção $f : \mathbb{N} \to Y$, onde $Y \subset X$, então X é infinito (basta compor f com a inclusão $i : Y \hookrightarrow X$, dada por $i(y) = y$ para todo $y \in Y$).

Observe também que se X é finito e $Y \subset X$, então Y é finito. Caso contrário, existiria injeção $f : \mathbb{N} \to Y$. Logo, $i \circ f : \mathbb{N} \to X$, onde i é a inclusão de Y em X, seria injetora. Portanto, X seria infinito. Isto é uma contradição.

O primeiro exemplo de conjunto infinito que daremos, usando a definição acima, é o conjunto $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Mais especificamente, provaremos, no resultado abaixo, que a função $s : \mathbb{N} \to \mathbb{N}^*$ é uma bijeção.

Teorema 1.1. *Seja $s : \mathbb{N} \to \mathbb{N}$ a função sucessor. Então, são válidos os seguintes itens:*

i) *Nenhum número natural é sucessor de si próprio, isto é, $s(n) \neq n$ para todo $n \in \mathbb{N}$;*

ii) *$Im(s) = \mathbb{N}^*$.*

[3]Uma função $f : A \to B$ é dita bijetora se esta é injetora e sobrejetora ao mesmo tempo. Aqui f é denominada sobrejetora quando $Im(f) = B$.

Demonstração. Primeiramente vamos provar o item **i**). Para este fim, seja

$$X = \{n \in \mathbb{N}/s(n) \neq n\} \subseteq \mathbb{N}.$$

Agora, vamos utilizar o Princípio de Indução para mostrar que $X = \mathbb{N}$. Assim sendo, é fácil ver que $0 \in X$, pois $s(0) \neq 0$ (já que $0 \notin \text{Im}(s)$). Resta somente, então, verificarmos que vale a seguinte implicação:

$$k \in X \Rightarrow s(k) \in X.$$

De fato, se $k \in X$, então, pela definição de X, $s(k) \neq k$. Logo, aplicando s, obtemos $s(s(k)) \neq s(k)$ (pois s é injetora). Deste modo, $s(k) \in X$. Por fim, pelo Princípio da Indução, $X = \mathbb{N}$. Isto nos diz que $s(n) \neq n$, para todo $n \in \mathbb{N}$.

ii) Novamente, aplicaremos o Princípio da Indução ao conjunto $X = \{0\} \cup \text{Im}(s)$. Dessa forma, segue facilmente que $0 \in X$. Agora suponha que $k \in X$. É sabido que $s(k) \in Im(s) \subseteq X$; logo, $X = \mathbb{N}$. Consequentemente, usando o fato que $0 \notin \text{Im}(s)$, obtém-se $\text{Im}(s) = \mathbb{N}^*$. □

A partir do Teorema 1.1, temos que dado $n \in \mathbb{N}^*$ existe um único $m \in \mathbb{N}$ tal que $s(m) = n$ (pois $s : \mathbb{N} \to \mathbb{N}^*$ é uma bijeção). Isto nos possibilita estabelecer a definição do que significa antecessor de um número natural. Mais especificamente, se $n \in \mathbb{N}^*$ temos que o antecessor de n é o elemento $m \in \mathbb{N}$ tal que $s(m) = n$. Gostaríamos de frisar aqui que tal denominação não será utilizada neste trabalho.

1.2 Operações Elementares com Números Naturais

Nesta seção, estudaremos duas operações sobre o conjunto dos números naturais, as quais serão chamadas adição ($+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$) e multiplicação ($\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$).

1.2.1 Propriedades Elementares da Adição

Nesta subseção, formalizaremos o que significa adicionar números naturais; além disso, provaremos algumas propriedades elementares envolvendo tal adição. Mais precisamente, definimos adição da seguinte forma.

Definição 1.3. Definimos, recursivamente, a aplicação $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, denominada adição, que associa dois números naturais m e n a um outro $m + n$, do seguinte modo:

$$\begin{cases} m + 0 = m; \\ m + s(n) = s(m + n). \end{cases} \tag{1.1}$$

Obs 1.1. É importante ressaltar que, por definição, 0 é o elemento neutro[4] para a adição do naturais.

O resultado a seguir nos mostra como garantir que a adição, do maneira que está estabelecida acima, está bem definida.

Proposição 1.1. *A adição entre números naturais está bem definida, ou seja,* $m + n \in \mathbb{N}$ *para todo* $m, n \in \mathbb{N}$.

Demonstração. Inicialmente, fixe $m \in \mathbb{N}$ e considere o conjunto

$$X_m = \{n \in \mathbb{N} / m + n \in \mathbb{N}\}.$$

Segue diretamente de (1.1) que $0 \in X_m$ (pois $m + 0 = m \in \mathbb{N}$). Por outro lado, considere que $k \in X_m$; então, $m + k \in \mathbb{N}$. Por conseguinte, $s(k) \in X_m$ desde que $m + s(k) = s(m + k) \in \mathbb{N}$ (ver (1.1)). Por fim, aplicando o Princípio de Indução, obtemos $X_m = \mathbb{N}$. Isto completa a prova da proposição em questão. □

A partir da definição de soma entre números naturais é possível estabelecer a notação que estamos acostumados a utilizar no ensino elementar usando a definição de aplicação sucessor. Mais especificamente, temos a seguinte definição.

Definição 1.4. Denotaremos por 1, lê-se "um", o número natural que é sucessor de 0, isto é, $1 = s(0)$. Também definimos, $2 = s(1)$ (lê-se dois), $3 = s(2)$ (lê-se três), $s(3) = 4$ (lê-se quatro), e assim por diante.

Usando a notação da Definição 1.4, podemos escrever o conjunto dos números naturais de maneira usual.

Teorema 1.2. *É verdade que* $\mathbb{N} = \{0, 1, 2, 3, ...\}$.

[4] Um elemento 0 de um conjunto A, com uma operação de adição estabelecida, é chamado de elemento neutro da adição se $a + 0 = a$, para todo $a \in A$.

Demonstração. Seja $X = \{0, 1, 2, 3...\}$. Claramente, $0 \in X$. Além disso, o sucessor de cada elemento de X está em X. Portanto, pelo Princípio da Indução, $X = \mathbb{N}$. Por fim, $\mathbb{N} = \{0, 1, 2, 3, ...\}$. □

Note que a Definição 1.3 estabelece a forma de adicionar números naturais conhecida na literatura elementar. Com efeito,

i) $1 + 1 = 1 + s(0) = s(1) = 2$;

ii) $2 + 1 = 2 + s(0) = s(2) = 3$;

iii) $2 + 2 = 2 + s(1) = s(2 + 1) = s(3) = 4$;

iv) $2 + 3 = 2 + s(2) = s(2 + 2) = s(4) = 5$,

e assim por diante.

Em ordem a apresentar uma nova caracterização para a adição de números naturais, lembremos a notação usual de composição iterada de funções. Sendo assim, seja $f : X \to X$ uma função definida em um conjunto qualquer X. Defina

$$f^0 = Id_X \text{ e } f^{s(n)} = f \circ f^n,$$

onde $n \in \mathbb{N}$ e $Id_X(x) = x$ para todo $x \in X$.

Proposição 1.2. *Sejam $m, n \in \mathbb{N}$. Então, $m + n = s^n(m)$.*

Demonstração. Fixe $m \in \mathbb{N}$. Considere o conjunto

$$X_m = \{n \in \mathbb{N} / m + n = s^n(m)\}.$$

Em ordem a provar que $X = \mathbb{N}$, vamos aplicar indução sobre n. É fácil ver que $0 \in X_m$, pois

$$m + 0 = m = Id_{X_m}(m) = s^0(m).$$

Agora mostraremos que se $n \in X_m$, acarreta que $s(n) \in X_m$. De fato,

$$\begin{aligned} m + s(n) &:= s(m + n) = s\left(s^n(m)\right) \\ &= s \circ s^n(m) =: s^{s(n)}(m), \end{aligned}$$

onde na segunda igualdade acima usamos a hipótese de indução. Logo, $s(n) \in X_m$. Assim, pelo Princípio da Indução , $X_m = \mathbb{N}$. Isto conclui a prova da proposição em questão. □

Vejamos alguns exemplos de como aplicar a definição de soma dada na Proposição 1.2.

Exemplo 1.1. É fácil ver que os itens abaixo são válidos:

i) $2 + 5 = s^5(2) = s(s(s(s(2)))) = s(s(s(3))) = s(s(4)) = s(5)) = s(6) = 7$;

ii) $13 + 10 = s^{10}(13) = \underbrace{s \circ s \circ ... \circ s}_{10 \text{ vezes}}(13) = 23$.

Ainda precisamos provar a propriedade associativa[5] (ver Teorema 1.3 abaixo) para garantir que a comutatividade entre números naturais, com relação à adição, é válida.

Teorema 1.3 (Associatividade)**.** *Sejam $m, n, p \in \mathbb{N}$. Então, $m + (n + p) = (m + n) + p$.*

Demonstração. Fixaremos os naturais m e n e aplicaremos indução sobre p. Sendo assim, considere o conjunto

$$X_{m,n} = \{p \in \mathbb{N} / m + (n + p) = (m + n) + p\}.$$

É fácil ver que $0 \in X_{m,n}$, pois

$$m + (n + 0) := m + n = (m + n) + 0,$$

ver (1.1). Mostraremos agora que o fato de $k \in X_{m,n}$ acarreta que $s(k) \in X_{m,n}$. Com efeito, seja $k \in X_{m,n}$. Então, $m+(n+k) = (m+n)+k$. Por conseguinte, através do uso de (1.1), encontramos

$$\begin{aligned} m + (n + s(k)) &:= m + s(n + k) \\ &:= s(m + (n + k)) \\ &= s((m + n) + k) \\ &= (m + n) + s(k). \end{aligned}$$

Logo, $s(k) \in X_{m,n}$. Portanto, $X_{m,n} = \mathbb{N}$. Isto prova o teorema em questão. □

Agora, vamos provar que a adição entre números naturais é comutativa. Começaremos mostrando, através de uma caracterização bem conhecida de um sucessor, que qualquer número natural comuta com 1.

[5] A igualdade dada no Teorema 1.3 nos diz que a adição é associativa.

Lema 1.1. *Seja $m \in \mathbb{N}$. Então, $s(m) = m + 1$ e $s(m) = 1 + m$. Em particular, $m + 1 = 1 + m$.*

Demonstração. Para a primeira igualdade acima, temos

$$m + 1 = m + s(0) = s(m + 0) = s(m).$$

Já a prova da segunda igualdade provém de uma aplicação do Princípio da Indução ao conjunto

$$X = \{m \in \mathbb{N} / s(m) = 1 + m\}.$$

Claramente, $0 \in X$, pois $s(0) = 1 = 1 + 0$ (ver (1.1)). Seja $m \in X$. Vamos mostrar que $s(m) \in X$. De fato, como $s(m) = 1 + m$ ($m \in X$), temos que

$$1 + s(m) = s(1 + m) = s(s(m)),$$

ou seja, $s(m) \in X$. Assim, pelo Princípio da Indução, temos $X = \mathbb{N}$. Em particular,

$$m + 1 = s(m) = 1 + m, \forall m \in \mathbb{N}.$$

□

Agora, estamos prontos para provar a comutatividade[6], com relação à adição, entre dois números naturais.

Teorema 1.4 (Comutatividade)**.** *Sejam $m, n \in \mathbb{N}$. Então, $n + m = m + n$.*

Demonstração. Fixando arbitrariamente $m \in \mathbb{N}$ e considere o conjunto

$$X_m = \{n \in \mathbb{N} / n + m = m + n\}.$$

Mostremos por indução sobre n que $X_m = \mathbb{N}$.

Inicialmente, mostraremos que $m + 0 = 0 + m$. Note que $m + 0 = m$, por (1.1). Sendo assim, é suficiente mostrar que $m = 0 + m$. Para este fim, assuma que

$$X = \{m \in \mathbb{N} / m = 0 + m\}.$$

Provaremos que $X = \mathbb{N}$. É fácil ver que $0 \in X$, pois $0 = 0 + 0$ (ver (1.1)). Agora suponha que $m \in X$. Logo, $m = 0 + m$. Por conseguinte, inferimos

[6] A igualdade exposta no Teorema 1.4 nos diz que a adição é comutativa.

$$0 + s(m) := s(0 + m) = s(m).$$

Deste modo, $s(m) \in X$. Portanto, $X = \mathbb{N}$. Logo, $m + 0 = m = 0 + m$.

Agora estamos aptos a provar que $X_m = \mathbb{N}$. Vimos acima que $0 \in X_m$. Por outro lado, assumindo o fato de que $n \in X_m$ e aplicando o Lema 1.1 e o Teorema 1.3, obtemos

$$\begin{aligned} m + s(n) =: s(m + n) &= (m + n) + 1 \\ &= 1 + (m + n) = 1 + (n + m) \\ &= (1 + n) + m = (n + 1) + m \\ &:= s(n) + m. \end{aligned}$$

Portanto, $X_m = \mathbb{N}$. Isto completa a prova do teorema em questão. □

O resultado a seguir nos mostra que a lei de cancelamento para a adição[7], definida sobre o conjunto dos números naturais, é válida.

Teorema 1.5 (Lei do Cancelamento)**.** *Sejam $m, n, p \in \mathbb{N}$. Então, vale a seguinte implicação: $m + p = n + p \Rightarrow m = n$.*

Demonstração. Fixe $m, n \in \mathbb{N}$ e considere o conjunto

$$X_{m,n} = \{p \in \mathbb{N} / m + p = n + p \Rightarrow m = n\}.$$

Apliquemos indução sobre p para mostrar que $X_{m,n} = \mathbb{N}$. É fácil ver que se $m + 0 = n + 0$, então, por (1.1), temos que

$$m = m + 0 = n + 0 = n.$$

Isto nos diz que $0 \in X_{m,n}$. Suponhamos, agora, que $p \in X_{m,n}$ e

$$m + s(p) = n + s(p).$$

Deste modo,

$$s(m + p) = s(n + p).$$

Consequentemente, como s é injetiva, chegamos a $m + p = n + p$. Como $p \in X_{m,n}$, então $m = n$. Por fim, pelo Princípio da Indução, concluímos $X_{m,n} = \mathbb{N}$. Isto completa a prova do teorema em questão. □

[7] A implicação estabelecida no Teorema 1.5 nos diz que a lei do cancelamento para a adição é válida.

A seguir, provaremos que o elemento neutro da adição do naturais é único.

Proposição 1.3. *Suponha que exista $u \in \mathbb{N}$ tal que $m + u = m$ (ou $u + m = m$) para todo $m \in \mathbb{N}$. Então, $u = 0$.*

Demonstração. Se $m + u = m$, para todo $m \in \mathbb{N}$, então, assumindo $m = 0$, chegamos a

$$0 = 0 + u =: u,$$

por (1.1). Isto prova a proposição em questão. □

1.2.2 Propriedades Elementares da Multiplicação

Nesta subseção, definiremos a multiplicação envolvendo números naturais juntamente com algumas propriedades elementares relacionadas a esta operação.

Definição 1.5. *Definimos a aplicação $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, denominada multiplicação, que associa dois números naturais m e n a um outro $m \cdot n$, do seguinte modo:*

$$\begin{cases} m \cdot 0 = 0; \\ m \cdot (n + 1) = m \cdot n + m. \end{cases} \tag{1.2}$$

Adiante, em alguns momentos oportunos, adotaremos a notação de justaposição para multiplicação, isto é,

$$m \cdot n = mn, \forall m, n \in \mathbb{N}.$$

Exemplo 1.2. É fácil ver que:

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

Proposição 1.4. *A multiplicação está bem definida, isto é, $m \cdot n \in \mathbb{N}$ para todo $m, n \in \mathbb{N}$.*

Demonstração. Sejam $m, n \in \mathbb{N}$, com m fixo. Consideremos o conjunto

$$X_m = \{n \in \mathbb{N} / m \cdot n \in \mathbb{N}\}.$$

É fácil checar que $0 \in X_m$, pois $m \cdot 0 = 0 \in \mathbb{N}$ (ver (1.2)). Agora, assuma que $n \in X_m$ em ordem a provar que $s(n) \in X_m$. Assim sendo, pelo Lema 1.1, concluímos que

$$m \cdot s(n) = m \cdot (n+1) := m \cdot n + m \in \mathbb{N},$$

pois $n \in X_m$ ($m \cdot n \in \mathbb{N}$). Portanto, pelo Princípio da indução, $X_m = \mathbb{N}$. □

A seguir apresentaremos algumas propriedades elementares envolvendo a multiplicação entre números naturais. Entre estas, permita-nos mostrar que 1 é o elemento neutro[8] desta operação.

Teorema 1.6 (Elemento Neutro)**.** *Seja $n \in \mathbb{N}$. Então, $1 \cdot n = n \cdot 1 = n$.*

Demonstração. Mostraremos inicialmente que $n \cdot 1 = n$. Com efeito, usando (1.1), (1.2) e o Teorema 1.4, segue que

$$n \cdot 1 = n \cdot (0+1) = n \cdot 0 + n = 0 + n = n.$$

Agora por indução em n, mostraremos que $1 \cdot n = n$. Seja

$$X = \{n \in \mathbb{N} / 1 \cdot n = n\}.$$

É fácil ver que $1 \cdot 0 = 0 \in X$, por (1.2). Suponha, agora, que $n \in X$. Logo, $1 \cdot n = n$. Consequentemente, obtemos

$$1 \cdot (n+1) = 1 \cdot n + 1 = n + 1.$$

Deste modo, $n + 1 \in X$. Por fim, o resultado segue pelo Princípio de Indução. □

O corolário a seguir nos mostra que o elemento neutro da multiplicação, assim como o da adição, entre números naturais é único.

Corolário 1.7. *Seja $p \in \mathbb{N}$ tal que $n \cdot p = n$ (ou $p \cdot n = n$) para todo $n \in \mathbb{N}^*$. Então, $p = 1$.*

Demonstração. Assuma que $n = 1 \in \mathbb{N}^*$ (ver Teorema 1.1) em ordem a obter

$$1 = 1 \cdot p = p,$$

onde na última igualdade aplicamos o Teorema 1.6. Isto mostra que $1 = p$. □

[8] Um elemento 1 de um conjunto A, com uma operação de multiplicação definida, é chamado de elemento neutro se $a \cdot 1 = 1 \cdot a = a$, para todo $a \in A$.

Usando as definições dadas em (1.1) e (1.2), vamos mostrar uma propriedade envolvendo números naturais conhecida como distributividade[9].

Teorema 1.8 (Distributividade)**.** *Sejam* $m, n, p \in \mathbb{N}$. *Então,* $m \cdot (n + p) = m \cdot n + m \cdot p$ *e* $(m + n) \cdot p = m \cdot p + n \cdot p$.

Demonstração. Assuma que m e n estão fixos e considere o conjunto

$$X_{m,n} = \{p \in \mathbb{N} / m \cdot (n + p) = m \cdot n + m \cdot p\}.$$

Vamos provar que $X_{m,n} = \mathbb{N}$ por indução sobre p. Primeiramente, é fácil checar que

$$m(n + 0) := mn =: mn + 0 =: mn + n0,$$

por (1.1) e (1.2). Logo, $m(n + 0) = mn + m0$. Assim, $0 \in X_{m,n}$. Mostraremos que se $p \in X_{m,n}$ acarreta que $p + 1 \in X_{m,n}$. Com efeito, assumindo que $p \in X_{m,n}$ (isto é, $m(n + p) = mn + mp$), chegamos a

$$\begin{aligned} m(n + s(p)) &= m(n + (p + 1)) = m((n + p) + 1) \\ &= m(n + p) + m = (mn + mp) + m \\ &= mn + (mp + m) = mn + m(p + 1) \\ &= mn + ms(p), \end{aligned}$$

onde aplicamos o Lema 1.1, o Teorema 1.3 e (1.2). Deste modo, $s(p) \in X_{m,n}$. Com isso, concluímos, pelo Princípio da Indução, que $X_{m,n} = \mathbb{N}$. Isto prova que a primeira igualdade exposta no Teorema em questão.

De forma similar , usando indução sobre p, prova-se que $(m + n) \cdot p = m \cdot p + n \cdot p$. De fato, seja

$$Y_{m,n} = \{p \in \mathbb{N} / (m + n) \cdot p = m \cdot p + n \cdot p\}.$$

É fácil ver que $0 \in Y_{m,n}$, pois

$$(m + n)0 = 0 = 0 + 0 = m0 + n0.$$

[9] A igualdade dada no Teorema 1.8 nos diz que a propriedade distributiva é válida.

Por outro lado, se $p \in Y_{m,n}$, então $(m+n)p = mp + np$. Consequentemente,

$$\begin{aligned}(m+n)s(p) &= (m+n)(p+1) = (m+n)p + (m+n)\\ &= (mp+np) + (m+n) = (mp+m) + (np+n)\\ &= m(p+1) + n(p+1) = ms(p) + ns(p).\end{aligned}$$

Logo, $s(p) \in Y_{m,n}$. Concluímos, pelo Princípio da Indução, que $Y_{m,n} = \mathbb{N}$. □

Permita-nos provar a propriedade associativa[10] para a multiplicação de números naturais como segue.

Teorema 1.9 (Associatividade)**.** *Sejam $m, n, p \in \mathbb{N}$. Então, $m \cdot (n \cdot p) = (m \cdot n) \cdot p$.*

Demonstração. Fixe $m, n \in \mathbb{N}$.Considere que

$$X_{m,n} = \{p \in \mathbb{N} / m(np) = (mn)p\}.$$

Mostraremos que $X_{m,n} = \mathbb{N}$, por indução. Inicialmente, é fácil ver que $0 \in X_{m,n}$, pois

$$m(n0) = m0 = 0 = (mn)0.$$

Agora, suponha que $p \in X_{m,n}$ (ou seja, $m(np) = (mn)p$). Então,

$$\begin{aligned}m(ns(p)) &= m[n(p+1)] = m(np+n)\\ &= m(np) + mn = (mn)p + (mn)\\ &= (mn)(p+1) = (mn)s(p),\end{aligned}$$

onde aplicamos o Lema 1.1 e (1.2). Deste modo, $s(p) \in X_{m,n}$. Portanto, pelo Princípio da Indução, $X_{m,n} = \mathbb{N}$. O teorema em questão segue.

□

Agora, vamos provar que o conjunto dos números naturais não possui divisores de zero[11]. Para este fim, demonstraremos inicialmente o seguinte resultado:

Lema 1.2. *Sejam $m, n \in \mathbb{N}$. Então, $m + n = 0 \Rightarrow m = n = 0$.*

[10] A igualdade dada no Teorema 1.9 nos diz que a associatividade para a multiplicação é válida.

[11] Um conjunto A, com uma multiplicação estabelecida, é dito não conter divisores de zero se $x \cdot y = 0$, com $x, y \in A$, implicar $x = 0$ ou $y = 0$.

Demonstração. Suponhamos, por absurdo, que $n \neq 0$. Então,

$$n = s(n') = n' + 1, \text{ para algum } n' \in \mathbb{N},$$

pelos Teorema 1.1 e Lema 1.1. Consequentemente, pelo Teorema 1.3, chegamos a

$$0 = m + n = m + (n' + 1) = (m + n') + 1 = s(m + n'),$$

pelo Lema 1.1 novamente. Isto é um absurdo, pois zero não é sucessor de nenhum número (ver Teorema 1.1). Logo, $n = 0$. Dessa forma, concluímos

$$0 = m + n = m + 0 = m.$$

Isto completa a prova do lema em questão. □

Vejamos agora como utilizar o Lema 1.2 para provar que só existe uma maneira para que a multiplicação entre dois números naturais resulte em 0: pelo menos um deste elementos tem que ser 0.

Teorema 1.10. *Sejam $m, n \in \mathbb{N}$. Então, $\mathbb{N}$ não possui divisores de zero, isto é, $m \cdot n = 0 \Rightarrow m = 0$ ou $n = 0$.*

Demonstração. Suponhamos que $n \neq 0$. Assim, sendo, temos que

$$n = s(k) = k + 1, \text{ para algum } k \in \mathbb{N},$$

ver Teorema 1.1 e Lema 1.1. Segue que

$$0 = mn = m(k + 1) = mk + m,$$

ver (1.2). Logo, pelo Lema 1.2, obtemos $m = 0$. □

Para finalizar esta subseção, mostraremos que a multiplicação entre números naturais, assim como a adição, é uma operação comutativa[12]. Este fato está verificado no teorema a seguir.

Teorema 1.11 (Comutatividade)**.** *Sejam $m, n \in \mathbb{N}$. Então, $n \cdot m = m \cdot n$.*

[12] A igualdade dada no Teorema 1.11 nos diz que a propriedade comutativa para a multiplicação é válida.

Demonstração. Primeiramente, vamos mostrar que $0m = 0 \forall m \in \mathbb{N}$. Seja $X = \{m \in \mathbb{N}/0 \cdot m = 0\}$. Vamos provar por indução que $X = \mathbb{N}$. Note que, por (1.2), $0 \cdot 0 = 0$. Logo, $0 \in X$. Agora, suponha que $m \in X$. Daí, $0m = 0$. Dessa forma,

$$0s(m) = 0(m + 1) = 0m + 0 = 0 + 0 = 0,$$

ver Lema 1.1. Isto nos diz que $s(m) \in X$. Logo, $X = \mathbb{N}$.

Agora, fixemos $m \in \mathbb{N}$ natural arbitrariamente e apliquemos indução sobre n ao conjunto

$$X_m = \{n \in \mathbb{N}/m \cdot n = n \cdot m\}.$$

Temos que $0 \in X_m$, pois $m0 = 0 = 0m$ (ver argumentação acima). Considere que $n \in X_m$ (isto é, $mn = nm$). Deste modo, pelos Teoremas 1.6 e 1.8, encontramos

$$ms(n) = m(n + 1) = mn + m = nm + 1m = (n + 1)m = s(n)m.$$

Isto mostra que $s(n) \in X_m$. Portanto, pelo Princípio da Indução, $X_m = \mathbb{N}$. □

1.3 Relação de Ordem e Potências em $\mathbb{N}$

Nesta seção, faremos um estudo, envolvendo números naturais, que nos proporcionará comparar os números naturais com a bem conhecida ideia elementar quando um elemento é menor (ou maior) que o outro; formalizando, assim, a ideia intuitiva de que 0 é menor que 1, 1 é menor do que 2, e assim por diante. Por fim, mostraremos como definir potências de números naturais.

Comecemos com a definição de uma relação de ordem em um conjunto qualquer.

Definição 1.6. Seja X um conjunto não vazio. Dizemos que uma relação binária R é uma relação de ordem em X quando esta satisfizer as condições seguintes, para quaisquer $x, y, z \in X$:

i) [Reflexividade]: xRx;

ii) [Antissimetria]: xRy e $yRx \Rightarrow x = y$;

iii) [Transitividade]: xRy e $yRz \Rightarrow xRz$.

O par (X, R) é chamado um conjunto ordenado. Quando não houver possibilidade de confusão com a relação de ordem R, diremos que X é um conjunto ordenado.

Exemplo 1.3. Sejam $m, n \in \mathbb{N}$. Defina uma relação R da seguinte forma:

$$mRn \text{ se existe } p \in \mathbb{N} \text{ tal que } n = m + p.$$

Mostraremos que R é uma relação de ordem em $\mathbb{N}$. De fato,

i) R é reflexiva, pois $m = m + 0$ $(\Rightarrow mRm)$;

ii) Se mRn e nRm, então $n = m + p$ e $m = n + q$ para alguns $p, q \in \mathbb{N}$. Substituindo a primeira igualdade na segunda, e usando associatividade, obtemos

$$m = n + q = (m + p) + q = m + (p + q).$$

Logo, pela lei do cancelamento, encontramos $p + q = 0$. Portanto, pelo Lema 1.2, chegamos a $p = q = 0$. Deste modo, $n = m$. Isto nos diz que R é antissimétrica;

iii) Por fim, se $r \in \mathbb{N}$, mRn e nRr, então $n = m+p'$ e $r = n+q'$ para alguns $p', q' \in \mathbb{N}$. Substituindo a primeira igualdade na segunda, e aplicando a associatividade, obtemos

$$r = (m + p') + q = m + (p' + q').$$

Portanto, mRr. Isto nos informa que R é transitiva.

A relação R, definida em $\mathbb{N}$, do exemplo anterior nos possibilita informar quando um número natural é menor do que ou igual outro.

Definição 1.7. Sejam $n, m \in \mathbb{N}$. Dizemos que n é menor do que ou igual a m, e escreveremos $n \leq m$, se existe $p \in \mathbb{N}$ tal que $m = n + p$.

Vimos, no exemplo acima, que $\leq$ é uma relação de ordem em $\mathbb{N}$.

Obs 1.2. Neste texto, também utilizaremos as seguintes notações:

1. Se $n \leq m$ e $n \neq m$, então escreveremos $n < m$ e dizemos que n é menor do que m;
2. Escreveremos $n \geq m$, como alternativa a $m \leq n$. Leremos n é maior do que ou igual a m;
3. Escreveremos $n > m$, como alternativa a $m < n$. Leremos n é maior do que m.

Obs 1.3. É fato que se $n < m$, com $n, m \in \mathbb{N}$, então existe $p \in \mathbb{N}$ tal que $m = n + p$ e $n \neq m$. Como $p \neq 0$ (caso contrário, teríamos $n = m$), então $m = n + p$, onde $p \in \mathbb{N}^*$. Reciprocamente, se $m = n + p$ com $p \in \mathbb{N}^*$, tem-se que $n \leq m$ e $p \neq 0$. Se $n = m$, teríamos $n = n + p$. Pela lei do cancelamento, encontraríamos $p = 0$ (um absurdo). Dessa forma, resumindo, podemos caracterizar a relação $<$ da seguinte forma:

$$n < m \Leftrightarrow m = n + p, \text{com } p \in \mathbb{N}^*.$$

Exemplo 1.4. É fácil ver, através da Definição 1.7 que:

i) $0 < 1$, pois $1 = 0 + 1$ e $0 \neq 1$;

ii) $3 \leq 5$, já que $5 = 3 + 2$;

O exemplo anterior nos informa que $1 > 0$. Na verdade, qualquer número natural diferente de 0 é maior do que 0. Mais precisamente, apresentamos a seguinte proposição.

Proposição 1.5. *Seja $n \in \mathbb{N}^*$. Então, $n > 0$.*

Demonstração. Suponhamos, por absurdo, que $n < 0$. Então, pela Definição 1.7, existe $p \in \mathbb{N}$ tal que $0 = n + p$. Assim sendo, aplicando o Lema 1.2, obtemos que $n = 0$. Isto é uma contradição, pois $n \in \mathbb{N}^*$. Portanto, $n > 0$. □

Agora, estamos aptos a provar que o sucessor de qualquer número natural é estritamente maior do que ele próprio.

Proposição 1.6. *Seja $n \in \mathbb{N}$. Então, $s(n) > n$.*

Demonstração. Sabemos do Lema 1.1 que $s(n) = n + 1$, para qualquer $n \in \mathbb{N}$. Portanto, por definição, $s(n) > n$, para todo $n \in \mathbb{N}$ (pois $1 \neq 0$). □

Obs 1.4. Poderíamos estabelecer uma prova da proposição acima usando indução. De fato, considere o conjunto

$$X = \{n \in \mathbb{N} / s(n) > n\}.$$

Note que $0 \in X$, pois $s(0) = 1 > 0$. Agora, se assumirmos que $n \in X$ $(s(n) > n)$, obtemos

$$s(n + 1) = (n + 1) + 1 = s(n) + 1.$$

Como $s(n) > n$, temos que existe $p \in \mathbb{N}$ tal que $s(n) = n + p$. Dessa forma, pela associatividade, chegamos a

$$s(n) + 1 = (n + p) + 1 = n + (p + 1) = n + (1 + p) = (n + 1) + p.$$

Portanto, $s(n + 1) > n + 1$. Deste modo, $s(n) \in X$. Por fim, pelo Princípio da Indução, $X = \mathbb{N}$.

O resultado a seguir nos mostra que é sempre possível comparar dois números naturais através da Definição 1.7. Mais precisamente, temos o seguinte teorema.

Teorema 1.12 (Lei da Tricotomia)**.** *Sejam $m, n \in \mathbb{N}$. Então, somente uma das relações abaixo ocorre:*

i) $m < n$*;*

ii) $m = n$*;*

iii) $m > n$.

Demonstração. Inicialmente, suponha, por absurdo, que **i)** e **ii)** valem simultaneamente. Assim, $m < n$ e $m = n$. Então $n = m + p = n + p$, para algum $p \in \mathbb{N}^*$. Logo, pela lei do cancelamento, encontramos $p = 0$. Isto é uma contradição, visto que $p \in \mathbb{N}^*$. De forma análoga, verifica-se que **ii)** e **iii)** são incompatíveis.

Agora, suponhamos que **i)** e **iii)** ocorrem ao mesmo tempo. Dessa forma, teríamos

$$n = m + p \text{ e } m = n + q,\ p, q \in \mathbb{N}^*.$$

Consequentemente,

$$n = m + p = (n + q) + p = n + (q + p).$$

Portanto, novamente pela lei do cancelamento, obteríamos $q + p = 0$. Por aplicar o Lema 1.2, chegaríamos a $p = q = 0$ (contradição).

Mostraremos agora que uma as três relações acontece. Sendo assim, primeiramente, fixe $m \in \mathbb{N}$ e considere o conjunto

$$X_m = \{n \in \mathbb{N} / n = m \text{ ou } n > m \text{ ou } n < m\}.$$

Vamos provar por indução sobre n, que $X_m = \mathbb{N}$. É fácil checar que $0 \in X_m$, pois, pela Proposição 1.5, $0 = m$ ou $m > 0$. Assuma que $k \in X_m$ ($k = m$ ou $k > m$ ou $k < m$). Assim, devemos considerar três situações:

1ª) $k = m$.

Neste caso, $k + 1 = m + 1$. Logo, $k + 1 > m$ e, portanto, $s(k) = k + 1 \in X_m$;

2ª) $k > m$.

Neste caso, existe $p \in \mathbb{N}^*$ tal que $k = m + p$. Então, por associatividade, chegamos a

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

Com isso, $k + 1 > m$. Daí, $s(k) = k + 1 \in X_m$;

3ª) $k < m$.

Neste caso, existe $p \in \mathbb{N}^*$ tal que $m = k + p$. Daí, como $p = s(j) = j + 1$, para algum $j \in \mathbb{N}$, tem-se que

$$m = k + p = k + (j + 1) = k + (1 + j) = (k + 1) + j.$$

Se $j = 0$, então $s(k) = k + 1 = m$ e consequentemente $s(k) \in X_m$ (pois $m \in X_m$). Se $j \neq 0$, então $m > k + 1 = s(k)$. Por fim, $s(k) \in X_m$.

Isto completa a prova do teorema em questão. □

A lei da tricotomia, estabelecida acima, equivale dizer que, dados $m, n \in \mathbb{N}$, tem-se, necessariamente, que $m \leq n$ ou $n \leq m$. Isto nos diz que dois naturais quaisquer são sempre comparáveis pela relação de ordem $\leq$. Por isso, dizemos que $\leq$ é uma relação de ordem total e; neste caso, $\mathbb{N}$, munido deste relação, é dito ser totalmente ordenado.

Proposição 1.7. *A relação $<$, definida em $\mathbb{N}$ não é uma relação de ordem; porém, esta é transitiva e antissimétrica.*

Demonstração. Suponhamos que $<$ é reflexiva. Então, teríamos $n < n$, para todo $n \in \mathbb{N}$. Isto é uma contradição, já que $n = n$ (ver Teorema 1.12).

Mostraremos que $<$ é transitiva. De fato, se $m < n$ e $n < p$, então existem $q, r \in \mathbb{N}^*$ tais que $n = m + q$ e $p = n + r$. Segue que,

$$p = n + r = (m + q) + r = m + (q + r),$$

onde $q + r \neq 0$; caso contrário, $q = r = 0$ (ver Lema 1.2). Logo, $m < p$. Isto nos informa que $<$ é transitiva.

Por fim, por vacuidade, se $m \neq n$ então $m < n$ ou $n < m$, pela tricotomia. Isto nos diz que a antissimetria é satisfeita por $<$. □

É importante notar que, a proposição anterior pode ser reformulada com a relação $>$ no lugar de $<$.

Agora vamos estabelecer um resultado que apresenta de que maneira podemos utilizar a relação de ordem $\leq$ juntamente com as operações de adição e multiplicação entre números naturais.

Teorema 1.13. *Sejam $m, n, p \in \mathbb{N}$. Então, são válidas as seguintes afirmações:*

i) $n \leq m \Leftrightarrow n + p \leq m + p$;

ii) $n \leq m \Rightarrow np \leq mp$. *A recíproca é verdadeira se $p \in \mathbb{N}^*$.*

Demonstração. **i)** ($\Rightarrow$) Se $n \leq m$, então existe $p' \in \mathbb{N}$ tal que $m = n + p'$. Segue que,

$$m + p = (n + p') + p = n + (p' + p) = n + (p + p') = (n + p) + p'.$$

De onde, obtemos $n + p \leq m + p$.

($\Leftarrow$) Reciprocamente, considere que $n + p \leq m + p$. Então, $m + p = (n + p) + d$ para algum $d \in \mathbb{N}$. Daí,

$$m + p = (n + p) + d = n + (p + d) = n + (d + p) = (n + d) + p.$$

Pela lei do cancelamento, chegamos a $m = n + d$. Logo, $n \leq m$.

ii) ($\Rightarrow$) Assuma que $n \leq m$, então existe $q \in \mathbb{N}$ tal que $m = n + q$. Multiplicando ambos os lados da igualdade por p, obtemos

$$mp = (n + q)p = np + qp.$$

Portanto, $np \leq mp$.

($\Leftarrow$) Pela lei da tricotomia, se $n \nleq m$ então $n > m$. Logo, $n = m + d$, para algum $d \in \mathbb{N}^*$. Multiplicando ambos os lados da igualdade por $p \in \mathbb{N}^*$, obtemos

$$np = (m + d)p = mp + dp.$$

Portanto, $mp < np$, pois $dp \in \mathbb{N}^*$.

□

Obs 1.5. A reformulação do teorema acima para a relação $\geq$ segue passos análogos aos da prova estabelecida acima.

Vejamos como reescrever o teorema acima substituindo a relação de ordem $\leq$ por $<$.

Proposição 1.8. *Sejam $n, m, p \in \mathbb{N}$. Então, são válidas as seguintes afirmações:*

i) $n < m \Leftrightarrow n + p < m + p$;

ii) $n < m \Leftrightarrow np < mp$, *fornecido que* $p \neq 0$.

Demonstração. **i)** ($\Rightarrow$) Se $n < m$ então existe $p' \in \mathbb{N}^*$ tal que $m = n + p'$. Segue que,

$$m + p = (n + p') + p = n + (p' + p) = n + (p + p') = (n + p) + p'.$$

De onde obtemos $n + p < m + p$.

($\Leftarrow$) Reciprocamente, assuma que $n + p < m + p$. Sendo assim, $m + p = (n + p) + d$, para algum $d \in \mathbb{N}^*$. Daí,

$$m + p = (n + p) + d = n + (p + d) = n + (d + p) = (n + d) + p.$$

Pela lei do cancelamento, chegamos a $m = n + d$ com $d \neq 0$. Por fim, $n < m$.

ii) ($\Rightarrow$) Se $n < m$ então existe $q \in \mathbb{N}^*$ tal que $m = n + q$. Multiplicando ambos os lados desta igualdade, por p, obtemos

$$mp = (n + q)p = np + qp.$$

Como $p, q \neq 0$, então $qp \neq 0$. Assim, temos que $np < mp$.

($\Leftarrow$) Pela lei da tricotomia, se $n \not< m$, então $n \geq m$. Logo, pelo Teorema 1.13, concluímos que $np \geq mp$.

Isto conlcui a prova da proposição em questão. □

Obs 1.6. A demostração da proposição anterior para a relação $>$ é análoga a que fizemos.

A seguir, provaremos que a lei do cancelamento para a multiplicação[13] de números naturais, assim como para a adição, é válida. Mais precisamente, temos o seguinte resultado.

Teorema 1.14 (Lei do Cancelamento)**.** *Sejam $n, m, p \in \mathbb{N}$, com $p \neq 0$. Então, $np = mp \Rightarrow n = m$.*

Demonstração. Suponha, por absurdo, que $n \neq m$. Então, pela tricotomia, temos que $n < m$ ou $m < n$. Assim sendo, se $n < m$, teríamos $np < mp$ (ver Proposição 1.8). Por outro lado, se $m < n$, teríamos $mp < np$ (ver Proposição 1.8). Isto prova o teorema em questão. □

O resultado a seguir tem como uma de suas aplicações a prova de que o único elemento inversível de $\mathbb{N}$ é 1.

Proposição 1.9. *Sejam $n, m \in \mathbb{N}$. Então, $n < m \Leftrightarrow n + 1 \leq m$.*

Demonstração. ($\Rightarrow$) Considere que $n < m$ então $m = n + p$, para algum $p \in \mathbb{N}^*$. Sabemos que, $p = s(c) = c + 1$, para um certo $c \in \mathbb{N}$. Dessa forma, concluímos que

$$m = n + p = n + (c + 1) = n + (1 + c) = (n + 1) + c.$$

Consequentemente, chegamos a $n + 1 \leq m$.

($\Leftarrow$) Se $n + 1 \leq m$, então

$$n < s(n) = n + 1 \leq m.$$

Portanto, por transitividade, encontramos $n < m$. □

O resultado abaixo nos mostra que o único número natural que possui inverso multiplicativo[14] é 1, o qual é dado pelo próprio 1. Mais especificamente, temos a seguinte proposição.

Proposição 1.10. *Sejam $n, m \in \mathbb{N}$ tais que $nm = 1$, então $n = m = 1$.*

Demonstração. Note que se $nm = 1$, então $n, m \neq 0$ (caso contrário, $nm = 0$). Dessa forma, temos que $0 < n, m$ (ver Proposição 1.5). Com isso, concluímos que $1 \leq n, m$ (ver Proposição 1.9).

[13] A implicação dada no Teorema 1.14 nos diz que a lei do cancelamento para a multiplicação é válida.

[14] Seja A um conjunto, com uma multiplicação definida, dizemos que $b \in A$ é inverso de $a \in A$ se $a \cdot b = b \cdot a = 1$.

Suponha, por contradição que $1 < n$ (ou seja, que $n \neq 1$). Logo, pela Proposição 1.8, inferimos

$$m = m1 < mn = nm = 1.$$

Isto é um absurdo, pois $m \geq 1$ (ver tricotomia). Por fim, $n = 1$. Consequentemente,

$$m = 1m = nm = 1.$$

□

Agora, vamos mostrar que a soma de dois números naturais resulta em 1 se, e somente se, um deles é 0 e o outro é 1.

Proposição 1.11. *Sejam $n, m \in \mathbb{N}$ números naturais. Então, $n + m = 1 \Rightarrow n = 1$ e $m = 0$ ou $m = 1$ e $n = 0$.*

Demonstração. Suponhamos $n \neq 0$, então $n = s(a) = a + 1$, para algum $a \in \mathbb{N}$. Segue, daí, que

$$1 = n + m = (a + 1) + m = (1 + a) + m = 1 + (a + m).$$

Logo, pela lei do cancelamento, chegamos a $a + m = 0$. Assim, pela Proposição 1.2, encontramos $a = m = 0$. Portanto, $n = 0 + 1 = 1$ e $m = 0$. Por outro lado, se $n = 0$, então $m = 0 + m = 1$. Assim, $n = 0$ e $m = 1$. □

Já sabemos que $0+2 = 2+0 = 2$. Vamos mostrar agora que a única outra maneira de somarmos dois naturais resultando em 2 é somando 1 a ele próprio.

Proposição 1.12. *Sejam $n, m \in \mathbb{N}$. Então, $nm \neq 0$ e $n + m = 2 \Rightarrow n = m = 1$.*

Demonstração. Note que, $n \neq 0$ e $m \neq 0$ (pois $nm \neq 0$). Então, $n = s(a) = a+1$ e $m = s(b) = b+1$ para alguns $a, b \in \mathbb{N}$. Daí, segue que

$$2 = n + m = (a + 1) + (b + 1) = (a + 1) + (1 + b) = (a + 2) + b = (2 + a) + b = 2 + (a + b).$$

Assim, pela lei do cancelamento, encontramos $a + b = 0$. Logo, pela Proposição 1.2, temos que $a = b = 0$. Portanto, $n = 0 + 1 = 1$ e $m = 0 + 1 = 1$. □

A seguir, provaremos que a multiplicação entre dois números naturais não nulos é maior do que ou igual a qualquer um de seus fatores.

Proposição 1.13. *Sejam $n, m \in \mathbb{N}$. Então, $nm \neq 0 \Rightarrow n \leq nm$.*

Demonstração. Se $nm \neq 0$, então $n, m \neq 0$. Logo, $n, m > 0$ (ver Proposição 1.5). Daí $1 \leq n, m$ (ver Proposição 1.9). Por conseguinte, multiplicando a desigualdade $1 \leq m$ por n, obtemos $n = n1 \leq nm$. □

Vejamos abaixo uma adaptação do Princípio da Indução.

Lema 1.3. *Seja X um subconjunto de $\mathbb{N}$ satisfazendo as afirmações abaixo:*

i) $a \in X$

ii) $n \in X \Rightarrow n + 1 \in X$.

Então, $\{a + m/m \in \mathbb{N}\} \subset X$.

Demonstração. Considere o conjunto

$$Y = \{m \in \mathbb{N}/a + m \in X\}.$$

Mostraremos por indução sobre m que $Y = \mathbb{N}$. Primeiramente, é fácil verificar que $0 \in Y$, pois $a + 0 = a \in X$ (por **i**)). Agora assuma que $m \in Y$. Por conseguinte $a + m \in X$. Portanto, por **ii**), concluímos que $(a+m)+1 \in X$. Logo, pelo Teorema 1.3, chegamos a $a+s(m) = a+(m+1) \in X$. Dessa forma, $s(m) \in Y$. Portanto pelo Princípio da Indução, $Y = \mathbb{N}$. □

Como uma aplicação do Lema acima, provaremos a seguinte proposição.

Proposição 1.14. Seja $n \in \mathbb{N}^*$. Então, $s^n(0) \neq s^k(0)$, para todo $k < n$.

Demonstração. Seja $X = \{n \in \mathbb{N}^*/s^n(0) \neq s^k(0), \forall k < n\}$. Mostraremos, usando o Lema 1.3 que $X = \mathbb{N}^*$. De fato,

i) $1 \in X$, pois $s^1(0) = s(0) = 1 \neq 0 = s^0(0)$;

ii) Seja $n \in X$, ou seja, $s^n(0) \neq s^k(0)$, para todo $k < n$. Mostraremos que $n + 1 \in X$. De fato, aplicando s (ver Teorema 1.1), obtemos

$$s^{n+1}(0) \neq s^{k+1}(0), \forall k < n.$$

O que nos diz que $s^{n+1}(0) \neq s^l(0)$, para todo $1 \leq l \leq n$. Como também $s^{n+1}(0) \neq 0 = s^0(0)$ (ver Teorema 1.1), concluímos que $s^{n+1}(0) \neq s^l(0)$, para todo $l < n+1$. Logo, $n+1 \in X$. Portanto, pelo Lema 1.3, concluímos que $X = \mathbb{N}^*$.

□

Agora vejamos como definir uma potência envolvendo números naturais.

Definição 1.8. Sejam $a, n \in \mathbb{N}$ com $a \neq 0$. Definimos a potência a^n, recursivamente, por

$$a^n = \begin{cases} 1, & \text{se } n = 0; \\ a, & \text{se } n = 1; \\ a^k \cdot a, & \text{se } n > 1, \text{ onde } n = 1 + k \text{ com } k \in \mathbb{N}^*. \end{cases}$$

Aqui a é chamado base da potência e n o expoente.

Exemplo 1.5. É fácil ver que

$$2^3 = 2^2 \cdot 2 = (2 \cdot 2) \cdot 2 = 4 \cdot 2 = 8.$$

Obs 1.7. Podemos checar que $a^n \in \mathbb{N}$, para todo $n \in \mathbb{N}$. De fato, seja $X = \{n \in \mathbb{N} / a^n \in \mathbb{N}\}$. Dessa forma, $0 \in X$, pois $a^0 = 1 \in \mathbb{N}$. Considere que $n \in X$, isto é, $a^n \in \mathbb{N}$. Com isso,

$$a^{s(n)} = a^{n+1} = a^n a \in \mathbb{N},$$

desde que $a^n, a \in \mathbb{N}$. Isto nos informa que $s(n) \in X$. Por indução, concluímos que $X = \mathbb{N}$.

A seguir mostraremos que para realizarmos o produto de potências de mesma base, é suficiente repetir a base e somar os expoentes.

Proposição 1.15. *Sejam $a, m, n \in \mathbb{N}$, tais que $a \neq 0$. Então, $a^{m+n} = a^m \cdot a^n$.*

Demonstração. Fixe $m \in \mathbb{N}$ e considere $X_m = \{n \in \mathbb{N} / a^{m+n} = a^m \cdot a^n\}$. É fácil verificar que

$$a^{m+0} = a^m = a^m \cdot 1 = a^m \cdot a^0.$$

Logo, $0 \in X$. Suponha agora que $n \in X_m$. Assim, $a^{m+n} = a^m \cdot a^n$. Daí,

$$a^{m+s(n)} = a^{m+(n+1)} = a^{(m+n)+1} = a^{m+n} \cdot a = (a^m \cdot a^n) \cdot a = a^m \cdot (a^n \cdot a) = a^m \cdot a^{n+1}.$$

Dessa forma, $s(n) \in X$. Logo, $X = \mathbb{N}$. □

Nosso interesse, agora, é provar que a aplicação $n \mapsto a^n$, onde $a, n \in \mathbb{N}$ e $a > 1$, é bijetora. Para este fim, verificaremos a veracidade dos dois seguintes lemas.

Lema 1.4. *Sejam $a, n \in \mathbb{N}$ tais que $a \neq 0$. Então, $a^n \neq 0$.*

Demonstração. Seja $X = \{n \in \mathbb{N}/a^n \neq 0\}$. É fácil checar que $a^0 = 1 \neq 0$. Logo, $0 \in X$. Suponha que $n \in X$. Assim, $a^n \neq 0$. Portanto,

$$a^{s(n)} = a^{n+1} = a^n \cdot a \neq 0,$$

pois $a \neq 0$ e $a^n \neq 0$. Dessa forma, $s(n) \in X$. Isto nos informa, pelo Princípio da Indução, que $X = \mathbb{N}$. □

Lema 1.5. *Sejam $a, n \in \mathbb{N}$ tais que $a > 1$. Então, $a^n = 1 \Rightarrow n = 0$.*

Demonstração. Suponhamos que $a^n = 1$ e $n \neq 0$. Então, existe $m \in \mathbb{N}$ tal que $n = s(m)$. Isto nos diz que $n = m + 1$. Deste modo, chegamos a

$$1 = a^n = a^{m+1} = a^m a.$$

Portanto, pela Proposição 1.10, obtém-se $a = 1$. Isto contradiz o fato de que $a \neq 1$. □

Como aplicação da proposição acima temos o seguinte corolário. Tal resultado terá papel importante na prova da enumerabilidade de $\mathbb{Q}$.

Corolário 1.15. *Sejam $a, m, n \in \mathbb{N}$ tais que $a > 1$. Então, $a^m = a^n \Rightarrow m = n$.*

Demonstração. Suponha, por absurdo, que $a^m = a^n$ e $m \neq n$. Sem perda de generalidade, podemos supor que $m > n$. Daí, existe $q \in \mathbb{N}^*$ tal que $m = n + q$. Daí, pela Proposição 1.15, chegamos a

$$a^n a^q = a^{n+q} = a^m = a^n.$$

Como $a^n \neq 0$ (ver Lema 1.4), então, pela lei do corte, temos que $a^q = 1$. Portanto, pelo Lema 1.5, obtemos $q = 0$. Isto é um absurdo ($q \in \mathbb{N}^*$). Dessa forma, concluímos que $m = n$. □

Sabemos que $\mathbb{N} = \{0, 1, 2, ...\}$, ou seja, $\mathbb{N}$ é formado por 0 e seus sucessores. Da relação de ordem em $\mathbb{N}$ e suas propriedades, decorre que $0 < 1 < 2 < ....$, isto é, se $n \in \mathbb{N}$, então $n < s(n)$

(pois $0 < 1$ e $s(n) = n + 1$). Além disso, não há naturais compreendidos entre n e $s(n)$, qualquer que seja $n \in \mathbb{N}$; caso contrário, se existisse $r \in \mathbb{N}$ tal que $n < r < n + 1$ teríamos, pelo teorema anterior, que $n + 1 \leq n < n + 1$ (uma contradição pela tricotomia).

Assim, vemos que os Axiomas de Peano e suas consequências cumprem o objetivo de tornar rigoroso o conceito de número natural.

1.4 Princípio da Boa Ordem, Indução na Segunda Forma e Algoritmo da Divisão

Nesta seção, provaremos o Princípio da Boa Ordem por aplicar o axioma do Princípio da Indução. Além disso, mostraremos que, na verdade, este primeiro princípio é equivalente ao segundo. Por fim, exibiremos uma forma alternativa de apresentar o Princípio da Indução, o chamado Segundo Princípio da Indução.

Comecemos caracterizando o que significa elemento mínimo em qualquer conjunto.

Definição 1.9. Seja X um conjunto não vazio. Dizemos que $x_0 \in X$ é um elemento mínimo se $x_0 \leq x$ para todo $x \in X$. A notação deste x_0 é dada por $x_0 = \min X$.

Exemplo 1.6. Note que $\min\{0, 1, 2\} = 0$ e $\min \mathbb{N} = 0$.

O exemplo acima lista dois subconjuntos de $\mathbb{N}$ que possuem elemento mínimo. Na verdade, todo subconjunto de $\mathbb{N}$, exceto o vazio, tem um mínimo.

Teorema 1.16 (Príncipio da Boa Ordem)**.** *Todo subconjunto não vazio de* $\mathbb{N}$ *possui um elemento mínimo.*

Demonstração. Seja X um tal subconjunto de $\mathbb{N}$ e consideremos o conjunto $M = \{n \in \mathbb{N}/n \leqslant x, \forall x \in X\}$. Claro que $0 \in M$, pois $0 \leq x$, para todo $x \in X \subset \mathbb{N}$. Como $X \neq \varnothing$, então existe $y \in X$. Note que $y + 1$ não pertence a M, pois $y + 1 > y$. Sendo assim, podemos concluir que $M \neq \mathbb{N}$. Como $0 \in M$ e $M \neq \mathbb{N}$, deve existir $x_0 \in M$ tal que $x_0 + 1 \notin M$; caso contrário, pelo Princípio da Indução, M deveria ser $\mathbb{N}$. Afirmamos que um tal x_0 é o elemento mínimo de X, isto é, $x_0 = \min X$. Como $x_0 \in M$, então $x_0 \leq x$, para todo $x \in X$. Só falta verificar que $x_0 \in X$. Vamos supor o contrário, que $x_0 \notin X$. Então $x_0 < x$, para todo $x \in X$. Pela Proposição 1.9, teríamos $x_0 + 1 \leq x$, para todo $x \in X$. Como um resultado, segue que $x_0 + 1 \in M$. Isto é uma contradição ($x_0 + 1 \notin M$). Logo $x_0 \in X$. □

Vimos no Teorema 1.16 que o Princípio da Indução pode ser utilizado para provar o Princípio da Boa Ordem. Gostaríamos de ressaltar que a recíproca para esta afirmação é verdadeira e será provada no próximo corolário.

Corolário 1.17 (Princípio da Indução)**.** Seja X subconjunto de $\mathbb{N}$ com as seguintes propriedades:

i) $0 \in X$;

ii) $n \in X \Rightarrow n+1 \in X$.

Então, $X = \mathbb{N}$.

Demonstração. Seja $K = \mathbb{N} \backslash X$. Suponhamos que $X \neq \varnothing$. Então, existe $a = \min K$ (ver Teorema 1.16). Daí, temos que $a \notin X$ ($a \in K$). Além disso, $0 \notin K$ (pois $0 \in X$); dessa forma, $a \neq 0$. Consequentemente, $a = s(b) = b + 1$, com $b \in \mathbb{N}$. Com isso, $b \notin X$; caso contrário, por **ii**), teríamos $a = b + 1 \in X$ (mas, $a \notin X$). Logo, $b \in K$. Por outro lado, $b < s(b) = a$. Isto é um absurdo, por usar a tricotomia. Portanto, $K = \varnothing$. Por fim, $X = \mathbb{N}$. □

Vamos agora enunciar o Segundo Princípio da Indução (também chamado Princípio da Indução na Segunda Forma). Por isso, podemos renomear o Princípio da Indução (ver Axiomas de Peano) como Primeiro Princípio da Indução ou Princípio da Indução na Primeira Forma.

Teorema 1.18 (Segundo Princípio de Indução)**.** Seja $X \subset \mathbb{N}$. Considere as seguintes afirmações são verdadeira:

i) $0 \in X$;

ii) $n \in X$, fornecido que X contém todos os números naturais m tais que $m < n$.

Então, $X = \mathbb{N}$.

Demonstração. Seja $K = \mathbb{N} \backslash X$. Afirmamos que $K = \varnothing$. Com efeito, se K não fosse vazio, existiria $p = \min K$ (ver Teorema 1.16). Por **i**), teríamos que $p \neq 0$ ($0 \in X$ e $p \notin X$). Logo, $p > 0$ (ver Proposição 1.5). Então, para todo número natural $m < p$ (0 seria um desses elementos), teríamos que m não pertenceria a K ($p = \min K$), ou equivalentemente, m estaria em X. Por **ii**), obteríamos $p \in X$. Isto é um absurdo. Dessa forma, $X = \mathbb{N}$. □

Uma outra aplicação do Princípio da Boa Ordem está exposta no próximo teorema. Tal resultado pode ser encontrado na literatura nomeado como Algoritmo da Divisão de Euclides e mostra como dividir um número natural por outro (observe que, não necessariamente, o resultado é um elemento de $\mathbb{N}$).

Teorema 1.19 (Algoritmo da Divisão)**.** *Sejam $n \in \mathbb{N}$ e $d \in \mathbb{N}^*$. Então, existem únicos $q, r \in \mathbb{N}$ tais que*

$$n = dq + r, \text{ com } 0 \leq r < d.$$

Aqui n, d, q e r são chamados dividendo, divisor, quociente e resto na divisão de n por d.

Demonstração. Existência: Por hipótese $d > 0$. Logo, $d \geq 1$ (ver Proposição 1.9). Se assumirmos que $d = 1$, então considere que $q = n$ e $r = 0$ em ordem a obter

$$n = 1 \cdot n + 0 = dq + r, \text{ onde } 0 \leq r < d.$$

Note que se $n < d$, então, sendo $q = 0$ e $r = n$, obtemos

$$n = d \cdot 0 + n = dq + r, \text{ onde } 0 \leq r = n < d.$$

Portanto, podemos assumir que $n \geq d > 1$ (tricotomia).

Afirmamos que existe $q_0 \in \mathbb{N}$ tal que

$$dq_0 \leq n < d(q_0 + 1). \tag{1.3}$$

Suponha, por contradição, que

$$n < dq \text{ ou } n \geq d(q + 1), \forall q \in \mathbb{N}. \tag{1.4}$$

Assim, considere o conjunto

$$X = \{q \in \mathbb{N} / n \geq dq\}.$$

Vamos provar, por indução sobre q, que $X = \mathbb{N}$. Com efeito, $0 \in X$, pois $n \geq 0 = d \cdot 0$. Além disso, se $q \in X$, temos que $n \geq dq$. Logo, por (1.4), concluímos que $n \geq d(q + 1) = ds(q)$. Então, $s(q) \in X$. Por isso, pelo Princípio da Indução, $X = \mathbb{N}$. Deste modo, $n \in X$, ou seja, $n \geq dn$. Como $n \geq d > 0$, inferimos que $1 \geq d$. Mas, $1 < d$. Isto é um absurdo, pela tricotomia. Sendo assim (1.3) é válida.
Com isso,

$$Y = \{q \in \mathbb{N} / dq \leq n < d(q+1)\} \neq \emptyset,$$

pois $q_0 \in Y$. Pelo Princípio da Boa Ordem, existe $q_1 = \min Y$. Como $q_1 \in Y$, tem-se que

$$dq_1 \leq n < d(q_1 + 1).$$

Portanto, existe $r_1 \in \mathbb{N}$ tal que $n = dq_1 + r_1$; além disso,

$$dq_1 + r_1 < dq_1 + d,$$

ou equivalentemente, $0 \leq r_1 < d$ (lembre que $r_1 \in \mathbb{N}$). Por fim, existem $q_1, r_1 \in \mathbb{N}$ tais que

$$n = dq_1 + r_1, \text{ onde } 0 \leq r_1 < d.$$

Unicidade: Suponha que existem q_2 e $r_2 \in \mathbb{N}$ tais que

$$n = dq_2 + r_2, \text{ onde } 0 \leq r_2 < d.$$

Somando dq_2 a esta última desigualdade encontramos

$$dq_2 \leq n < dq_2 + d = d(q_2 + 1).$$

Isto significa que $q_2 \in Y$. Porém, $q_1 = \min Y$. Consequentemente, $q_1 \leq q_2$. Suponha, por absurdo, que $q_1 < q_2$. Assim, existe $s \in \mathbb{N}^*$ tal que $q_2 = q_1 + s$. Daí, obtemos

$$dq_1 + r_1 = n = dq_2 + r_2 = d(q_1 + s) + r_2 = dq_1 + ds + r_2.$$

Pela lei do cancelamento, temos que

$$r_1 = ds + r_2.$$

Por conseguinte, pelo fato que $d > 0$ e $s \geq 1$ (ver Proposição 1.9), podemos escrever

$$r_1 \geq ds \geq d.$$

Isto é um absurdo, pois $r_1 < d$ (tricotomia). Por fim, $q_1 = q_2$. Assim,

$$dq_1 + r_1 = n = dq_2 + r_2 = dq_1 + r_2.$$

Pela lei do cancelamento, chegamos a $r_1 = r_2$. Isto finaliza a prova do teorema em questão. □

Uma aplicação que podemos compartilhar com o leitor, para o Algoritmo da divisão, é que qualquer número natural n se escreve na forma $n = 2k$ (neste caso, n é dito natural par) ou $n = 2k' + 1$ (aqui, n é chamado natural ímpar), onde $k, k' \in \mathbb{N}$.

Proposição 1.16. *Sejam* $2\mathbb{N} = \{2n/n \in \mathbb{N}\}$ (*conjunto dos números naturais pares*) *e* $2\mathbb{N} + 1 = \{2m + 1/m \in \mathbb{N}\}$ (*conjunto dos números naturais ímpares*). *Então,* $\mathbb{N} = 2\mathbb{N} \cup (2\mathbb{N} + 1)$.

Demonstração. Seja $n \in \mathbb{N}$. Pelo Algoritmo da divisão, temos que existem únicos $q, r \in \mathbb{N}$ tais que

$$n = 2q + r, \text{ onde } 0 \leq r < 2.$$

Vimos que $r = 0$ ou 1. Logo,

$$n = 2q \text{ ou } n = 2q + 1.$$

Assim, $n \in 2\mathbb{N}$ ou $n \in 2\mathbb{N} + 1$. Isto prova que $\mathbb{N} \subseteq 2\mathbb{N} \cup (2\mathbb{N} + 1)$. A inclusão recíproca é trivial. □

1.5 Enumerabilidade de $\mathbb{N}$

Nesta seção, estamos interessados em provar que o conjunto dos números naturais é enumerável. Para este fim, definamos o que significa enumerabilidade.

Definição 1.10. Seja X um conjunto qualquer. Se X é finito ou se existe uma bijeção entre o conjunto X e $\mathbb{N}$, dizemos que X é enumerável[15]. Dizemos ainda que qualquer bijeção de $\mathbb{N}$ em um conjunto enumerável X chama-se enumeração para X.

O primeiro exemplo de conjunto enumerável é o próprio $\mathbb{N}$.

Teorema 1.20. $\mathbb{N}$ *é enumerável.*

Demonstração. Considere a função identidade $I_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ definida por $I_{\mathbb{N}}(n) = n$, para todo $n \in \mathbb{N}$. É fácil ver que $I_{\mathbb{N}}$ é injetora, pois

[15]Conjuntos Enumeráveis também são chamados de Conjuntos Contáveis.

$$I_{\mathbb{N}}(n_0) = I_{\mathbb{N}}(n_1) \Rightarrow n_0 = n_1.$$

A sobrejetividade é também facilmente verificável, basta tomarmos $n \in \mathbb{N}$ em ordem a garantir que $I_{\mathbb{N}}(n) = n$. Portanto, $\mathbb{N}$ é enumerável. □

Na verdade, demonstraremos que qualquer subconjunto de $\mathbb{N}$ é enumerável. Para este fim, precisaremos do seguinte lema.

Lema 1.6. *Sejam X um subconjunto de um conjunto universo U e A_n, $n \in \mathbb{N}$, uma família de subconjuntos de U. Então,*

$$X\backslash(\cup_{n\in\mathbb{N}}A_n) = \cap_{n\in\mathbb{N}}(X\backslash A_n) \text{ e } X\backslash(\cap_{n\in\mathbb{N}}A_n) = \cup_{n\in\mathbb{N}}(X\backslash A_n).$$

Demonstração. **i)** É fácil ver que

$$x \in X\backslash(\cup_{n\in\mathbb{N}}A_n) \Leftrightarrow x \in X \text{ e } x \notin \cup_{n\in\mathbb{N}}A_n \Leftrightarrow x \in X \text{ e } x \notin A_n, \forall n \in \mathbb{N} \Leftrightarrow x \in X\backslash A_n, \forall n \in \mathbb{N}$$

$$\Leftrightarrow x \in \cap_{n\in\mathbb{N}}(X\backslash A_n).$$

ii) Também temos que

$$x \in X\backslash(\cap_{n\in\mathbb{N}}A_n) \Leftrightarrow x \in X \text{ e } x \notin \cap_{n\in\mathbb{N}}A_n \Leftrightarrow x \in X \text{ e } x \notin A_{n_0}, n_0 \in \mathbb{N} \Leftrightarrow x \in X\backslash A_{n_0}, n_0 \in \mathbb{N}$$

$$\Leftrightarrow x \in \cup_{n\in\mathbb{N}}(X\backslash A_n).$$

□

Estamos pronto para provar que $X \subset \mathbb{N}$ é sempre enumerável.

Proposição 1.17. *Todo subconjunto de $\mathbb{N}$ é enumerável.*

Demonstração. Seja $X \subset \mathbb{N}$. Se X é finito então, por definição, X é enumerável. Considere, então, que X é infinito. Logo, pelo Teorema 1.16, existe $x_0 = \min X$ $(X \neq \emptyset)$. Como X é infinito, o conjunto $Y_0 = X\backslash\{x_0\}$ é não vazio. Novamente, pelo Teorema 1.16, existe $x_1 = \min Y_0$. Obtidos $x_0, x_1, x_2, ..., x_n (n \in \mathbb{N})$ da forma acima, encontramos $x_{n+1} = \min Y_n = X\backslash\{x_0, x_1, x_2, ..., x_n\}$, que existe, pois Y_n é não vazio (ver Teorema 1.16), para todo n natural; caso contrário, X seria finito.

Afirmamos que

$$X = \{x_0, x_1, x_2, ..., x_n, ...\} = \{x_0\} \cup \{x_0, x_1\} \cup ... = \cup_{n\in\mathbb{N}} A_n,$$

onde $A_n = \{x_0, x_1, x_2, ..., x_n\}$. De fato, pelo Lema 1.6, temos que

$$X\backslash(\cup_{n\in\mathbb{N}} A_n) = \cap_{n\in\mathbb{N}}(X\backslash A_n) = \cap_{n\in\mathbb{N}} Y_n.$$

Assim, se existisse $x \in X\backslash(\cup_{n\in\mathbb{N}} A_n)$, esse x também seria elemento de $\cap_{n\in\mathbb{N}} Y_n$, e como tal, deveria ser maior do que x_0 (pois $x_0 = \min X$), por estar em $Y_0 = X\backslash\{x_0\}$, que deveria também ser maior do que x_1(pois $x_1 = \min Y_0$) e por estar em Y_1 ($Y_1 = X\backslash\{x_0, x_1\}$) e, assim sucessivamente x deveria ser maior do que x_n, para todo $n \in \mathbb{N}$.

Afirmamos que

$$X\backslash I_x \subseteq X\backslash(\cup_{n\in\mathbb{N}} A_n), \tag{1.5}$$

onde $I_x = \{0, 1, 2, 3, ..., x\}$. Com efeito, se $x^{'} \in X\backslash I_x$, então $x^{'} \in X$ e $x^{'} > x$. Como $x > x_n$, para todo $n \in \mathbb{N}$, tem-se que $x^{'} > x_n$, para todo $n \in \mathbb{N}$. O que implica que

$$x^{'} \in \cap_{n\in\mathbb{N}} Y_n,$$

já que $x^{'} \in X$ e $x^{'} \neq x_n$, para todo $n \in \mathbb{N}$. Consequentemente, $x^{'} \in X\backslash(\cup_{n\in\mathbb{N}} A_n)$. Por (1.5), concluímos que

$$\cup_{n\in\mathbb{N}} A_n \subseteq I_x.$$

Como I_x é finito, então $\cup_{n\in\mathbb{N}} A_n = \{x_0, x_1, ..., x_n, ...\}$ ($x_i \neq x_j, i \neq j$) também o é. Mas isto é um absurdo, pela construção dos $x_n^{'}s$. Por fim, $X\backslash(\cup_{n\in\mathbb{N}} A_n) = \emptyset$. Consequentemente, $X = \cup_{n\in\mathbb{N}} A_n = \{x_0, x_1, ..., x_n, ...\}$. □

Abaixo exibimos mais uma maneira de obtermos conjuntos enumeráveis.

Proposição 1.18. A união de uma família finita de conjuntos infinitos enumeráveis é infinito enumerável.

Demonstração. Vamos primeiramente provar que $A \cup B$ é enumerável, se A e B o são.

Suponhamos, primeiramente, que $A \cap B = \varnothing$. Como A é enumerável, existe uma função $f_1 : A \to \mathbb{N}$ bijetora. Defina $g_1 : \mathbb{N} \to 2\mathbb{N}$, por $g_1(n) = 2n$ para todo $n \in \mathbb{N}$. É fácil ver que

g_1 é bijetora. Como para todo $2n$ existe n, tal que $g_1(n) = 2n$ então g_1 é sobrejetiva. Além disso, se $g_1(m) = g_1(n)$ temos que $m = n$, logo a função é bijetora. Sendo assim, a função $h_1 = g_1 \circ f_1 : A \to 2\mathbb{N}$, dada por $h_1(x) = 2f_1(x)$ é bijetora. Do mesmo modo, como B é enumerável existe uma função bijetora $f_2 : B \to \mathbb{N}$. Defina $g_2 : \mathbb{N} \to 2\mathbb{N} + 1$, por $g_2(n) = 2n + 1$ para todo $n \in \mathbb{N}$, analogamente ao que foi feito acima, concluímos que g_2 é bijetora. Desta forma, obtemos $h_2 : g_2 \circ f_2 : B \to 2\mathbb{N} + 1$, dada por $h_2(x) = 2f_2(x) + 1$, bijetora. Sendo assim, $f : A \cup B \to \mathbb{N}$, dada por:

$$f(n) = \begin{cases} h_1(n), \ se \ n \in A; \\ h_2(n), \ se \ n \in B, \end{cases}$$

é bijetora. Como $A \cap B = \varnothing$, f está bem definida e como $2\mathbb{N} \cup (2\mathbb{N} + 1) = \mathbb{N}$ (ver Proposição 1.16), concluímos que $A \cup B$ é enumerável.

Seja agora, $A \cap B \neq \varnothing$. Considere agora que $C = A \backslash B$. Claramente, temos que $B \cap C = \varnothing$, portanto pelo que já foi demonstrado acima, $C \cup B$ é enumerável.

Sejam agora $A_1, A_2, A_3, ..., A_n$ conjuntos enumeráveis. Temos que mostrar que $\cup_{k \in \{1,2,...,n\}} A_k$ é enumerável. Provaremos por indução finita. Sabemos que se $n = 2$ isto é verdade, então suponhamos que $\cup_{k \in \{1,2,...,n-1\}} A_k$ é enumerável e provemos que $\cup_{k \in \{1,2,...,n\}} A_k$ também é. Daí, como $\cup_{k \in \{1,2,...,n-1\}} A_k$ é enumerável e A_n também, obviamente, $(\underset{\cup}{k \in \{1, 2, ..., n-1\}} \ A_k) \cup A_n$ é enumerável, como queríamos. □

O fato de um subconjunto de $\mathbb{N}$ ser enumerável pode ser generalizado para um conjunto enumerável qualquer da seguinte forma:

Proposição 1.19. Todo subconjunto de um conjunto enumerável é enumerável.

Demonstração. Seja X um conjunto enumerável e Y um subconjunto de X. Se X é finito, então Y é finito e, por definição, Y é enumerável. Assuma, que X é infinito. Novamente, se Y é finito, então Y é enumerável. Considere, dessa forma, que Y é infinito. Como X (infinito) é enumerável, então existe uma função $f : X \to \mathbb{N}$ bijetora. Dessa forma, tomemos $f|_Y : Y \to \mathbb{N}$ (restrição de f a Y), como isso, $f(Y) \subset \mathbb{N}$, daí pela Proposição 1.17, $f(Y)$ é enumerável. Logo, existe $g : f(Y) \to \mathbb{N}$ bijetora. Sabendo que g e $f|_Y$ são bijetoras, obtemos que $g \circ f|_Y : Y \to \mathbb{N}$ é bijetora, portanto Y é enumerável, como queríamos. □

1.6 Aplicação lúdica dos números naturais (Torre de Hanói)

A torre de Hanói, também conhecida por torre de bramanismo ou quebra-cabeças do fim do mundo, foi inventada e vendida como brinquedo, no ano de 1883, pelo matemático francês Edouard Lucas. Segundo ele, o jogo que era popular na China e no Japão veio do Vietnã. O matemático foi inspirado por uma lenda Hindu, a qual falava de um templo em Benares, cidade Santa da Índia, onde existia uma torre sagrada do bramanismo, cuja função era melhorar a disciplina mental dos jovens monges. De acordo com a lenda, no grande templo de Benares, debaixo da cúpula que marca o centro do mundo, há uma placa de bronze sobre a qual estão fixadas três hastes de diamante. Em uma dessas hastes, o deus Brama, no momento da criação do mundo, colocou 64 discos de ouro puro, de forma que o disco maior ficasse sobre a placa de bronze e os outros decrescendo até chegar ao topo. A atribuição que os monges receberam foi de transferir a torre formada pelos discos, de uma haste para outra, usando a terceira como auxiliar com as restrições de movimentar um disco por vez e de nunca colocar um disco maior sobre um menor. Os monges deveriam trabalhar com eficiência noite e dia e, quando terminassem o trabalho, o templo seria transformado em pó e o mundo acabaria.

O jogo consiste em uma base de madeira onde estão firmados três hastes verticais, e um certo número de discos de madeira, de diâmetros diferentes, furados no centro. Vamos chamar de A, B e C, as três hastes, conforme a figura.

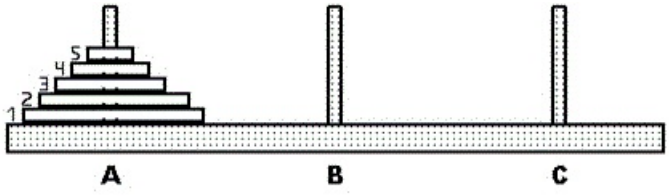


Figura 1.1: Torre de Hanói

No começo do jogo os discos estão todos enfiados na haste A, em ordem decrescente de tamanho, com o menor disco acima de todos. O objetivo é mover todos os discos, de A para C, obedecendo às seguintes regras:
1)Somente um disco pode ser posto de cada vez.
2)Um disco maior nunca pode ser posto sobre um disco menor.

As perguntas naturais que surgem são as seguintes:

1. O jogo tem solução para cada $n \in \mathbb{N}$?
2. Caso afirmativo, qual é o número mínimo T(n) de movimentos para resolver o problema com n discos.

Inicialmente, mostraremos de forma intuitiva, que a primeira afirmação é válida. Depois, usando indução matemática, formalmente, vamos ver que a resposta à primeira pergunta de fato é afirmativa para qualquer que seja o valor de n. Em seguida, deduziremos uma fórmula que nos fornecerá o número T(n).

Considere a sentença aberta p(n) : o jogo com n discos tem solução.

Obviamente, p(1) é verdade.

Consideremos agora um caso geral com n discos. Vamos imaginar que os discos tenham sido numerados de cima para baixo: $1, 2, ..., n$. O menor disco é o 1, e o maior é o n.

Para remover o disco n é preciso tirar todos de cima, ou seja, tirar todos os $n - 1$ discos que estão acima dele, lembrando-se que queremos mover os discos todos para a haste C, e o disco n é o que deve ficar mais embaixo nesta haste. Então é preferível colocar os outros discos na haste B, ou seja, devemos mover os $n - 1$ discos menores, de A para B um de cada vez respeitando as regras. Feito isso removemos o disco n para a haste C. Agora, para mover os $n - 1$ discos para C, só é possível se for repetindo o jogo, de modo a passar todos os discos (um a um) de B para C.

Podemos observar que temos que fazer o jogo com $n - 1$ discos duas vezes: primeiro movemos os $n - 1$ discos de A para B (usando C como intermediário). Isto descobre o disco n . Movemos então n para C. Agora jogamos com os $n - 1$ discos mais uma vez: de B para C, usando A como intermediário e com isto empilhamos todos em C sem violar as regras. Mas, usaremos uma maior formalidade e demonstraremos usando o princípio de indução. Então, vamos agora provar que é verdade a seguinte sentença:

$\forall n, p(n) \Rightarrow p(n + 1)$

De fato, vamos supor, para um valor n arbitrário, que p(n) é verdade, ou seja, que o jogo com n discos tem solução, e provar que o jogo com n + 1 discos tem solução.

Para ver isto, inicialmente resolva o problema para os n discos superiores da pilha, transferindo-os para uma das hastes livre (isto é possível, pois o problema com n discos tem solução):

Em seguida, transfira o disco que restou na pilha original (o maior dos discos) para a haste

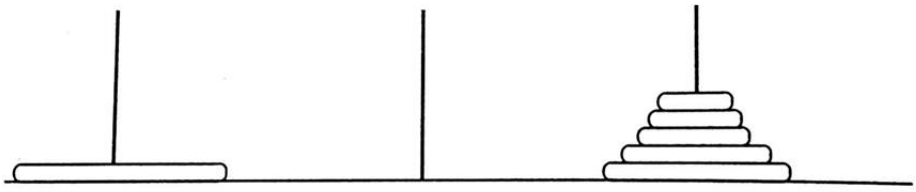


Figura 1.2: Tipo de Jogada

vazia. Feito isso, resolva novamente o problema para os n discos que estão juntos, transferindo-os para a haste que contém o maior dos discos: Isto mostra que o problema com $n+1$ discos possui

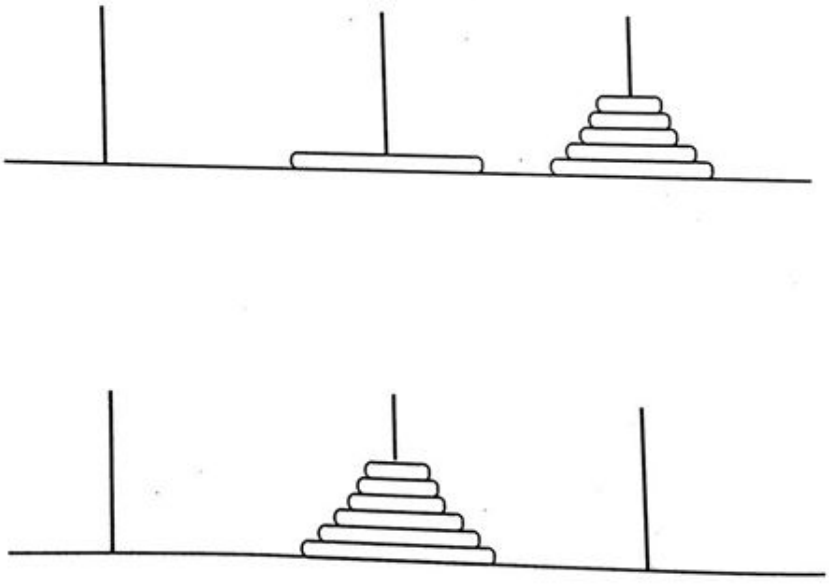


Figura 1.3: Termini do Jogo

solução, e, portanto, pelo princípio de indução, que p(n) é verdade para todo $n \in \mathbb{N}^*$.

Vamos então verificar qual é o número mínimo de movimentos.

Para facilitar, vamos dizer que o número mínimo de movimentos necessários para completar o jogo de n discos é T(n). Como não há como chegar ao disco n sem mover os $n-1$ de cima, então

o número de movimentos que fizemos para isto é $T(n-1)$. Como movemos os $n-1$ para a haste B, a haste C está livre, logo podemos mover o disco n para C, ou seja, o número de movimentos desde o começo do jogo é de $T(n-1)+1$. Então, falta mover os $n-1$ discos de B para C, para ficarem em cima do disco n , ou seja, o número mínimo de movimentos para fazer isto é $T(n-1)$.

Logo desde o começo do jogo fizemos $T(n-1)+1+T(n-1) = 2T(n-1)+1$ movimentos. Pelo que vimos na análise do jogo, mostramos que não é possível fazer um número menor de movimentos, então T(n) é o menor número de movimentos para completar o jogo de n discos, ou seja $T(n) = 2T(n-1)+1$. Já vimos que $T(1) = 1$. Logo, $T(2) = 2T(1)+1 = 3$, $T(3) = 7$, $T(4) = 15$, $T(5) = 31$, $T(6) = 63$.

Por meio de tentativas, descobrimos que para um disco o número de movimentos é apenas um, colocando o disco direto na haste C. Para dois discos é 3 se começarmos na haste B ou 6 se começarmos na haste C. Para três discos é 7 se começarmos na haste C ou 14 se começarmos na haste B. Repetindo o processo para 4,5,...,n discos, podemos observar que se o número inicial de discos da torre inicial for ímpar, o primeiro disco da torre deverá ser colocado, inicialmente, na haste C e, se o número inicial de discos da torre for par, o primeiro disco da torre deverá ser colocado, inicialmente, na haste B.

Tabelando estes resultados temos:

Nº de discos	Quantidade mínima de movimentos
1	1
2	3
3	7
4	15
5	31
6	63

Observando a tabela vemos que:

$1 \to 3 \to 7 \to 15 \to 31 \to 63...$

Note que a diferença entre os termos da sequencia acima é dada pela sequencia $2 \to 4 \to 8 \to 16 \to 32 \to 64...$

Podemos notar então, que o número somado é sempre o dobro do anterior, que já havia sido somado. Analisando mais atentamente a tabela, temos que o resultado da quantidade mínima de movimentos é sempre 1 a menos do número que foi somado, ou resumidamente:

Nº de discos	Quantidade mínima de movimentos	Nº somado
1	1	-1 +2
2	3	-1 +4
3	7	-1 +8
4	15	-1 +16
5	31	-1 +32
6	63	-1 +64

Veja que o número somado é um número do tipo 2^n, e assim a sequência de números somados forma a PG: $(2, 4, 8, 16, 32, ...)$ de razão $q = 2$. Logo, a quantidade mínima de movimentos é igual ao número somado menos 1, ou seja, igual a $2^n - 1$. Então descobrimos que $T(n) = 2^n - 1$.

Como obtivemos a fórmula a partir de alguns dados numéricos, queremos saber se é mesmo verdadeira. Para isso vamos usar o *princípio de indução finita*. Já vimos que $T(1) = 1$, ou seja, $2^1 - 1 = 1$; a fórmula vale neste caso. Suponhamos que $T(n) = 2^n - 1$, queremos mostrar que $T(n+1) = 2^{n+1} - 1$. Temos que a hipótese de indução, isto é, a suposição de que a proposição vale para n é $T(n) = 2^n - 1$. Temos que $T(n+1) = 2T(n) + 1$ através do resultado obtido anteriormente $(T(n) = 2T(n-1) + 1)$.

Começamos com $T(n + 1) = 2T(n) + 1$. Como, pela hipótese de indução, $T(n) = 2^n - 1$, podemos substituir isto na primeira fórmula para obter:

$$T(n + 1) = 2T(n) + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 1$$

que era o resultado esperado. Logo a fórmula $T(n) = 2^n - 1$ vale para qualquer n natural.

Assim, pôde-se descobrir que a quantidade mínima de movimentos necessários para se efetuar a tarefa com os 64 discos é de 18.446.073.709.551.615 movimentos, levando os monges, muitos bilhões de anos para efetuar a tarefa.

Contudo, o leitor não deve preocupar-se com a iminência do fim do mundo pois, se, a cada segundo um sacerdote movesse um disco, o tempo mínimo para que ocorresse a fatalidade seria de um bilhão de séculos!

Capítulo 2

Construção dos Números Inteiros

Neste capítulo, estudaremos a construção dos chamados números inteiros a partir da estrutura aritmética que abordamos no capítulo anterior para $\mathbb{N}$ e das noções básicas de relações de equivalência. Aproveitamos para ressaltar que as propriedades mais elementares, envolvendo números naturais, serão utilizadas, a partir de agora, sem maiores explicações.

2.1 O Conjunto dos Números Inteiros

Faremos uso da definição de relação de equivalência para estabelecer quem são os elementos que vão formar o conjunto dos números inteiros. A referência que serviu como base nesta seção está apresentada em [3].

Definição 2.1. Seja X um conjunto. Uma relação binária R em X diz-se uma relação de equivalência se esta satisfizer as seguintes propriedades:

i) [Reflexividade]: xRx, para todo $x \in X$;

ii) [Simetria]: $x, y \in X$ e $xRy \Rightarrow yRx$;

iii) [Transitividade]: $x, y, z \in X$, xRy e $yRz \Rightarrow xRz$.

O exemplo que daremos, aqui neste capítulo, para uma relação de equivalência está implícito na definição que segue.

Definição 2.2. Sejam $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Dizemos que (a, b) é equivalente a (c, d), e escrevemos $(a, b) \sim (c, d)$, quando $a + d = b + c$.

Vamos, agora, provar que, de fato, a relação binária $\sim$, definida acima, é de equivalência.

Proposição 2.1. *A relação $\sim$, estabelecida na Definição 2.2 é uma relação de equivalência.*

Demonstração. É fácil ver que

i) $(a, b) \sim (a, b)$, pois $a + b = b + a$.

(ii) Se $(a, b) \sim (c, d)$, então $a + d = b + c$. Logo, $c + b = d + a$. Daí, $(c, d) \sim (a, b)$.

(iii) Se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então $a+d = b+c$ e também $c+f = d+e$. Portanto, tem-se

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

Logo, $a + f = b + e$. O que nos diz que $(a, b) \sim (e, f)$.

Por fim, $\sim$ é uma relação de equivalência. □

Definição 2.3. Seja $(a, b) \in \mathbb{N} \times \mathbb{N}$. O conjunto

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N}/(x, y) \sim (a, b)\}$$

é chamado a classe de equivalência do par ordenado (a, b) com relação a $\sim$.

Exemplo 2.1. Por exemplo, é fácil checar que

i) $\overline{(4, 0)} = \{(4, 0), (5, 1), (6, 2), (7, 3), ...\}$;

ii) $\overline{(0, 4)} = \{(0, 4), (1, 5), (2, 6), (3, 7), ...\}$;

iii) $\overline{(6, 2)} = \{(4, 0), (5, 1), (6, 2), (7, 3), ...\}$.

Abaixo, estabelecemos a definição do conjunto dos números inteiros.

Definição 2.4. Definimos o conjuntos dos números inteiros, e denotamos por $\mathbb{Z}$, como sendo o conjunto quociente $\mathbb{N} \times \mathbb{N}/\sim$, isto é,

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

No restante deste capítulo, exibiremos condições para que a definição de $\mathbb{Z}$, dada acima, coincida com a conhecida do ensino elementar.

2.2 Operações Elementares com Números Inteiros

Nesta seção, como em $\mathbb{N}$, definiremos as operações de adição, $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, e multiplicação, $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, em $\mathbb{Z}$. Além disso, estabeleceremos algumas propriedades elementares envolvendo estas duas operações.

2.2.1 Propriedades Elementares da Adição em $\mathbb{Z}$

Comecemos definindo como somar dois números inteiros.

Definição 2.5. Dados $\overline{(a,b)}$ e $\overline{(c,d)}$ em $\mathbb{Z}$, definimos a adição $\overline{(a,b)} + \overline{(c,d)}$ como sendo o inteiro $\overline{(a+c, b+d)}$.

Exemplo 2.2. É fácil checar que:

1. $\overline{(0,1)} + \overline{(2,3)} = \overline{(0+2, 1+3)} = \overline{(2,4)}$;
2. $\overline{(4,2)} + \overline{(1,1)} = \overline{(4+1, 2+1)} = \overline{(5,3)}$.

Vamos agora provar que dois elementos de $\mathbb{N} \times \mathbb{N}$ são equivalentes se, e somente se, estes representam a mesma classe de equivalência.

Lema 2.1. *Sejam* (a,b) *e* $(a',b') \in \mathbb{N} \times \mathbb{N}$. *Então,* $(a,b) \sim (a',b') \Leftrightarrow \overline{(a,b)} = \overline{(a',b')}$.

Demonstração. ($\Leftarrow$) Note que, $(a,b) \in \overline{(a,b)} = \overline{(a',b')}$. Logo, $(a,b) \sim (a',b')$.

($\Rightarrow$) Suponha, agora, que $(x,y) \in \overline{(a,b)}$, então $(x,y) \sim (a,b)$. Assim, $(x,y) \sim (a,b) \sim (a',b')$, por hipótese. Dessa forma, $(x,y) \in \overline{(a',b')}$. Consequentemente, $\overline{(a,b)} \subset \overline{(a',b')}$. A inclusão recíproca é análoga. □

Note que a definição de adição entre dois inteiros é realizada através de classes de equivalência. Portanto, precisamos verificar se esta depende dos elementos que representam tais classes.

Proposição 2.2. *Sejam* $\overline{(a,b)}$ *e* $\overline{(c,d)} \in \mathbb{Z}$. *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. Como $\overline{(a,b)} = \overline{(a',b')}$, então, pelo Lema 2.1, temos que $(a,b) \sim (a',b')$. Segue deste fato que $a + b' = b + a'$. Da mesma maneira, $\overline{(c,d)} = \overline{(c',d')} \Leftrightarrow (c,d) \sim (c',d')$. Assim, $c + d' = d + c'$.

Por outro lado, temos que

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

Mostraremos que as duas expressões dos lados direitos das igualdades acima coincidem. Pelo Lema 2.1, isso equivale a mostrar que

$$(a+c, b+d) \sim (a'+c', b'+d').$$

Mas, é verdade que

$$(a+c)+(b'+d') = (a+b')+(c+d') = (b+a')+(d+c') = (b+d)+(a'+c').$$

O resultado segue da Definição 2.2. □

Agora, estamos interessados em provar que a adição de números inteiros satisfaz propriedades elementares tais como: associatividade, comutatividade, existência de um único elemento neutro e lei do cancelamento. Comparando com os elementos de $\mathbb{N}$, veremos que cada número inteiro apresentará um simétrico aditivo, o que não é verificado em $\mathbb{N}$.

Comecemos provando que a adição em $\mathbb{Z}$ é associativa.

Teorema 2.1 (Associatividade)**.** *Sejam* $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$*. Então,*

$$[\overline{(a,b)} + \overline{(c,d)}] + \overline{(e,f)} = \overline{(a,b)} + [\overline{(c,d)} + \overline{(e,f)}].$$

Demonstração. É fácil checar que

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

Isto completa a prova do teorema em questão. □

Agora, permita-nos enunciar e demonstrar a propriedade comutativa.

Teorema 2.2 (Comutatividade)**.** *Sejam* $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$*. Então,* $\overline{(a,b)} + \overline{(c,d)} = \overline{(c,d)} + \overline{(a,b)}$.

Demonstração. Observe que,

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

Isto completa a prova deste teorema. □

Usando o elemento neutro da adição em $\mathbb{N}$, 0, é possível provar que $\overline{(0,0)}$ é o elemento neutro da adição entre números inteiros.

Teorema 2.3 (Elemento Neutro)**.** *Seja* $\overline{(a,b)} \in \mathbb{Z}$*. Então,* $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$.

Demonstração. Podemos escrever o seguinte:

$$\overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)}.$$

Portanto, $\overline{(0,0)}$ é o elemento neutro aditivo em $\mathbb{Z}$. □

A lei do cancelamento exposta em $\mathbb{N}$, com relação à adição, também é válida em $\mathbb{Z}$. Mais precisamente, temos o seguinte teorema.

Teorema 2.4 (Lei do Cancelamento)**.** *Seja* $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$*. Então,*

$$\overline{(a,b)} + \overline{(e,f)} = \overline{(c,d)} + \overline{(e,f)} \Rightarrow \overline{(a,b)} = \overline{(c,d)}.$$

Demonstração. De fato, por hipótese, temos que

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

Daí, pela Definição 2.5, chegamos a

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

Logo,

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

Com isso, aplicando a lei do cancelamento em $\mathbb{N}$, obtemos $a+d = b+c$, isto é, $(a,b) \sim (c,d)$. O Lema 2.1 nos informa que $\overline{(a,b)} = \overline{(c,d)}$. □

A seguir provaremos que cada número inteiro tem um simétrico[1]. Este fato não é válido em $\mathbb{N}$.

Teorema 2.5 (Simétrico)**.** *Dado $\overline{(a,b)} \in \mathbb{Z}$, existe um único $\overline{(c,d)} \in \mathbb{Z}$ tal que $\overline{(a,b)}+\overline{(c,d)} = \overline{(0,0)}$. Na verdade, temos que $\overline{(c,d)} = \overline{(b,a)}$.*

Demonstração. Vamos provar primeiramente a existência. Assim sendo, note que

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, b+a)} = \overline{(0,0)}.$$

De fato, segue da igualdade $(a+b)+0 = 0+(b+a)$ que $(a+b, b+a) \sim (0,0)$. Portanto, pelo Lema 2.1, obtemos $\overline{(a+b,b+a)} = \overline{(0,0)}$. Com isso, $\overline{(a,b)} + \overline{(b,a)} = \overline{(0,0)}$.

Agora, chequemos a unicidade do simétrico. Consideremos que existe $\overline{(c',d')}$ tal que $\overline{(a,b)} + \overline{(c',d')} = \overline{(0,0)}$. Assim,

$$\overline{(a,b)} + \overline{(c',d')} = \overline{(0,0)} = \overline{(a,b)} + \overline{(b,a)}.$$

Pela lei do cancelamento, concluímos que $\overline{(c',d')} = \overline{(b,a)}$. Portanto, o elemento simétrico existe e é único. □

Definição 2.6. Dado $\alpha \in \mathbb{Z}$, o único $\beta \in \mathbb{Z}$ tal que $\alpha + \beta = \overline{(0,0)}$ é chamado simétrico de α e é denotado por $-\alpha$.

Exemplo 2.3. É fácil ver que $\overline{(0,1)}$ e $\overline{(2,5)}$ são os simétricos de $\overline{(1,0)}$ e $\overline{(5,2)}$, respectivamente, em $\mathbb{Z}$.

Lembre que verificamos, na Proposição 1.2, que o único elemento natural que possui simétrico (com uma definição análoga a dada acima) é 0. Assim sendo, o conjunto $\mathbb{Z}$ já apresenta uma propriedade que não é observada em $\mathbb{N}$.

É importante ressaltar que provamos que $\alpha + (-\alpha) = \overline{(0,0)}$ (ver Teorema 2.5), onde $\alpha = \overline{(a,b)}$ e $-\alpha = \overline{(b,a)} \in \mathbb{Z}$. A existência e a unicidade do simétrico para cada elemento de $\mathbb{Z}$ nos permite que definamos uma terceira operação em $\mathbb{Z}$ (esta não está bem estabelecida em $\mathbb{N}$).

Definição 2.7. A subtração em $\mathbb{Z}$, denotada por $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, é a operação definida da seguinte forma: Se $\alpha, \beta \in \mathbb{Z}$, então

$$\alpha - \beta := \alpha + (-\beta).$$

[1]Seja A um conjunto com uma adição definida. Assuma que $a \in A$. Um elemento $b \in A$ é denominado simétrico de a se $a + b = b + a = 0$.

Note que a subtração de $\alpha \in \mathbb{Z}$ por $\beta \in \mathbb{Z}$ é, na verdade, a adição de α com o simétrico de β.

Exemplo 2.4. Um simples exemplo de subtração pode ser dado pelas seguintes igualdades:

$$\overline{(0,1)} - \overline{(2,5)} = \overline{(0,1)} + \overline{(5,2)} = \overline{(5,3)}.$$

Vejamos algumas regras de sinal envolvendo a subtração em $\mathbb{Z}$.

Proposição 2.3. *Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$. Então, vale as seguintes igualdades:*

i) $-(-\alpha) = \alpha$;

ii) $-\alpha + \beta = \beta - \alpha$;

iii) $\alpha - (-\beta) = \alpha + \beta$;

iv) $-\alpha - \beta = -(\alpha + \beta)$;

v) $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$.

Demonstração. Consideremos que $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$.

i) Se $\alpha = \overline{(a,b)}$, então

$$-(-\alpha) = -\overline{(b,a)} = \overline{(a,b)} = \alpha.$$

ii) Pela comutatividade, temos que

$$\beta - \alpha := \beta + (-\alpha) = (-\alpha) + \beta = -\alpha + \beta.$$

iii) Por **i**), obtemos

$$\alpha + \beta = \alpha + [-(-\beta)] =: \alpha - (-\beta).$$

iv) Pela comutatividade, chegamos a

$$\begin{aligned} -(\alpha + \beta) &= -[\overline{(a,b)} + \overline{(c,d)}] = -\overline{(a+c, b+d)} \\ &= \overline{(b+d, a+c)} = \overline{(b,a)} + \overline{(d,c)} \\ &= \overline{(d,c)} + \overline{(b,a)} = -\overline{(c,d)} + [-\overline{(a,b)}] \\ &= -\beta + (-\alpha) =: -\beta - \alpha. \end{aligned}$$

v) Por fim, segue, de **iv**) e da associatividade, que

$$\begin{aligned}\alpha - (\beta + \gamma) &:= \alpha + [-(\beta + \gamma)] = \alpha + (-\beta - \gamma) \\ &= [\alpha + (-\beta)] + (-\gamma) = \alpha - \beta + (-\gamma) \\ &=: \alpha - \beta - \gamma.\end{aligned}$$

□

2.2.2 Propriedades Elementares da Multiplicação em $\mathbb{Z}$

Nesta subseção, apresentaremos uma definição para a multiplicação entre dois números inteiros quaisquer. Além disso, mostraremos que algumas propriedades elementares, já conhecidas do ensino elementar, são, de fato, verdadeiras.

Definição 2.8. Dados $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$, definimos o produto $\overline{(a,b)} \cdot \overline{(c,d)}$ como sendo o inteiro $\overline{(ac+bd, ad+bc)}$.

Permita-nos informar que, em alguns momentos, denotaremos a multiplicação de $\overline{(a,b)}$ por $\overline{(c,d)}$ da seguinte maneira: $\overline{(a,b)}\,\overline{(c,d)}$.

Exemplo 2.5. É fácil checar que:

1. $\overline{(4,2)} \cdot \overline{(10,7)} = \overline{(4 \cdot 10 + 2 \cdot 7, 4 \cdot 7 + 2 \cdot 10)} = \overline{(54,48)}$;
2. $\overline{(3,5)} \cdot \overline{(10,7)} = \overline{(3 \cdot 10 + 5 \cdot 7, 3 \cdot 7 + 5 \cdot 10)} = \overline{(65,71)}$.

Como a definição de multiplicação entre dois inteiros, assim como a adição, depende de classes de equivalência, provaremos que os representantes de cada uma das classes envolvidas não alteram o resultado da operação.

Proposição 2.4. *Sejam* $\overline{(a,b)}, \overline{(a',b')}, \overline{(c,d)}, \overline{(c',d')} \in \mathbb{Z}$. *Se* $\overline{(a,b)} = \overline{(a',b')}$ *e* $\overline{(c,d)} = \overline{(c',d')}$, *então* $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.

Demonstração. Como $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$, então

$$a + b' = b + a' \text{ e } c + d' = d + c'.$$

Daí temos,

i $(a+b')\cdot c' = (b+a')\cdot c'$

ii $(b+a')\cdot d' = (a+b')\cdot d'$

iii $(a+b')\cdot c = (b+a')\cdot c$

iv $(b+a')\cdot d = (a+b')\cdot d$

v $(c+d')\cdot a' = (d+c')\cdot a'$

vi $(d+c')\cdot b' = (c+d')\cdot b'$

vii $(c+d')\cdot a = (d+c')\cdot a$

viii $(d+c')\cdot b = (c+d')\cdot b$

Somando os termos dos primeiros membros das equações acima e igualando à soma dos termos dos segundos membros, obtemos daí ,após algumas manipulações algébricas, que:

$$\begin{aligned} &2(ac+bd+a'd'+b'c') + ac' + b'c + a'd + bd' + ca' + d'a + db' + c'b \\ &= 2(ad+bc+a'c'+b'd') + a'c + bc' + ad' + b'd + da' + c'a + cb' + d'b. \end{aligned}$$

E usando a lei do cancelamento em $\mathbb{N}$, obtemos

$$ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'.$$

O que significa dizer que $\overline{(a,b)}\cdot\overline{(c,d)} = \overline{(a',b')}\cdot\overline{(c',d')}$ (ver Lema 2.1). □

Vamos provar que a multiplicação em $\mathbb{Z}$, assim como a adição, é associativa, comutativa, tem um único elemento neutro e satisfaz a lei do cancelamento. Além disso, mostraremos que a distributividade da multiplicação com relação a adição em $\mathbb{Z}$ também é válida.

Comecemos com a prova da comutatividade.

Teorema 2.6 (Comutatividade)**.** *Sejam* $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$*. Então,* $\overline{(a,b)}\cdot\overline{(c,d)} = \overline{(c,d)}\cdot\overline{(a,b)}$.

Demonstração. As seguintes igualdades são válidas:

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

□

Permita-nos provar que a multiplicação entre números inteiros é associativa.

Teorema 2.7 (Associatividade)**.** *Sejam* $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$*. Então,*

$$[\overline{(a,b)} \cdot \overline{(c,d)}] \cdot \overline{(e,f)} = \overline{(a,b)} \cdot [\overline{(c,d)} \cdot \overline{(e,f)}].$$

Demonstração. É fácil ver que

$$\begin{aligned}[\overline{(a,b)} \cdot \overline{(c,d)}] \cdot \overline{(e,f)} &= \overline{(ac+bd, ad+bc)} \cdot \overline{(e,f)} \\ &= \overline{((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e)} \\ &= \overline{((ac)e + (bd)e + (ad)f + (bc)f, (ac)f + (bd)f + (ad)e + (bc)e)} \\ &= \overline{(a(ce) + b(de) + a(df) + b(cf), a(cf) + b(df) + a(de) + b(ce))} \\ &= \overline{(a(ce+df) + b(cf+de), a(cf+de) + b(ce+df))} \\ &= \overline{(a,b)} \cdot \overline{(ce+df, cf+de)} \\ &= \overline{(a,b)} \cdot [\overline{(c,d)} \cdot \overline{(e,f)}].\end{aligned}$$

□

O elemento neutro da multiplicação entre números naturais é dado por $\overline{(1,0)}$. Mais precisamente, temos o seguinte resultado.

Teorema 2.8 (Elemento Neutro)**.** *Sejam* $\overline{(a,b)} \in \mathbb{Z}$*. Então,* $\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a,b)}$.

Demonstração. As seguintes igualdades são verdadeiras:

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

Logo, $\overline{(1,0)}$ é o elemento neutro multiplicativo em $\mathbb{Z}$. □

Agora faremos a prova para a propriedade distributiva, a qual relaciona em uma mesma igualdade as operações de adição e multiplicação entre números inteiros.

Teorema 2.9 (Distributividade)**.** *Sejam* $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$*. Então,*

$$\overline{(a,b)} \cdot [\overline{(c,d)} + \overline{(e,f)}] = \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)}.$$

Demonstração. A distributividade segue diretamente das seguintes igualdades:

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

Isto completa a prova do teorema em questão. □

É fácil ver que a distributividade

$$[\overline{(a,b)} + \overline{(c,d)}] \cdot \overline{(e,f)} = \overline{(a,c)} \cdot \overline{(e,f)} + \overline{(c,d)} \cdot \overline{(e,f)},$$

segue diretamente da comutatividade.

Resta-nos provar a lei de cancelamento para a multiplicação entre números inteiros.

Teorema 2.10. *Sejam* $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in \mathbb{Z}$ *com* $\overline{(e,f)} \neq \overline{(0,0)}$*. Então,*

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

Demonstração. Através da igualdade $\overline{(a,b)} \cdot \overline{(e,f)} = \overline{(c,d)} \cdot \overline{(e,f)}$, concluímos que

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

Logo, pelo Lema 2.1, chegamos a

$$(ae+bf, af+be) \sim (ce+df, cf+de).$$

Portanto,

$$ae + bf + cf + de = af + be + ce + df.$$

Usando a aritmética dos números naturais nessa igualdade, obtemos

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

Por hipótese, concluímos que $e \neq f$ ($\overline{(e, f)} \neq \overline{(0, 0)}$). Suponhamos, sem perda de generalidade, que $e > f$. Daí $e = f + k$, para algum $k \in \mathbb{N}^*$. Segue, daí, que

$$(f + k)(a + d) + f(b + c) = (f + k)(b + c) + f(a + d).$$

Assim sendo, obtemos

$$f(a + d) + k(a + d) + f(b + c) = f(a + d) + k(b + c) + f(b + c).$$

Usando o cancelamento aditivo em $\mathbb{N}$, obtemos $k(a + d) = k(b + c)$. Como $k \in \mathbb{N}^*$, segue, do cancelamento multiplicativo em $\mathbb{N}$, que $a + d = b + c$. Consequentemente, $(a, b) \sim (c, d)$. Por fim, pelo Lema 2.1, encontramos $\overline{(a, b)} = \overline{(c, d)}$. □

Como na definição da multiplicação entre números naturais, provaremos a seguir que qualquer número inteiro multiplicado por $\overline{(0, 0)}$ resulta em $\overline{(0, 0)}$.

Proposição 2.5. *Seja $\alpha \in \mathbb{Z}$. Então, $\overline{(0, 0)} \cdot \alpha = \overline{(0, 0)}$.*

Demonstração. Note que,

$$\begin{aligned}
\overline{(0, 0)} \cdot \alpha &= \overline{(0, 0)} \cdot \overline{(a, b)} \\
&= \overline{(0 \cdot a + 0 \cdot b, 0 \cdot b + 0 \cdot a)} \\
&= \overline{(0 + 0, 0 + 0)} \\
&= \overline{(0, 0)}.
\end{aligned}$$

Isto completa a prova da proposição em questão. □

É também verdade que o conjunto dos números inteiros não possui divisores de zero. Mais precisamente, temos o resultado abaixo.

Proposição 2.6. *Sejam α,$\beta \in \mathbb{Z}$ tais que $\alpha \cdot \beta = \overline{(0, 0)}$, então $\alpha = \overline{(0, 0)}$ ou $\beta = \overline{(0, 0)}$.*

Demonstração. Pela Proposição 2.5, temos que $\overline{(0,0)} \cdot \gamma = \overline{(0,0)}$, para todo $\gamma \in \mathbb{Z}$. Suponhamos que $\beta \neq \overline{(0,0)}$. Segue, daí, que

$$\overline{(0,0)} \cdot \beta = \overline{(0,0)} = \alpha \cdot \beta.$$

Pela lei do cancelamento em $\mathbb{Z}$, concluímos que $\alpha = \overline{(0,0)}$. □

Agora, mostraremos que as famosas regras de sinais, com relação a multiplicação, entre os números inteiros são válidas.

Proposição 2.7 (Regra de Sinais)**.** *Se $\alpha, \beta \in \mathbb{Z}$, então $(-\alpha)\cdot\beta = -(\alpha\cdot\beta) = \alpha\cdot(-\beta)$ e $(-\alpha)\cdot(-\beta) = \alpha \cdot \beta$.*

Demonstração. Se $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$, então $-\alpha = \overline{(b,a)}$ e $-\beta = \overline{(d,c)}$. Inicialmente mostraremos que $(-\alpha) \cdot \beta = -\alpha \cdot \beta = \alpha \cdot (-\beta)$. De fato,

$$(-\alpha) \cdot \beta = \overline{(b,a)} \cdot \overline{(c,d)} = \overline{(bc+ad, bd+ac)} = \overline{(ad+bc, ac+bd)}.$$

Analogamente, temos

$$-(\alpha \cdot \beta) = -\overline{(ac+bd, ad+bc)} = \overline{(ad+bc, ac+bd)}$$

e também

$$\alpha \cdot (-\beta) = \overline{(a,b)} \cdot \overline{(d,c)} = \overline{(ad+bc, ac+bd)}.$$

Logo, podemos concluir

$$(-\alpha) \cdot \beta = -\alpha \cdot \beta = \alpha \cdot (-\beta).$$

Veremos agora que $(-\alpha) \cdot (-\beta) = \alpha \cdot \beta$. É fácil ver que

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

Isto prova a proposição em questão. □

Para terminar esta subseção, exibiremos uma prova para a distributividade que envolve a multiplicação e a subtração entre números inteiros.

Proposição 2.8. *Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$. Então, $\alpha \cdot (\beta - \gamma) = \alpha \cdot \beta - \alpha \cdot \gamma$.*

Demonstração. Através da Proposição 2.7, as seguintes igualdades são claramente verdadeiras:

$$\alpha \cdot (\beta - \gamma) := \alpha \cdot [\beta + (-\gamma)] = \alpha \cdot \beta + \alpha \cdot (-\gamma) = \alpha\beta + (-\alpha\gamma) =: \alpha\beta - \alpha\gamma.$$

□

2.3 Relação de Ordem em $\mathbb{Z}$

Nesta seção, estamos interessados em discutir uma relação de ordem para o conjunto dos números inteiros; além disso, mostraremos que tal relação é compatível com as operações de multiplicação e adição em $\mathbb{Z}$, definidas na seção anterior. Por fim, provaremos que a lei de tricotomia permanece válida em $\mathbb{Z}$.

Comecemos, por usar a relação de ordem de $\mathbb{N}$, mostrando como definir quando um número inteiro é menor do que ou igual a outro.

Definição 2.9. Sejam $\overline{(a,b)}, \overline{(c,d)} \in \mathbb{Z}$. Dizemos que $\overline{(a,b)}$ é menor do que ou igual a $\overline{(c,d)}$, e escrevemos $\overline{(a,b)} \leq \overline{(c,d)}$, quando $a + d \leq b + c$.

Os símbolos $\geq, >$ e $<$ definem-se de forma análoga.

A primeira informação que desejamos transmitir, neste momento, é que a relação binária $\leq$, definida acima, é uma relação de ordem.

Proposição 2.9. *A relação $\leq$, estabelecida acima, é uma relação de ordem em $\mathbb{Z}$.*

Demonstração. Sejam, $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)} \in \mathbb{Z}$. Assim,

i) [Reflexividade]: Como $a + b = b + a$, temos que $\overline{(a,b)} \leq \overline{(a,b)}$;

ii) [Antissimetria]: Suponhamos $\overline{(a,b)} \leq \overline{(c,d)}$ e $\overline{(c,d)} \leq \overline{(a,b)}$. Assim,

$$a + d \leq b + c \text{ e } c + b \leq d + a,$$

donde concluímos, pela tricotomia em $\mathbb{N}$, que $a + d = b + c$, isto é, $\overline{(a,b)} = \overline{(c,d)}$ (ver Lema 2.1).

iii) [Transitividade]: Se $\overline{(a,b)} \leq \overline{(c,d)}$ e $\overline{(c,d)} \leq \overline{(e,f)}$, temos que

$$a + d \leq b + c \text{ e } c + f \leq d + e.$$

Daí, somando f a desigualdade acima, chegamos a

$$(a + d) + f \leq (b + c) + f.$$

Logo, inferimos

$$(a + f) + d \leq b + (c + f) \leq b + (d + e).$$

Consequentemente, $(a + f) + d \leq (b + e) + d$. Aplicando as propriedades da relação de ordem em $\mathbb{N}$, obtemos

$$a + f \leq b + e.$$

Logo, $\overline{(a,b)} \leq \overline{(e,f)}$.

Isto demonstra que $\leq$ é uma relação de ordem. □

Permita-nos checar a veracidade da compatibilidade da relação $\leq$ com as operações de adição e multiplicação entre os números inteiros.

Proposição 2.10. *Sejam $\alpha, \beta, \gamma \in \mathbb{Z}$. Então, valem as seguintes afirmações:*

i) $\alpha \leq \beta \Leftrightarrow \alpha + \gamma \leq \beta + \gamma$;

ii) $\alpha \leq \beta \Rightarrow \alpha\gamma \leq \beta\gamma$, *onde* $\gamma \geq \overline{(0,0)}$. *A recíproca desta afirmação é verdadeira se considerarmos* $\gamma > \overline{(0,0)}$.

iii) $\alpha \leq \beta \Rightarrow \alpha\gamma \geq \beta\gamma$, *onde* $\gamma \leq \overline{(0,0)}$. *A recíproca desta implicação é válida se assumirmos* $\gamma < \overline{(0,0)}$.

Demonstração. Sejam $\alpha = \overline{(a,b)}$, $\beta = \overline{(c,d)}$ e $\gamma = \overline{(e,f)}$.

i) ($\Rightarrow$) Se $\alpha \leq \beta$, então $a+d \leq b+c$. Somando $e+f$ em ambos os lados desta última desigualdade, obtemos

$$(a+e)+(d+f) = (a+d)+(e+f) \leq (b+c)+(e+f) = (b+f)+(c+e).$$

Segue que,

$$(a+e)+(d+f) \leq (b+f)+(c+e).$$

Portanto, podemos concluir

$$\overline{(a+e,b+f)} \leq \overline{(c+e,d+f)}.$$

Com isso, chegamos a

$$\overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)} + \overline{(e,f)}.$$

Por fim, inferimos que $\alpha + \gamma \leq \beta + \gamma$.

($\Leftarrow$) Agora, consideremos $\overline{(a,b)} + \overline{(e,f)} \leq \overline{(c,d)} + \overline{(e,f)}$. Daí,

$$\overline{(a+e,b+f)} \leq \overline{(c+e,d+f)}.$$

Assim sendo, podemos escrever

$$a+e+d+f \leq b+f+c+e.$$

Aplicando a lei do cancelamento de $\mathbb{N}$, temos que

$$a+d \leq b+c.$$

Logo, $\alpha \leq \beta$.

ii) ($\Rightarrow$) A hipótese se reescreve como: $a+d \leq b+c$ e $f \leq e$. Logo, existem $p, q \in \mathbb{N}$ tais que

$$b+c = (a+d)+p \text{ e } e = f+q. \tag{2.1}$$

Dessa forma, obtemos

$$(b+c)e = (a+d+p)e \text{ e } (b+c)f = (a+d+p)f.$$

Por conseguinte, chegamos a

$$be + ce = ae + de + pe \text{ e } bf + cf = af + df + pf.$$

Segue que

$$ae + de + pe + bf + cf = af + df + pf + be + ce. \tag{2.2}$$

Por outro lado, por (2.1), também temos que

$$pe = pf + pq \tag{2.3}$$

Assim, substituindo (2.3) em (2.2), encontramos

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

Segue que

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

desde que $pq \geq 0$. Com isso, encontramos

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

Isto nos diz que $\alpha\gamma \leq \beta\gamma$.

($\Leftarrow$) Suponha, agora, que $\alpha\gamma \leq \beta\gamma$, com $\gamma > \overline{(0,0)}$. Logo,

$$(a+d)e + (b+c)f \leq (a+d)f + (b+c)e$$

e também $f < e$. Sabemos que $e = f + p$, onde $p \in \mathbb{N}^*$. Logo,

$$(a+d)(f+p) + (b+c)f \leq (a+d)f + (b+c)(f+p).$$

Pela lei do cancelamento em $\mathbb{N}$, chegamos a $(a+d)p \leq (b+c)p$. Como $p > 0$ (ver Proposição 1.5), então temos que $a + d \leq b + c$. Isto nos informa que $\alpha \leq \beta$.

iii) Primeiramente, note que as seguintes equivalências são válidas para quaisquer $\alpha = \overline{(a,b)}, \beta = \overline{(c,d)}, \gamma = \overline{(e,f)} \in \mathbb{Z}$:

$$\begin{aligned}
\alpha(-\gamma) \leq \beta(-\gamma) &\Leftrightarrow \overline{(a,b)} \cdot \overline{(f,e)} \leq \overline{(c,d)} \cdot \overline{(f,e)} \\
&\Leftrightarrow \overline{(af+be, ae+bf)} \leq \overline{(cf+de, ce+df)} \\
&\Leftrightarrow af + be + ce + df \leq ae + bf + cf + de \\
&\Leftrightarrow \overline{(ce+df, cf+de)} \leq \overline{(ae+bf, af+be)} \\
&\Leftrightarrow \overline{(c,d)} \cdot \overline{(e,f)} \leq \overline{(a,b)} \cdot \overline{(e,f)} \\
&\Leftrightarrow \alpha\gamma \geq \beta\gamma.
\end{aligned} \tag{2.4}$$

($\Rightarrow$) Por hipótese, temos que

$$\overline{(e,f)} \leq \overline{(0,0)} \Rightarrow e \leq f \Rightarrow \overline{(0,0)} \leq \overline{(f,e)} = -\gamma.$$

Daí, como $\alpha \leq \beta$ e $-\gamma \geq \overline{(0,0)}$, por **ii**), temos $\alpha(-\gamma) \leq \beta(-\gamma)$. Por fim, por (2.4), chegamos a $\alpha\gamma \geq \beta\gamma$.

($\Leftarrow$) Agora suponhamos que $\alpha\gamma \geq \beta\gamma$ e $\gamma < \overline{(0,0)}$. Por (2.4), concluímos que $\alpha(-\gamma) \leq \beta(-\gamma)$. Como

$$\overline{(e,f)} < \overline{(0,0)} \Rightarrow e < f \Rightarrow \overline{(0,0)} < \overline{(f,e)} = -\gamma,$$

então, por **ii**), inferimos que $\alpha \leq \beta$.

Isto completa a prova do teorema em questão. □

Gostaríamos de destacar que a lei da tricotomia, provada para o conjunto $\mathbb{N}$, também vale para o conjunto dos números inteiros. Comecemos demonstrando o seguinte lema.

Lema 2.2. *Seja $\alpha \in \mathbb{Z}$. Então, apenas uma das situações deve ocorrer: $\alpha = \overline{(0,0)}$ ou $\alpha < \overline{(0,0)}$ ou $\alpha > \overline{(0,0)}$.*

Demonstração. Seja $\alpha = \overline{(a,b)}$. É sabido, através da tricotomia em $\mathbb{N}$, que ou $a = b$ ou $a < b$ ou $a > b$. Daí, concluímos que ou $a + 0 = b + 0$ ou $a + 0 < b + 0$ ou $a + 0 > b + 0$. Portanto, ou $\alpha = \overline{(0,0)}$ ou $\alpha < \overline{(0,0)}$ ou $\alpha > \overline{(0,0)}$. □

Agora estamos prontos para enunciar e provar a lei da tricotomia para números inteiros.

Corolário 2.11 (Tricotomia)**.** *Sejam $\alpha, \beta \in \mathbb{Z}$. Então, apenas uma das situações seguintes deve ocorrer: $\alpha = \beta$, ou $\alpha < \beta$ ou $\alpha > \beta$.*

Demonstração. Considere que $\alpha = \overline{(a,b)}$ e $\beta = \overline{(c,d)}$. Pela tricotomia em $\mathbb{N}$, temos que dados x, y naturais, apenas uma das situações seguintes ocorre: $x = y$ ou $x < y$ ou $x > y$. Tomemos $x = a + d$ e $y = b + c$. Daí, obtemos que ou $a + d = b + c$ ou $a + d < b + c$ ou $a + d > b + c$. Portanto, ou $\alpha = \beta$ ou $\alpha < \beta$ ou $\alpha > \beta$. □

2.4 Caracterização Usual de $\mathbb{Z}$

Nesta seção, utilizaremos as definições, bem como as propriedades, das relações $<, \leq, >, \geq$ em $\mathbb{Z}$, definida na seção anterior, com a finalidade de provar que o conjunto dos números inteiros pode ser identificado com a apresentação usual dada no ensino elementar.

Permita-nos começar com a definição de números inteiros positivos, negativos, não negativos e não positivos.

Definição 2.10. Dado $\overline{(a,b)} \in \mathbb{Z}$, dizemos que:

i) $\overline{(a,b)}$ é positivo quando $\overline{(a,b)} > \overline{(0,0)}$;

ii) $\overline{(a,b)}$ é não negativo quando $\overline{(a,b)} \geq \overline{(0,0)}$;

iii) $\overline{(a,b)}$ é negativo quando $\overline{(a,b)} < \overline{(0,0)}$;

iv) $\overline{(a,b)}$ é não positivo quando $\overline{(a,b)} \leq \overline{(0,0)}$.

Observe que $\overline{(a,b)} > \overline{(0,0)}$ significa $a + 0 > b + 0$, ou seja, $a > b$. De maneira análoga, temos que

$$\overline{(a,b)} \geq \overline{(0,0)} \Leftrightarrow a \geq b,\ \overline{(a,b)} < \overline{(0,0)} \Leftrightarrow a < b \text{ e } \overline{(a,b)} \leq \overline{(0,0)} \Leftrightarrow a \leq b.$$

Note ainda que se $\overline{(a,b)}$ é positivo, então existe $m \in \mathbb{N}^*$, tal que $a = b + m$. Logo, $a + 0 = b + m$. Dessa forma, $\overline{(a,b)} = \overline{(m,0)}$ (ver Lema 2.1). Analogamente, se $\overline{(a,b)}$ é negativo, então $b = a + n$, para algum $n \in \mathbb{N}^*$. Com isso, $b + 0 = a + n$. O que significa $\overline{(a,b)} = \overline{(0,n)}$ (ver Lema 2.1). Essas observações, juntamente com a lei da tricotomia em $\mathbb{Z}$, nos dizem que

$$\mathbb{Z} = \{\overline{(0,n)}/n \in \mathbb{N}^*\} \cup \{\overline{(0,0)}\} \cup \{\overline{(m,0)}/m \in \mathbb{N}^*\},$$

sendo a união disjunta.

A partir das observações feitas, passaremos a utilizar as seguintes notações:

$\mathbb{Z}_-^* = \{\overline{(0,n)}/n \in \mathbb{N}^*\}$, $\mathbb{Z}_- = \mathbb{Z}_-^* \cup \overline{(0,0)}$, $\mathbb{Z}_+^* = \{\overline{(m,0)}/m \in \mathbb{N}^*\}$ e $\mathbb{Z}_+ = \mathbb{Z}_+^* \cup \overline{(0,0)}$.

Consequentemente, $\mathbb{Z} = \mathbb{Z}_-^* \cup \mathbb{Z}_+^* \cup \{\overline{(0,0)}\}$.

Observe ainda que o conjunto, $\mathbb{Z}_+$ está em bijeção com $\mathbb{N}$, esta bijeção mostra que $\mathbb{Z}_+$ é uma cópia algébrica de $\mathbb{N}$, no sentido dado pelo teorema abaixo:

Teorema 2.12. Seja $f_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ dada por $f_{\mathbb{N}}(m) = \overline{(m, 0)}$, para todo $m \in \mathbb{N}$. Então, valem as seguintes afirmações:

i) $f_{\mathbb{N}}$ é injetora;

ii) $f_{\mathbb{N}}(m + n) = f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n)$;

iii) $f_{\mathbb{N}}(m \cdot n) = f_{\mathbb{N}}(m) \cdot f_{\mathbb{N}}(n)$;

iv) $m < n \Leftrightarrow f_{\mathbb{N}}(m) < f_{\mathbb{N}}(n)$, isto é, $f_{\mathbb{N}}$ é uma função estritamente crescente.

A função $f_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ acima é chamada imersão de $\mathbb{N}$ em $\mathbb{Z}$. Esta imersão mostra que $\mathbb{Z}$ é infinito, pois $f_{\mathbb{N}}$ é injetora e $\mathbb{N}$ é infinito (através da aplicação identidade).

Demonstração. Note que

i) $f_{\mathbb{N}}(m) = f_{\mathbb{N}}(n) \Leftrightarrow \overline{(m, 0)} = \overline{(n, 0)} \Leftrightarrow m + 0 = 0 + n \Leftrightarrow m = n$.

ii) $f_{\mathbb{N}}(m) + f_{\mathbb{N}}(n) = \overline{(m, 0)} + \overline{(n, 0)} = \overline{(m + n, 0)} = f_{\mathbb{N}}(m + n)$;

iii) $f_{\mathbb{N}}(m) \cdot f_{\mathbb{N}}(n) = \overline{(m, 0)} \cdot \overline{(n, 0)} = \overline{(mn + 0 \cdot 0, 0)} = \overline{(mn, 0)} = f_{\mathbb{N}}(mn)$;

iv) $m < n \Leftrightarrow m + 0 < 0 + n \Leftrightarrow \overline{(m, 0)} < \overline{(n, 0)} \Leftrightarrow f_{\mathbb{N}}(m) < f_{\mathbb{N}}(n)$.

Isto completa a prova do teorema em questão. □

Note que, o teorema acima nos mostrou que o conjunto $f_{\mathbb{N}}(\mathbb{N}) = \mathbb{Z}_+$ possui a mesma estrutura algébrica que $\mathbb{N}$. Por exemplo, $2 + 7 = 9$, em $\mathbb{N}$, corresponde, via $f_{\mathbb{N}}$, $\overline{(2, 0)} + \overline{(7, 0)} = \overline{(9, 0)}$ em $\mathbb{Z}$. Da mesma forma, $2 \cdot 7 = 14$ corresponde via $f_{\mathbb{N}}$, $\overline{(2, 0)} \cdot \overline{(7, 0)} = \overline{(14, 0)}$. Finalmente, a relação de $2 < 7$ se preserva via $f_{\mathbb{N}}$, com $\overline{(2, 0)} < \overline{(7, 0)}$. Em outras palavras, ordem em $\mathbb{Z}$ é uma extensão da ordem em $\mathbb{N}$.

Observe que se $a \in \mathbb{N}$, o simétrico de $\overline{(a, 0)}$ é $\overline{(0, a)}$, logo identificando $\overline{(a, 0)}$ com a através $f_{\mathbb{N}}$, obtemos $-a = -\overline{(a, 0)} = \overline{(0, a)}$. Obtemos assim, sob a identificação de $\mathbb{N}$ com $\mathbb{Z}_+$, via $f_{\mathbb{N}}$, que

$$\mathbb{Z} = \{-a / a \in \mathbb{N}^*\} \cup \{0\} \cup \mathbb{N}^* = \{..., -a, ..., -1, 0, 1, ..., a, ...\}.$$

Daí passamos a adotar esta identificação, considerando assim $\mathbb{N}$ um subconjunto de $\mathbb{Z}$. Sob tal identificação, obtemos, para n e m naturais, que

$$n - m = \overline{(n,0)} - \overline{(m,0)} = \overline{(n,0)} + [-\overline{(m,0)}] = \overline{(n,0)} + \overline{(0,m)} = \overline{(n,m)}.$$

Exemplo 2.6. Vamos efetuar as seguintes operações em $\mathbb{Z}$:

1) $3 - 5 = \overline{(3,5)} = \overline{(0,2)} = -2$;

2) $13 - 8 = \overline{(13,8)} = \overline{(5,0)} = 5$;

3) $(-3) \cdot 5 = \overline{(0,3)} \cdot \overline{(5,0)} = \overline{(0,15)} = -15$.

Vejamos, agora, como interpretar a regra de sinais para números inteiros, usando a identificação dada acima.

Proposição 2.11. *Sejam $x, y \in \mathbb{Z}$. Então, os seguintes itens valem:*

i) *$x > 0$ e $y > 0 \Rightarrow x \cdot y > 0$;*

ii) *$x < 0$ e $y < 0 \Rightarrow x \cdot y > 0$;*

iii) *$x < 0$ e $y > 0 \Rightarrow x \cdot y < 0$.*

Demonstração. Primeiramente, como x, y e 0 são inteiros, então podemos identificá-los com $\overline{(x,0)}$, $\overline{(y,0)}$ e $\overline{(0,0)}$.

i) Como x e y são inteiros positivos, podemos identificá-los com $\overline{(x,0)} > \overline{(0,0)}$ e $\overline{(y,0)} > \overline{(0,0)}$, via o Teorema 2.12. Daí,

$$\overline{(x,0)} \cdot \overline{(y,0)} > \overline{(0,0)} \cdot \overline{(y,0)} = \overline{(0,0)}.$$

Logo, $x \cdot y > 0$.

ii) Se $x < 0$ e $y < 0$, então $\overline{(x,0)} < \overline{(0,0)}$ e $\overline{(y,0)} < \overline{(0,0)}$. Logo,

$$\overline{(x,0)} \cdot \overline{(y,0)} > \overline{(x,0)} \cdot \overline{(0,0)} = \overline{(0,0)}.$$

Portanto, $xy > 0$.

iii) Se $x < 0$ e $y > 0$, então $\overline{(x,0)} < \overline{(0,0)}$ e $\overline{(y,0)} > \overline{(0,0)}$. Assim sendo,

$$\overline{(x,0)} \cdot \overline{(y,0)} < \overline{(x,0)} \cdot \overline{(0,0)} = \overline{(0,0)}.$$

Portanto, $xy < 0$.

□

2.5 Princípio da Boa Ordem em $\mathbb{Z}$

Nesta seção, estamos interessados em provar o Princípio da Boa Ordem para subconjuntos de números inteiros. Primeiramente, vamos definir quando um subconjunto de $\mathbb{Z}$ é limitado superior e inferiormente.

Definição 2.11. Seja X um subconjunto não vazio de $\mathbb{Z}$. Dizemos que X é limitado inferiormente se existe $\alpha \in \mathbb{Z}$ tal que $\alpha \leq x$, para todo $x \in X$. Tal α é chamado cota inferior de X. Analogamente, dizemos que X é limitado superiormente se existe $\beta \in \mathbb{Z}$ tal que $x \leq \beta$, para todo $x \in X$. Tal β é denominado cota superior de X.

Exemplo 2.7. Trivialmente, o número 0 é cota inferior para $\mathbb{N} \subset \mathbb{Z}$, pois $0 \leq x$, para todo $x \in \mathbb{N}$. Da mesma forma, -1 o é, bem como qualquer inteiro negativo.

Proposição 2.12. *O conjunto $\mathbb{N}$ é ilimitado em $\mathbb{Z}$, isto é, $\mathbb{N}$ não admite cota superior em $\mathbb{Z}$.*

Demonstração. Veremos que dado $\alpha \in \mathbb{Z}$, existe $x \in \mathbb{N}$ tal que $\alpha < x$. A prova desta afirmação será dividida em três casos:

1) Se $\alpha = 0$, basta tomarmos $x = 1 \in \mathbb{N}$, que teremos $\alpha < x$.

2) Se $\alpha < 0$, basta tomarmos qualquer natural x, que teremos $\alpha < x$.

3) Se $\alpha > 0$ podemos concluir que $\alpha \in \mathbb{N}^*$ e consequentemente $\alpha < s(\alpha) \in \mathbb{N}$. Assim sendo, para todo $\alpha > 0$ em $\mathbb{Z}$, existe um $x = s(\alpha) \in \mathbb{N}$, tal que $\alpha < x$.

□

Permita-nos provar o Princípio da Boa Ordem para o conjunto dos números inteiros $\mathbb{Z}$. Este mesmo princípio já foi provado ser válido em $\mathbb{N}$. Neste caso, qualquer subconjunto já possuia a propriedade de ser limitado inferiormente em $\mathbb{Z}$; com isso, esta condição não precisava ser assumida como hipótese. Em geral, os subconjuntos de $\mathbb{Z}$ não possuem esta característica. Portanto, tal suposição será considerada no próximo teorema.

Teorema 2.13 (Princípio da Boa Ordem em $\mathbb{Z}$)**.** *Seja $X \subset \mathbb{Z}$ não vazio e limitado inferiormente. Então X possui elemento mínimo.*

Demonstração. Seja α uma cota inferior de X, isto é, $\alpha \leq x, \forall x \in X$ (com $\alpha \in \mathbb{Z}$). Considere o conjunto $X^{'} = \{x - \alpha / x \in X\}$. Claramente, $X^{'} \subset \mathbb{N}$ (identificado com $\mathbb{Z}_{+}$) e, pelo Princípio da Boa Ordem em $\mathbb{N}$, o conjunto $X^{'}$, possui elemento mínimo, digamos m'. Assim,

$$m' \in X^{'} \text{ e } m' \leq y, \forall y \in X^{'}.$$

Como $m' \in X^{'}$, m' é da forma $m - \alpha$, para algum $m \in X$. Afirmamos que $m = m' + \alpha$ é elemento mínimo de X. Só falta verificar que $m \leq x$, $\forall x \in X$, mas isso equivale a $m - \alpha \leq x - \alpha$, $\forall x \in X$, ou seja, $m' \leq y, \forall y \in X^{'}$, que é verdade pela definição de m'. Logo, m é o elemento mínimo de X. □

O resultado a seguir nos garante que não existe número inteiro entre 0 e 1.

Corolário 2.14. *Seja $x \in \mathbb{Z}$ tal que $0 < x \leq 1$. Então, $x = 1$.*

Demonstração. Seja $X = \{x \in \mathbb{Z} / 0 < x \leq 1\}$. Segue daí que, $X \neq \varnothing$, pelo fato de $1 \in X$ e X é limitado inferiormente por 0. Pelo Princípio da Boa Ordem, X possui elemento mínimo, digamos m. Suponhamos que $0 < m < 1$. Assim, $0 < m^2 < m < 1$, o que implica que $m^2 \in X$, contrariando a minimalidade de m. Assim, $m = 1$ e, consequentemente $X = \{1\}$. □

Mais é verdade, não existe nenhum número inteiro entre dois inteiros consecutivos. Mais precisamente, temos o seguinte corolário.

Corolário 2.15. *Sejam $n, x \in \mathbb{Z}$ tais que $n < x \leq n + 1$. Então, $x = n + 1$.*

Demonstração. Note que,

$$n < x \leq n + 1 \Leftrightarrow 0 < x - n \leq 1.$$

Como $n, x \in \mathbb{Z}$, então $x - n \in \mathbb{Z}$. Assim, pelo Corolário 2.14, tem-se que $x - n = 1$. Por fim, $x = n + 1$. □

2.6 Módulo e Algoritmo da Divisão em $\mathbb{Z}$

Nesta seção, definiremos o módulo de um número inteiro em ordem a garantir que os únicos elementos inversíveis em $\mathbb{Z}$ são 1 e -1.

Definição 2.12. Seja $x \in \mathbb{Z}$. Definimos o valor absoluto de x (ou módulo de x), denotado por $|x|$, como sendo:

$$|x| = \begin{cases} x, \text{ se } x \geq 0; \\ -x, \text{ se } x < 0. \end{cases} \tag{2.5}$$

Exemplo 2.8. $|-6| = |6| = 6$; $|0| = 0$.

Proposição 2.13. As seguintes afirmações são verdadeiras:

1) $|x| = 0 \Leftrightarrow x = 0$;

2) $|x| \geq 0$, $\forall x \in \mathbb{Z}$;

3) $|xy| = |x||y|$, $\forall x, y \in \mathbb{Z}$;

4) Para $n \in \mathbb{N}^*$, tem-se: $|x| = n$ se, e somente se, $x = n$ ou $x = -n$.

Demonstração. **1)** ($\Rightarrow$) Primeiramente, note que se $|x| = 0$, então devemos considerar os seguintes casos:

- Se $x > 0$, então $x = |x| = 0$, contradição pela tricotomia em $\mathbb{Z}$.
- Se $x < 0$, então $-x = |x| = 0$, novamente contradição pela tricotomia em $\mathbb{Z}$.

Logo, $x = 0$.

($\Leftarrow$) Segue da definição de módulo.

2) Consideremos os casos abaixo:

- Se $x \geq 0$, por definição, $|x| = x \geq 0$;
- Se $x < 0$, por definição, $|x| = -x$. Por outro lado, temos que, $x < 0 \Rightarrow -x > 0$. Portanto, $|x| > 0$.

3) Para mostrar que $|xy| = |x||y|$, para todo $x, y \in \mathbb{Z}$. Vamos considerar 4 casos:

- Se $x = 0$ ou $y = 0$, temos que $xy = 0$. Logo, $|xy| = 0$. Como $|x| = 0$, claramente, $|x||y| = 0 \cdot |y| = 0$. Logo, $|xy| = |x||y|$.
- Se $x < 0$ e $y > 0$ (o caso $x > 0$ e $y < 0$ é análogo), então $xy < 0$, isto é, $|xy| = -xy$. Por outro lado, temos que $|x| = -x$ e $|y| = y$. Sendo assim,

$$|x||y| = (-x) \cdot y = -xy.$$

Logo, $|xy| = |x||y|$.

• Se $x < 0$ e $y < 0$, então $xy > 0$, assim $|xy| = xy$. Por outro lado, temos $|x| = -x$ e $|y| = -y$. Daí,

$$|x||y| = (-x) \cdot (-y) = xy.$$

Logo, $|xy| = |x||y|$.

• Se $x > 0$ e $y > 0$, então $xy > 0$. Assim, $|xy| = xy = |x||y|$. Portanto, $|xy| = |x||y|$, $\forall x, y \in \mathbb{Z}$.

4) ($\Rightarrow$) Suponha que $|x| = n$.

• Se $x \geq 0$, então $|x| = x$. Logo, $x = |x| = n$.

• Se $x < 0$, então $|x| = -x$. Sendo assim, $-x = |x| = n$. Portanto, $x = -n$.

($\Leftarrow$) Vamos estudar dois casos:

• Se $x = n$, então $|x| = |n|$. Como $n \in \mathbb{N}^*$, temos que $|n| = n$, ou seja, $|x| = n$.

• Se $x = -n$, então $|x| = |-n|$. Como $n \in \mathbb{N}^*$, temos que $n > 0 \Rightarrow -n < 0$. Sendo assim, $|-n| = -(-n) = n$. Portanto, $|x| = n$.

□

Estamos prontos para provar que nenhum número inteiro admite inverso multiplicativo, exceto -1 e 1.

Proposição 2.14. *Os únicos elementos inversíveis de $\mathbb{Z}$ são 1 e -1. Um elemento $x \in \mathbb{Z}$ diz-se inversível se existe $y \in \mathbb{Z}$ tal que $xy = 1$.*

Demonstração. Note que o elemento 0 não é inversível em $\mathbb{Z}$; caso contrário, existiria um $y \in \mathbb{Z}$, tal que $0 \cdot y = 1$. Mas, $0 \cdot y = 0$. Daí, teríamos $0 = 1$. Absurdo!

Seja $x \in \mathbb{Z}^*$ e $y \in \mathbb{Z}$ tais que $xy = 1$. Segue que $1 = |xy| = |x||y|$. Como $|x| \geq 0$ e $|y| \geq 0$ e $|x||y| = 1$, então $|x| > 0$ e $|y| > 0$ e daí resulta que $|x| \geq 1$ e $|y| \geq 1$. Multiplicando ambos os membros da última desigualdade por $|x|$, obtemos

$$1 = |x||y| \geq |x| \geq 1,$$

de onde segue que $|x| = 1$ (ver tricotomia). Portanto, pela Proposição 2.13, $x = 1$ ou $x = -1$, como queríamos. □

O próximo resultado nos mostra como dividir um número inteiro por outro (observe que, não necessariamente, o resultado é um elemento de $\mathbb{Z}$).

Teorema 2.16 (Algoritmo da Divisão em $\mathbb{Z}$)**.** *Sejam $x, d \in \mathbb{Z}$ tais que $d > 0$. Então, existe únicos $q, r \in \mathbb{Z}$ tais que*

$$x = dq + r, \text{ onde } 0 \leq r < d.$$

Aqui x, d, q e r são chamados dividendo, divisor, quociente e resto na divisão de x por d.

Demonstração. Existência: Primeiramente, note que se existe $q' \in \mathbb{Z}$ tal que $x = dq'$, então basta assumir $r = 0$ para obter

$$x = dq' + 0 = dq' + r, \text{ com } 0 \leq r < d.$$

Caso contrário, $x \neq dk$, para todo $k \in \mathbb{Z}$, existe $q \in \mathbb{Z}$ tal que

$$dq < x < d(q + 1). \tag{2.6}$$

De fato, se $x \geq 0$, então, pela prova do Teorema 1.19 (Algoritmo da Divisão em $\mathbb{N}$), podemos garantir que tal q existe e é natural. Se $x < 0$, então $-x > 0$; por conseguinte, existe $q \in \mathbb{N}$ tal que

$$dq < -x < d(q + 1),$$

ver Teorema 1.19 (Algoritmo da divisão em $\mathbb{N}$). Assim, por (2.6), segue que $0 < x - dq < d$, basta somar $-dq$ a (2.6). Seja $r = x - dq \in \mathbb{Z}$. Assim,

$$x = dq + r, \text{ com } 0 \leq r < d.$$

Unicidade: Suponhamos, agora, que existam $q_1, r_1 \in \mathbb{Z}$ tais que

$$x = dq_1 + r_1, \text{ onde } 0 \leq r_1 < d.$$

Assim, conclui-se que

$$dq + r = x = dq_1 + r_1.$$

Logo, $d(q - q_1) = r_1 - r$. Assuma, por absurdo, que $r_1 \neq r$. Sem perda de generalidade, considere que $r_1 > r$. Daí,

$$d(q - q_1) = r_1 - r > 0.$$

Todavia, $d > 0$. Dessa forma, $q - q_1 > 0$, isto é, $q - q_1 \geq 1$ (ver Proposição 1.9). Por conseguinte,

$$r_1 = d(q - q_1) + r \geq d,$$

pois $q - q_1 \geq 1$, $d > 0$ e $r \geq 0$. Isto é um absurdo, pois $r_1 < d$ (tricotomia). Dessa forma, $r_1 = r$. Consequentemente,

$$d(q - q_1) = r_1 - r = 0.$$

Por fim, $q = q_1$ (pois $d > 0$). □

É importante ressaltar que o Algoritmo da divisão em $\mathbb{Z}$ pode ser considerado com divisor negativo. Neste caso a divisão de $x \in \mathbb{Z}$ por $d \in \mathbb{Z}^*_-$ é dada através da igualdade

$$x = dq + r, \text{ onde } 0 \leq r < |d|,$$

onde q e r são únicos. Basta dividir x por $-d > 0$ para obter únicos $q, r \in \mathbb{Z}$ tais que

$$x = (-d)q + r, \text{ com } 0 \leq r < -d = |d|,$$

ver Teorema 2.16. Daí, $x = d(-q) + r$, com $0 \leq r < |d|$.

Uma aplicação que podemos fornecer para o Algoritmo da divisão em $\mathbb{Z}$ é que qualquer número inteiro n se escreve na forma $n = 2k$ (neste caso, n é dito inteiro par) ou $n = 2k' + 1$ (aqui, n é chamado inteiro ímpar), onde $k, k' \in \mathbb{Z}$.

Proposição 2.15. *Sejam* $2\mathbb{Z} = \{2n/n \in \mathbb{Z}\}$ (*conjunto dos números inteiros pares*) *e* $2\mathbb{Z} + 1 = \{2m + 1/m \in \mathbb{Z}\}$ (*conjunto dos números inteiros ímpares*). *Então,* $\mathbb{Z} = 2\mathbb{Z} \cup (2\mathbb{Z} + 1)$.

Demonstração. Seja $n \in \mathbb{Z}$. Pelo Algoritmo da divisão em $\mathbb{Z}$, temos que existem únicos $q, r \in \mathbb{Z}$ tais que

$$n = 2q + r, \text{ onde } 0 \leq r < 2.$$

Vimos que $r = 0$ ou 1 ($r \in \mathbb{N}$). Logo,

$$n = 2q \text{ ou } n = 2q + 1.$$

Assim, $n \in 2\mathbb{Z}$ ou $n \in 2\mathbb{Z} + 1$. Isto prova que $\mathbb{Z} \subseteq 2\mathbb{Z} \cup (2\mathbb{Z} + 1)$. A inclusão recíproca é trivial. □

2.7 Fatorização Única em $\mathbb{Z}$

Nosso objetivo, nesta seção, é provar o famoso Teorema Fundamental da Aritmética. Este, por sua vez, fala sobre a fatorização de um número inteiro em um produto de números primos.

Primeiramente, vamos definir o significado de um número inteiro ser múltiplo de um outro.

Definição 2.13. Seja $x \in \mathbb{Z}$. Os números inteiros da forma $kx, k \in \mathbb{Z}$, são chamados múltiplos de x. Neste caso, também dizemos que tais números são divisíveis por x ou que x é um divisor de tais valores.

Exemplo 2.9. Os múltiplos do número inteiro 2 são

$$0, \pm 2, \pm 4, \pm 6, ...$$

Definição 2.14. Sejam $x, y \in \mathbb{Z}$. Dizemos que x divide y, e escrevemos $x|y$, quando $\exists k \in \mathbb{Z}$ tal que $y = kx$, i.e, quando y é um múltiplo de x.

Obs 2.1. $x|y \Leftrightarrow y$ é divisível por $x \Leftrightarrow x$ é um divisor de y.

A seguir, apresentaremos alguns propriedades elementares envolvendo $|$.

Proposição 2.16. *Sejam $x, y, z \in \mathbb{Z}$. Os seguintes itens são verdadeiros:*

i) [*Reflexividade*]*: $x|x$;*

ii) *$x|y$ e $y|x \Rightarrow \pm x = y$;*

iii) [*Transitividade*]*: $x|y$ e $y|z \Rightarrow x|z$;*

Demonstração. **i)** Note que $x = x \cdot 1, \forall x \in \mathbb{Z}$. Logo, $x|x$.

ii) Se $x|y$ e $y|x$, então $\exists q_1, q_2 \in \mathbb{Z}$ tais que

$$y = q_1 x \text{ e } x = q_2 y.$$

Logo,

$$x = q_2(q_1 x) = (q_2 q_1)x.$$

Se $x = 0$, então o resultado tem seguimento trivial. Assim, considere que $x \neq 0$. Pela lei do corte, chegamos a $q_2 q_1 = 1$. Portanto, pela Proposição 2.14, concluímos que $q_1 = \pm 1$. Por fim, $y = \pm x$.

iii) Se $x|y$ e $y|z$, então $\exists q_1, q_2 \in \mathbb{Z}$ tais que

$$y = q_1 x \text{ e } z = q_2 y.$$

Daí,

$$z = q_2(q_1 x) = (q_2 q_1)x.$$

Logo, $x|z$ (pois $q_0 q_1 \in \mathbb{Z}$).

□

Agora vejamos como podemos definir, precisamente, um número inteiro primo.

Definição 2.15. Seja $p \in \mathbb{Z}$. Dizemos que p é número primo se

i) $p \neq 0$ e $p \neq \pm 1$;

ii) $d|p \Rightarrow d = \pm p$ ou $d = \pm 1$ (os únicos divisores de p são $\pm p$ e ± 1).

Um número que não é primo é chamado composto.

Exemplo 2.10. 6 é um número composto, pois $2|6$. Por outro lado, 2 é um número primo, pois os únicos divisores de 2 são ± 1 e ± 2.

Lema 2.3. *Sejam $p, x \in \mathbb{Z}$, tais que $p \neq 0$. Se p é primo e $p \nmid x$, então existem $y, z \in \mathbb{Z}$ tais que* $1 = py + xz$.

Demonstração. Suponha, inicialmente, que $p \in \mathbb{N}^*$. Seja $X = \{pa + xb \in \mathbb{N}^* / a, b \in \mathbb{Z}\}$. Como $p \in X$, pois $p = p \cdot 1 + x \cdot 0 > 0$, então $X \neq \emptyset$. Logo, pelo Princípio da Boa Ordem em $\mathbb{N}$, temos que existe $d = \min X$. Como $d \in X$, então

$$d = py + xz,\ y, z \in \mathbb{Z}.$$

Vamos provar que $d = 1$. Já sabemos que $d \geq 1$. Suponha, então, por contradição, que $d > 1$. Pelo Algoritmo da Divisão, temos que existem únicos $q, r \in \mathbb{Z}$ tais que $p = dq + r,$ onde $0 \leq r < d$. Desta forma,

$$r = p - dq = p - pyq - xzq = p(1 - yq) + x(zq).$$

Isto nos diz que $r \in X$. Mas, $0 \leq r < d = \min X$. Logo, $r = 0$. Com isso, $p = dq$. Portanto, $d|p$. Consequentemente, como p é primo e $d > 1$, chegamos a $d = p$. Analogamente, pelo Algoritmo da Divisão, temos que existem únicos $q', r' \in \mathbb{Z}$ tais que $x = dq' + r',$ onde $0 \leq r' < d$. Desta forma,

$$r' = x - dq' = x - pyq' - xzq' = p(-yq') + x(1 - zq').$$

Isto nos diz que $r' \in X$. Todavia, $0 \leq r' < d = \min X$. Deste modo, $r' = 0$. Com isso, $x = dq' = pq'$. Por fim, $p|x$. Isto é uma contradição ($p \nmid x$). Por conseguinte, $d = 1$, isto é,

$$1 = py + xz,\ y, z \in \mathbb{Z}.$$

O caso $p < 0$ é trivial, pois, nesta situação, $-p > 0$ e, daí,

$$1 = (-p)y + xz, y, z \in \mathbb{Z}.$$

Portanto, $1 = p(-y) + xz,\ -y, z \in \mathbb{Z}$. □

A seguir estabeleceremos uma outra maneira de caracterizar números inteiros primos.

Teorema 2.17 (Lema de Euclides)**.** *Sejam $p, x, y \in \mathbb{Z}$ tais que $p \neq 0$. Então, p é primo se, e somente se, $p|xy \Rightarrow p|x$ ou $p|y$.*

Demonstração. ($\Rightarrow$) Seja p primo e suponha que $p|xy$. Considere que $p \nmid x$. Daí, pelo Lema 2.3, existem $a_0, b_0 \in \mathbb{Z}$ tais que $1 = a_0 p + b_0 x$. Como $p|xy$, então $xy = pk$, para algum $k \in \mathbb{Z}$. Logo,

$$y = a_0 py + b_0 xy = (a_0 y)p + (b_0 k)p = [a_0 y + b_0 k]p \Rightarrow p|y.$$

($\Leftarrow$) Suponha que $p|xy \Rightarrow p|x$ ou $p|y$. Se p não é primo, então $\exists x \neq \pm p$ e $x \neq \pm 1$ tal que $x|p$. Daí $\exists y \in \mathbb{Z}$ tal que $p = xy$. Dessa forma, $p|xy$. Consequentemente, $p|x$ ou $p|y$. Se $p|x$, então $x = \pm p$ (já que $x|p$). Isto é uma contradição ($x \neq \pm p$). Se $p|y$, então $y = \pm p$ (já que $y|p$). Daí, $p = \pm xp$. Deste modo, pela lei do cancelamento, $x = \pm 1$. Um absurdo ($x \neq \pm 1$). Por fim, p é primo. □

O Teorema 2.17 pode ser generalizado da seguinte forma:

Proposição 2.17. *Sejam $p, x_1, x_2, ..., x_n \in \mathbb{Z}$ tais que $p \neq 0$. Então, p é primo se, e somente se, $p|x_1 \cdot x_2 \cdot ... \cdot x_n \Rightarrow p|x_i$ para algum $i = 1, 2, ..., n$.*

Demonstração. Faremos a prova por indução sobre n. Seja

$$X = \{n \in \mathbb{N}^* / p|x_1 \cdot x_2 \cdot ... \cdot x_n \Rightarrow p|x_i, i = 1, 2, ..., n\}.$$

Nada há a fazer com o caso $n = 1$. Considere que

$$p|x_1 \cdot x_2 \cdot ... \cdot x_n \Rightarrow p|x_i, i = 1, 2, ..., n.$$

Suponha que $n \in X$, isto é, $p|x_1 \cdot x_2 \cdot ... \cdot x_n \cdot x_{n+1}$, então, pelo Teorema 2.17, temos que $p|x_1 \cdot x_2 \cdot ... \cdot x_n$ ou $p|x_{n+1}$. Dessa forma, $p|x_i$, para algum $i = 1, 2, ..., n + 1$, pela hipótese de indução. Isto nos diz que $n + 1 \in X$. Dessa forma, $X = \mathbb{N}^*$. □

Precisaremos do lema abaixo para provar o Teorema Fundamental da Aritmética.

Lema 2.4. *Seja $x \in \mathbb{Z}$ tal que $x \neq 0$ e $x \neq \pm 1$. Então, $\min\{y \in \mathbb{Z} / y > 1, y|x\}$ é primo.*

Demonstração. Seja $S = \{y \in \mathbb{Z} / y > 1, y|x\}$. Note que $|x| > 1$ ($x \neq 0$) e $|x||x$. Daí, $|x| \in S$. Isto nos diz que $S \neq \emptyset$. Além disso, S é limitado inferiormente por 1. Pelo Princípio da Boa Ordem, $\exists p = \min S$. Como $p \in S$, então $p > 1$. Logo, $p \neq 0$ e $p \neq \pm 1$.

Agora suponha, por absurdo, que existe $q \in \mathbb{Z}$ tal que $q \neq \pm 1$ e $q \neq \pm p$ e $q|p$. Consequentemente, $|q| > 1$ e $|q||p$. Dessa forma, $1 < |q| < p$. De fato, se $|q| > p$ ($|q| \neq p$), então, usando que $|q||p$ ($p = |q|k$, para algum $k \in Z_+^*$), teríamos

$$p = |q|k > pk \geq p,\ k \in \mathbb{Z}_+^*.$$

Uma contradição. Como $p \in S$, então $p|x$. Daí, por transitividade, $|q||p$ e $p|x \Rightarrow |q||x$. Isto nos diz que $1 < |q| < p$ e $|q||x$. Ou seja, $|q| \in S$ e $|q| < p = \min S$. Um absurdo! Por fim, p é primo. □

Teorema 2.18 (Teorema Fundamental da Aritmética)**.** *Seja $x \in \mathbb{Z}$ tal que $x > 1$. Então existem $p_1, p_2, ..., p_k$ números primos positivos $(k \geq 1)$ tais que $x = p_1 \cdot ... \cdot p_k$. Além disso, $x = q_1 \cdot ... \cdot q_s$, onde $q_1, q_2, ..., q_s$ $(s \geq 1)$ são números primos positivos, então $k = s$ e cada p_i é igual a um q_j.*

Demonstração. Usaremos o Princípio da Indução na Segunda forma sobre x.

i) Se $x = 2$, então $x = 2$, com $k = 1$ e $p_1 = 2$.

ii) Agora suponhamos que para todo $y \in \mathbb{Z}$ tal que $2 \leq y < x$, tem-se que $y = p_1 \cdot ... \cdot p_{k'}$, $(k' \geq 1)$, onde p_i é primo positivo, para todo $i = 1, 2, ..., k'$. Pelo Lema 2.4, temos que $\exists p$ primo tal que $p > 1$ e $p|x$. Assim, $\exists q \in \mathbb{Z}$ tal que $x = qp$. Note que se $q = 1$, então $x = p$ e o resultado estaria provado. Se q fosse primo, então $x = qp$. Assim sendo, o resultado seguiria. Dessa forma, considere que $2 \leq q < x$ $(q > 1)$. Por hipótese de indução, $q = p_1 \cdot ... \cdot p_{k'}$, onde p_i é primo positivo, para todo $i = 1, 2, ..., k'$. Portanto, $x = p_1 \cdot ... \cdot p_{k'} \cdot p$. Por fim, o resultado é válido por indução.

Agora suponha que

$$x = p_1 \cdot ... \cdot p_k = q_1 \cdot ... \cdot q_s,$$

onde q_j e p_i são primos positivos, para todo $j = 1, 2, ..., s$ e $i = 1, 2, ..., k$. Assim, $p_1|q_1 \cdot ... \cdot q_s$. Pelo Lema 2.17, $p_1|q_j$, para algum $j = 1, 2, ..., s$. Suponhamos, sem perda de generalidade, que $p_1|q_1$. Como q_1 é primo, então $p_1 = \pm q_1$ (já que $p_1 \neq \pm 1$). Como $p_1, q_1 > 0$, então $p_1 = q_1$. Portanto,

$$q_1 \cdot p_2 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_s.$$

Logo,

$$q_1(p_2 \cdot ... \cdot p_k - q_2 \cdot ... \cdot q_s) = 0.$$

Isto nos diz que

$$p_2 \cdot ... \cdot p_k = q_2 \cdot ... \cdot q_s.$$

Considere que $k \neq s$. Sem perda de generalidade, digamos que $k < s$. Usando o processo acima, chegamos a

$$1 = q_{k+1} \cdot ... \cdot q_s.$$

Isto implicaria, pela Preposição 2.14 que $q_{k+1} = \pm 1$. Um absurdo! Logo, $k = s$ e $p_i = q_i$, para todo $i = 1, 2, ..., k$.

□

Obs 2.2. Seja $x \in \mathbb{Z}$ tal que $x \neq 0$ e $x \neq \pm 1$. Se $x > 0$, podemos escrever x como um produto finito de inteiros primos positivos de maneira única (Teorema Fundamental da Aritmética). Se $x < 0$, então $-x = p_1 \cdot ... \cdot p_k$, onde p_i é primo positivo, para todo $i = 1, 2, ..., k$. Logo, $x = -p_1 \cdot ... \cdot p_k$. Geralmente, temos, então, $x = \pm p_1 \cdot ... \cdot p_k$ onde os p_i é primo positivo, para todo $i - 1, 2, ..., k$ (a igualdade acontecendo de maneira única).

2.8 Enumerabilidade de $\mathbb{Z}$

Nesta seção, estamos interessados em provar que o conjunto dos números inteiros $\mathbb{Z}$, assim como $\mathbb{N}$, é enumerável. Vamos direto ao nosso objetivo.

Teorema 2.19. $\mathbb{Z}$ é enumerável.

Demonstração. Vamos provar que $\sigma : \mathbb{Z} \to \mathbb{N}$ definida por

$$\sigma(n) = \begin{cases} 2n - 1, \text{ se } n > 0; \\ -2n, \text{ se } n \leq 0, \end{cases}$$

é bijetora. Na verdade, vamos mostrar que σ é inversível exibindo sua inversa. De fato, seja $\sigma^{-1} : \mathbb{N} \to \mathbb{Z}$, dada por

$$\sigma^{-1}(n) = \begin{cases} k + 1, \text{ se } n = 2k + 1; \\ -k', \text{ se } n = 2k', \end{cases}$$

onde $k, k' \in \mathbb{Z}$. Podemos ver que, se $n > 0$, temos que

$$\sigma^{-1} \circ \sigma(n) = \sigma^{-1}(\sigma(n)) = \sigma^{-1}(2n - 1) = \sigma^{-1}(2(n - 1) + 1) = (n - 1) + 1 = n.$$

Por outro lado, podemos concluir, para $n \leq 0$, que

$$\sigma^{-1} \circ \sigma(n) = \sigma^{-1}(\sigma(n)) = \sigma^{-1}(-2n) = \sigma^{-1}(2(-n)) = -(-n) = n.$$

Do mesmo modo, podemos concluir, para $n = 2k + 1$, que

$$\sigma \circ \sigma^{-1}(n) = \sigma(\sigma^{-1}(2k + 1)) = \sigma(k + 1) = 2(k + 1) - 1 = 2k + 1 = n.$$

Por outro lado, inferimos, para $n = 2k'$, que

$$\sigma \circ \sigma^{-1}(n) = \sigma(\sigma^{-1}(2k')) = \sigma(-k') = (-2)(-k') = 2k' = n.$$

Como $\sigma^{-1} \circ \sigma = I_{\mathbb{N}}$ (identidade) e $\sigma \circ \sigma^{-1} = I_{\mathbb{Z}}$ (identidade), fica claro que σ é inversível. Logo, σ é bijetora. Por fim, $\mathbb{Z}$ é enumerável. □

2.9 Uma aplicação dos números inteiros

2.9.1 Congruência

Além da aritmética usual no conjunto dos números inteiros, podemos explorar uma aritmética modular que envolve o conceito de congruência módulo m (m inteiro maior que 1) . Carl Friedrich Gauss foi o grande introdutor da congruência, ele começou a mostrar ao mundo a congruência a partir de um trabalho realizado em 1801, Disquisitiones Arithmeticae, quando tinha apenas 24 anos de idade. Várias ideias usadas na teoria dos números foram introduzidas neste trabalho, até mesmo o símbolo usado na congruência atualmente foi o que Gauss usou naquela época.

As operações de adição e multiplicação são definidas em um conjunto finito Zm cujos elementos são classes residuais, sendo cada classe, um subconjunto de números inteiros que têm restos da divisão por m sempre iguais a um determinado resto r. A congruência modulo m e aritmética modular têm muitas aplicações. Dentre elas, a justificativa para critérios de divisibilidade, exemplificação de conceitos que envolvem as propriedades das operações, construção de códigos e no estudo e modelagem de fenômenos periódicos que envolvem diferentes campos do conhecimento como: matemática (teoria dos jogos, teoria dos grafos), física, artes, música e etc..

A ideia de congruência é a seguinte: quando nos deparamos com um problema que relacione divisões, potenciações, etc., por que não trabalhamos com os restos das divisões ao invés dos próprios números? Quer dizer, por que não nos esquecemos dos números e ficamos apenas com os restos? Uma vez que esses restos são menores do que os números, é de se esperar que isso simplifique a solução desses problemas, o que de fato ocorre! Antes da nossa aplicação, vamos ver um pouco de teoria.

2.9.2 Congruência Módulo M

A congruência módulo m é uma relação de equivalência no conjunto dos números inteiros de tal forma que dados dois inteiros a e b, a é congruente a b módulo m, onde m é um número inteiro

positivo, se e somente se, a diferença $a - b$ for divisível por m. Usaremos a notação por $a \equiv b$(mod m), se os números inteiros a e b são congruentes módulo m ($m \ni \mathbb{Z}$, $m > 0$).

São válidos os seguintes resultados:

Se a e b são inteiros, temos que $a \equiv b$(mod m) se, e somente se, existir um inteiro q tal que $a - b = q.m$.

A congruência define uma relação de equivalência, pois atende às propriedades reflexiva, simétrica e Transitiva.

Se a, b, c e m são inteiros, $m > 0$, tais que $a \equiv b$(mod m), então:
• Se $a \equiv b$(mod m) existe um número inteiro k tal que $a = b + km$;
• Sempre $a \equiv a$(mod m);
• Se $a \equiv b$(mod m) então $b \equiv a$(mod m);
• Se $a \equiv b$(mod m) e $b \equiv c$(mod m) então $a \equiv c$(mod m);
• Se $ac \equiv b$(mod m) e $c \equiv d$(mod m) então $ad \equiv b$(mod m);
• Se $a \equiv b$(mod m), então $(a + c) \equiv (b + c)$(mod m), onde c é um inteiro;
• Se $a \equiv b$(mod m), então $(a - c) \equiv (b - c)$(mod m), onde c é um inteiro;
• Se $a \equiv b$(mod m), então $a.c \equiv b.c$(mod m), onde c é um inteiro;
• Se $a \equiv b$(mod m) e $c \equiv d$(mod m) então $a + c \equiv b + d$(mod m);
• Se $a \equiv b$(mod m) e $c \equiv d$(mod m) então $a - c \equiv b - d$(mod m);
• Se $a \equiv b$(mod m) e $c \equiv d$(mod m) então $a.c \equiv b.d$(mod m);
• Se $a.c \equiv b.c$(mod m), então $a \equiv b$(mod m/d), onde d é o máximo divisor comum de c e m.

2.9.3 Aritmética Modular

Neste texto, vamos considerar o conjunto $\mathbb{Z}_m = 0, 1, 2, .., m - 1$, sendo m um número inteiro positivo e r pertencente a $\mathbb{Z}_m$ uma classe residual, ou seja, r = y pertencentes a $\mathbb{Z} : r \equiv y$(mod m). Podemos observar que a classe residual r é formada por todos os números inteiros cuja divisão por m tem resto r. Definimos então as seguintes operações módulo m. Para todo a e b pertencentes a $\mathbb{Z}_m$, temos:

1. $a + b = r$, se r é o resto da divisão de $(a + b)$ por m;
2. $r \equiv (a + b)$(mod m) (adição modular)
3. $a.b = s$ se s é o resto da divisão de $(a.b)$ por m;

4. $s \equiv (a.b)(\text{mod m})$ (multiplicação modular)

Por exemplo, dado $Z_7 = 0, 1, 2, .., 7 - 1 = 0, 1, 2, .., 6$ então, $3 + 5 = (3 + 5) = 1$, pois $3 + 5 = 8$ e o resto da divisão de 8 por 7 é 1 , logo $8 \equiv 1(\text{mod } 7)$ e $4.5 = (4.5) = 6$, pois 4 vezes 5 é 20 e o resto da divisão de 20 por 7 é 6, logo $20 \equiv 6(\text{mod } 7)$.

As operações acima estão bem definidas e independem dos representantes das classes. Na aritmética modular, trabalhamos com o conceito de congruência módulo m. São válidas as seguintes propriedades em relação às operações de adição e multiplicação modular:

Sejam a, b, c elementos quaisquer de $\mathbb{Z}_m$ e m um número inteiro positivo então,

1. $a + b$ e $a.b$ pertencem a $\mathbb{Z}_m$ (fechamento)
2. $a + b = b + a$ e $a.b = b.a$ (comutatividade)
3. $(a + b) + c = a + (b + c)$ e $(a.b).c = a.(b.c)$(associatividade)
4. $a+0 = 0+a = a$ e $a.1 = 1.a = a$ (existência de elemento neutro, sendo 0 e 1, respectivamente, os elementos neutros da adição e da multiplicação em $\mathbb{Z}_m$). No caso da multiplicação, a não pode ser igual a 0.
5. $a.(b + c) = a.b + a.c$ (distributividade)
6. $a + (m - a) = (m - a) + a = 0$ (sendo m- a o elemento simétrico aditivo de a em $\mathbb{Z}_m$)

Além das propriedades acima, podemos garantir que, um elemento de $\mathbb{Z}_m$ terá simétrico multiplicativo (inverso) se ele e m forem primos entre si e diferentes de 0. Nesse caso, dado a pertencente a $\mathbb{Z}_m$ tal que MDC(a,m)=1 então existe b pertencente a $\mathbb{Z}_m$, tal que $a.b = 1$. Em $\mathbb{Z}_6$, todos os elementos têm simétrico aditivo, o mesmo não acontece quanto aos simétricos multiplicativos. Por exemplo, como o MDC(2,6)=2, logo não existe y tal que $2.y = 1$. De fato, $2.0 = 0$, $2.1 = 2$, $2.2 = 4$, $2.3 = 0$, $2.4 = 2$, $2.5 = 4$.

2.9.4 A equação linear numa variável

Consideramos a equação

$$ax \equiv b(\text{mod m})$$

De acordo com as definições dadas, um inteiro x será uma solução se existir $y \in \mathbb{Z}$ tal que $ax - b = my$. Seja $d = mdc(a, m)$; resulta diretamente da última equação que para que exista solução é necessário que $d \mid b$ pois $b = ax - my$.

Por outro lado, sabemos que existem inteiros x_0 e y_0 tais que

$$ax_0 + my_0 = d$$

x_0 e y_0 podem ser determinados por aplicação do algoritmo de Euclides com que se calcula d.

Mas então, se $d \mid b$, temos que

$$ax_0\frac{b}{d} + my_0\frac{b}{d} = b$$

e vemos que a equação modular tem a solução $x = x_0\dfrac{b}{d}$ (ou, mais precisamente, a classe de congruência deste número).

Que outras soluções (não congruentes com esta, claro) existem? Suponhamos que z e w satisfazem igualmente $az - mw = b$; então:

$$az - mw = ax - my \Leftrightarrow a(z - x) = m(w - y) \Leftrightarrow \frac{a}{d}(z - x) = \frac{m}{d}(w - y)$$

mas, como $\dfrac{a}{d}$ e $\dfrac{m}{d}$ são primos entre si, isso implica que:

$$\frac{m}{d} \mid (z - x)$$

ou seja

$$z = x + k\frac{m}{d}$$

Duas soluções desta forma serão congruentes m módulo m se $d \mid k$. Temos portanto d soluções distintas, correspondendo aos valores $0 \leq k < d$. Resumindo,

Proposição 2.18. *Para $m \in \mathbb{N}$, a inteiro e $d = mdc(a.m)$, a equação*

$$ax \equiv b(mod\ m)$$

tem d soluções distintas se $d \mid b$ e não tem soluções caso contrário. Se x_0 e y_0 são inteiros satisfazendo $ax_0 + my_0 = d$, as soluções do primeiro caso são

$$x_0\frac{b}{d} + k\frac{m}{d},\ 0 \leq k < d$$

É importante notar a seguinte interpretação deste resultado no caso $d = 1$; $mdc(a, m) = 1$ significa que a classe de a é invertível para a multiplicação em $\mathbb{Z}_m$: se $au + mv = 1$, então a classe de u é a inversa da classe de a; a solução da congruência

$$ax \equiv b(\text{mod m})$$

é, como numa equação "habitual", $x = a^{-1}b$ (em que a^{-1} designa a classe inversa da de a).

Por outro lado, no caso geral, se $d = mdc(a, m)$ divide b podemos observar que

$$ax \equiv b(\text{mod m}) \Leftrightarrow m \mid (ax - b) \Leftrightarrow \frac{m}{d} \mid (\frac{a}{d}x - \frac{b}{d}) \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d}(\text{mod } \frac{m}{d})$$

Assim, podemos começar por encontrar a solução (única) t desta última congruência e notar que as soluções da congruência inicial são as classes (mod m) dadas por $t + k\frac{m}{d}$ com $0 \leq k < d$, que são as classes de congruência módulo m que estão contidas na classe de t mod$(\frac{m}{d})$.

2.9.5 Um exemplo na Astronomia

Agora podemos realizar a nossa aplicação do capítulo.

Três satélites passarão sobre o Rio esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

Formulando o problema, usando nossa interpretação do módulo como o período de um movimento que se repete a intervalos regulares. Neste caso, o movimento é o dos satélites que giram em torno da Terra.

Chamaremos de x o número de horas, contadas a partir da meia noite de hoje, quando os três satélites passarão juntos sobre o Rio. O primeiro satélite passa sobre o Rio a cada 13 horas, a

contar da 1 da madrugada. Logo precisamos ter $x = 1 + 13.n_1$ para algum inteiro positivo n_1 que representa o número de voltas que o satélite 1 tem que dar em torno da Terra antes que passe junto com os dois outros satélites.

As equações correspondentes aos outros dois satélites são: $x = 4 + 15.n_2$ e $x = 8 + 19.n_3$; onde n_2 e n_3 representam o número de voltas que os satélites 2 e 3 darão antes dos três passarem juntos.

Podemos formular estas equações em termos de congruência, o que nos dá:

$$x \equiv 1 \pmod{13}$$
$$x \equiv 4 \pmod{15}$$
$$x \equiv 8 \pmod{19}$$

Começaremos a solução com as duas últimas equações. Tomando a última equação e substituindo-a na penúltima congruência, obtemos: $8 + 19n_3 \equiv 4(\text{mod } 15)$; que equivale a $19n_3 \equiv -4(\text{mod } 15)$.

Como $19 \equiv 4(\text{mod } 15)$, isto nos dá: $4n_3 \equiv -4(\text{ mod } 15)$. Como 4 é inversível módulo 15, podemos cancelá-lo de modo que $n_3 \equiv -1 \equiv 14(\text{mod } 15)$.

Assim, $n_3 = 14 + 15.n_4$, para algum inteiro positivo n_4. Mas, segundo a terceira equação, $x = 8 + 19.n_3$. Combinando estas duas expressões temos $x = 8 + 19(14 + 15.n_4) = 274 + 285.n_4$.

O que isso representa? Certamente não é a solução do problema, já que sequer usamos as condições impostas pelo primeiro satélite. Entretanto, como é fácil verificar usando congruências, $x = 274 + 285.n_4$ nos dá uma solução das duas últimas equações. Isto significa que esta família de soluções deve corresponder aos tempos nos quais os satélites 2 e 3 passam juntos sobre o Rio. E quanto ao satélite 1? Para incluir na solução a informação referente ao primeiro satélite, basta encontrar as soluções da forma $x = 274 + 285.n_4$ (isto é, as soluções comuns aos satélites 2 e 3) que, além disso, satisfazem a congruência $x \equiv 1(\text{mod } 13)$, relativa ao primeiro satélite. Efetuando a substituição, temos: $274 + 285.n_4 \equiv 1(\text{mod } 13)$; que depois da redução módulo 13 nos dá: $1 + 12.n_4 \equiv 1(\text{mod } 13)$.

Logo $12n_4 \equiv 0(\text{mod } 13)$ e , como 12 é inversível módulo 13, concluímos que $n_4 = 13.n_5$. Desta forma, a solução final será: $x = 274 + 285n_4 = 274 + 285(13.n_5) = 274 + 3705.n_5$, onde é fácil verificar substituindo esta fórmula para x nas congruências abaixo:

$$x \equiv 1(\text{mod } 13)$$
$$x \equiv 4(\text{mod } 15)$$

$$x \equiv 8(\text{mod } 19)$$

Resta-nos explicitar o que esta solução nos diz sobre os satélites. Em primeiro lugar, como é fácil verificar, 274 é o menos inteiro positivo que satisfaz as três congruências acima. Portanto, os satélites passam juntos sobre o céu do Rio pela primeira vez 274 horas depois da meia noite de hoje. Isto equivale a 11 dias e 10 horas. Mas isto não é tudo. Afinal, não importa qual seja o valor de n_5, a fórmula $274 + 3705.n_5$ nos dá uma solução do problema. Portanto, depois de passar juntos uma vez sobre o Rio 274 horas depois da zero hora de hoje, os satélites passarão juntos novamente a cada 3705 horas; isto é, a cada 154 dias e 9 horas.

Capítulo 3

Construção dos Números Racionais

Neste capítulo, estudaremos a construção dos chamados números racionais a partir da estrutura aritmética que temos em $\mathbb{Z}$ e das propriedades da relação de equivalência exposta no capítulo anterior. A referência que serviu como base neste capítulo está apresentada em [3].

3.1 O Conjunto dos Números Racionais

Nesta seção, definiremos precisamente o conjunto dos números racionais através de uma relação de equivalência que relaciona um número inteiro e outro não nulo. Tal relação pode ser definida da seguinte forma:

Definição 3.1. Sejam $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*$. Dizemos que (a, b) é equivalente a (c, d), e escrevemos $(a, b) \sim (c, d)$, quando $ad = bc$.

Exemplo 3.1. É fácil ver que $(1, 3) \sim (2, 6)$, pois $1 \cdot 6 = 3 \cdot 2 = 6$. Também podemos verificar que $(1, 2) \sim (2, 4) \sim (-31, -62)$.

A seguir vamos provar que a relação $\sim$, definida acima, é, de fato, uma relação de equivalência.

Proposição 3.1. *A relação binária $\sim$, dada na Definição* 3.1*, é de equivalência.*

Demonstração. Mostraremos que $\sim$ é reflexiva, simétrica e transitiva. Sejam $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}^*$.

i) [Reflexividade]: Como $ab = ba$, temos que $(a, b) \sim (a, b)$.

ii) [Simetria]: Se $(a,b) \sim (c,d)$, então $ad = bc$. Logo, $cb = da$. Por fim, $(c,d) \sim (a,b)$.

iii) [Transitividade]: Se $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$, então

$$ad = bc \tag{3.1}$$

e também

$$cf = de. \tag{3.2}$$

Agora, multiplicando (3.1) por f e (3.2) por b, obtemos

$$adf = bcf \text{ e } bcf = bde.$$

Logo, $adf = bde$. Pela lei do cancelamento, concluímos que, $af = be$ $(d \neq 0)$. Daí, $(a,b) \sim (e,f)$. Como queríamos demonstrar.

□

Se considerarmos, por um momento, nossas noções intuitivas de números racionais. Temos que, $ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d}$, ou seja, se as divisões de a por b e c por d coincidem, podemos dizer que $(a,b) \sim (c,d)$. Em ordem a fazer com que essas ideias sejam verificadas, impomos seguinte definição.

Definição 3.2. Seja $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Definimos, e denotamos, por $\frac{a}{b}$ a classe de equivalência do par (a,b) pela relação $\sim$, isto é,

$$\frac{a}{b} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* / (x,y) \sim (a,b)\}.$$

Exemplo 3.2. É fácil checar que

$$\frac{1}{2} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* / (x,y) \sim (1,2)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* / 2x = y\}.$$

Assim, temos que $(1,2) \in \frac{1}{2}$; $(-31,-62) \in \frac{1}{2}$; $(2,5) \notin \frac{1}{2}$. Da mesma forma, chegamos a

$$\frac{5}{1} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* / (x,y) \sim (5,1)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* / x = 5y\}.$$

Com isso, encontramos o seguinte: $(5,1) \in \frac{5}{1}$; $(-10,-2) \in \frac{5}{1}$; $(2,5) \notin \frac{5}{1}$.

Agora estamos prontos para caracterizar quando $\frac{a}{b} = \frac{c}{d}$, se $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}^*$.

Teorema 3.1. *Sejam $(a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}^*$. Então, $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $ad = bc$.*

Demonstração. ($\Rightarrow$) Suponha que $\frac{a}{b} = \frac{c}{d}$. Note que $(a,b) \in \frac{a}{b} = \frac{c}{d}$. Logo, $(a,b) \sim (c,d)$.

($\Leftarrow$) Assuma que $(a,b) \sim (c,d)$. Se $(x,y) \in \frac{a}{b}$, então $(x,y) \sim (a,b) \sim (c,d)$. Portanto, $(x,y) \sim (c,d)$, ou seja, $(x,y) \in \frac{c}{d}$. Isto nos informa que $\frac{a}{b} \subset \frac{c}{d}$. A inclusão recíproca é análoga. □

Em ordem a finalizar esta seção, vamos definir o conjunto dos números racionais.

Definição 3.3. Denotaremos por $\mathbb{Q}$, e denominamos conjunto dos números racionais, o conjunto quociente de $\mathbb{Z} \times \mathbb{Z}^*$ pela relação de equivalência $\sim$, isto é,

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/\sim = \left\{ \frac{a}{b} / a \in \mathbb{Z}, b \in \mathbb{Z}^* \right\}.$$

3.2 Operações Elementares com Números Racionais

Nesta seção, estamos interessados em desenvolver as propriedades aritméticas, conhecidas do ensino elementar, envolvendo a adição e a multiplicação de números racionais.

3.2.1 Propriedades Elementares da Adição em $\mathbb{Q}$

Nesta subseção, apresentaremos a definição de adição entre números racionais e provaremos propriedades que esta operação acarreta como, por exemplo, associatividade, comutatividade, entre outras.

Definição 3.4. Sejam $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Definimos a operação chamada adição em $\mathbb{Q}$, $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{b \cdot d}.$$

Obs 3.1. O sinal de adição no primeiro membro, nas igualdades acima, se refere a operação de adição em $\mathbb{Q}$; enquanto que, no segundo membro a adição e a multiplicação estão relacionadas a $\mathbb{Z}$.

Exemplo 3.3. É fácil ver que

$$\frac{2}{4} + \frac{5}{3} = \frac{2 \cdot 3 + 4 \cdot 5}{4 \cdot 3} = \frac{6 + 20}{12} = \frac{26}{12} = \frac{13}{6}.$$

Lembrando que um elemento racional é uma classe de equivalência, permita-nos mostrar que a adição em $\mathbb{Q}$ está bem definida.

Proposição 3.2. *Sejam* $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$. *Se* $\frac{a}{b} = \frac{a'}{b'}$ *e* $\frac{c}{d} = \frac{c'}{d'}$, *então*

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}.$$

Demonstração. É fato que temos, por hipótese, que

$$ab' = ba' \tag{3.3}$$

e também que

$$cd' = dc'. \tag{3.4}$$

Por outro lado, sabemos que

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ e } \frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'}.$$

Queremos mostrar que $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$, ou seja,

$$(ad + bc)b'd' = bd(a'd' + b'c').$$

Porém, se multiplicarmos (3.3) por dd' e (3.4) por bb', obtemos

$$ab'dd' = ba'dd' \tag{3.5}$$

e também

$$cd'bb' = dc'bb' \tag{3.6}$$

Somando (3.5) a (3.6), segue que,

$$(ad + bc)b'd' = bd(a'd' + b'c').$$

□

Abaixo, estabeleceremos que a adição, envolvendo números racionais, é comutativa.

Teorema 3.2 (Comutatividade)**.** *Sejam* $r, s \in \mathbb{Q}$. *Então,* $r + s = s + r$.

Demonstração. Sejam $r = \frac{a}{b}$ e $\frac{c}{d}$. Então, é fácil ver que

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b} = s + r.$$

Isto completa a prova do teorema em questão. □

A seguir mostraremos que a associatividade para a adição de números racionais, assim com em $\mathbb{N}$ e $\mathbb{Z}$, é válida.

Teorema 3.3 (Associatividade)**.** *Sejam $r, s, t \in \mathbb{Q}$. Então, $(r+s)+t = r+(s+t)$.*

Demonstração. $r = \frac{a}{b}$, $s = \frac{c}{d}$ e $t = \frac{e}{f}$. Dessa forma, podemos concluir que

$$\begin{aligned}(r+s)+t &= \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} = \frac{ad+bc}{bd}+\frac{e}{f} \\ &= \frac{(ad+bc)f+(bd)e}{(bd)f} = \frac{a(df)+b(cf+de)}{b(df)} \\ &= \frac{a}{b}+\frac{cf+de}{df} = \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right) \\ &= r+(s+t).\end{aligned}$$

Como queríamos demonstrar. □

A adição entre números racionais admite um único elemento neutro e este é dado por $\frac{0}{1}$.

Teorema 3.4 (Elemento Neutro)**.** *$\frac{0}{1}$ é o único elemento de $\mathbb{Q}$ tal que $r = r + \frac{0}{1}$, para todo $r \in \mathbb{Q}$.*

Demonstração. Assuma que $r = \frac{a}{b}$. Logo,

$$r + \frac{0}{1} = \frac{a}{b} + \frac{0}{1} = \frac{a1+b0}{b1} = \frac{a}{b} = r.$$

Isto prova que $\frac{0}{1}$ é o elemento neutro para a adição em $\mathbb{Q}$. Resta-nos provar que este é único. Suponhamos que existe $s \in \mathbb{Q}$ tal que $r = r + s$, para todo $r \in \mathbb{Q}$. Com isso, obtemos

$$\frac{0}{1} = \frac{0}{1} + s = s + \frac{0}{1} = s.$$

Portanto, $s = \frac{0}{1}$. □

A seguir, provaremos que dado um número racional podemos sempre obter um simétrico a este, com relação à adição em $\mathbb{Q}$.

Teorema 3.5 (Simétrico)**.** *Seja $r \in \mathbb{Q}$. Então, existe um único $r' \in \mathbb{Q}$ tal que $r + r' = \frac{0}{1}$.*

Demonstração. Considere que $r = \frac{a}{b}$. Tomemos $r' = \frac{-a}{b}$ em ordem a obter

$$r + r' = \frac{a}{b} + \frac{-a}{b} = \frac{ab+b(-a)}{b \cdot b} = \frac{0}{b \cdot b} = \frac{0}{1}.$$

Isto nos informa que r' é o simétrico de r. Agora, vamos provar que este elemento é único. Sendo assim, considere que existe $s \in \mathbb{Q}$ tal que $r + s = \frac{0}{1}$. Logo, pelas propriedades associativa e comutativa, chegamos a

$$r' = r' + \frac{0}{1} = r' + (r + s) = (r' + r) + s = (r + r') + s = \frac{0}{1} + s = s + \frac{0}{1} = s.$$

Daí, concluímos que $r' = s'$. □

Definição 3.5. O elemento r' tal que $r + r' = \frac{0}{1}$, devido a sua unicidade, é denotado por $-r$, este é chamado simétrico de r.

Exemplo 3.4. É fácil checar que $\frac{-1}{2}$ é o simétrico de $\frac{1}{2}$ em $\mathbb{Q}$, pois $\frac{1}{2} + \frac{-1}{2} = \frac{0}{1}$.

No resultado abaixo, mostraremos que a lei do cancelamento com relação à adição em $\mathbb{Q}$ é uma herança desta mesma lei, observada pela adição e também pela multiplicação em $\mathbb{Z}$.

Teorema 3.6 (Lei do Cancelamento)**.** *Sejam $r, s, t \in \mathbb{Q}$. Então, $r + s = t + s \Leftrightarrow r = t$.*

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

$$\begin{aligned} r + s = t + s &\Leftrightarrow \frac{a}{b} + \frac{c}{d} = \frac{e}{f} + \frac{c}{d} \Leftrightarrow \frac{ad + bc}{bd} = \frac{ed + fc}{fd} \\ &\Leftrightarrow (ad + bc)fd = bd(ed + cf) \Leftrightarrow (ad + bc)f = b(ed + cf) \\ &\Leftrightarrow adf + bcf = bed + bcf \Leftrightarrow adf = bed \\ &\Leftrightarrow af = be \Leftrightarrow \frac{a}{b} = \frac{e}{f} \\ &\Leftrightarrow r = t. \end{aligned}$$

Isto completa a prova do teorema em questão. □

Para finalizar esta subseção, apresentaremos outras maneiras de caracterizar o elemento simétrico a um número racional.

Proposição 3.3. *Seja $\frac{a}{b} \in \mathbb{Q}$. Então, $-\frac{a}{b} = \frac{a}{-b} = \frac{-a}{b} = -\frac{-a}{-b}$.*

Demonstração. Sabemos, pelo que já foi denotado acima, que $-\frac{a}{b} = \frac{-a}{b}$. Além disso,

$$\frac{a}{b} + \frac{a}{-b} = \frac{a(-b) + ba}{b(-b)} = \frac{0}{b(-b)} = \frac{0}{1}.$$

Por unicidade do simétrico, temos que $\frac{-a}{b} = \frac{a}{-b}$. Por fim, é fácil ver, através da prova do Teorema 3.5, que

$$-\frac{-a}{-b} = \frac{-(-a)}{-b} = \frac{a}{-b}.$$

Como queríamos demonstrar. □

É importante ressaltar que, a proposição acima nos permite informar que qualquer número racional r pode ser escrito na forma $\frac{a}{b}$, com $b > 0$, desde que $\frac{c}{-d} = \frac{-c}{d}$, para qualquer $\frac{c}{d} \in \mathbb{Q}$.

3.2.2 Propriedades Elementares da Multiplicação em $\mathbb{Q}$

Nesta subseção, definiremos a multiplicação entre números racionais e demonstraremos propriedades que esta operação implica como, por exemplo, associatividade, comutatividade, elemento neutro, entre outras.

Definição 3.6. Sejam $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Definimos a operação chamada multiplicação ($\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$), por

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

Obs 3.2. O sinal de multiplicação no primeiro membro, na igualdade acima, se refere a operação de multiplicação em $\mathbb{Q}$; enquanto que, no segundo membro a multiplicação está relacionada a $\mathbb{Z}$. Utilizaremos, porém, a mesma notação, neste trabalho.

Em alguns momentos, escreveremos $\frac{a}{b}\frac{c}{d}$ para representar $\frac{a}{b} \cdot \frac{c}{d}$.

Exemplo 3.5. É fácil checar que

$$\frac{2}{4} \cdot \frac{5}{3} = \frac{2 \cdot 5}{4 \cdot 3} = \frac{10}{12} = \frac{5}{6}.$$

Como os elementos de $\mathbb{Q}$ são dados por classes de equivalência, então precisamos estabelecer que a multiplicação entre números racionais está bem definida.

Proposição 3.4. *Sejam* $\frac{a}{b}, \frac{a'}{b'}, \frac{c}{d}, \frac{c'}{d'} \in \mathbb{Q}$. *Se* $\frac{a}{b} = \frac{a'}{b'}$ *e* $\frac{c}{d} = \frac{c'}{d'}$, *então*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

Demonstração. Como

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \text{ e } \frac{a'}{b'} \cdot \frac{c'}{d'} = \frac{a'c'}{b'd'},$$

então desejamos provar que $acb'd' = bda'c'$. Por hipótese, temos que $ab^{'} = ba^{'}$ e $cd' = dc'$. Dessa forma, multiplicando, estas igualdades por cd' e ba', respectivamente, obtemos $acb'd' = cd'ba' = bda'c'$. □

Permita-nos provar que a multiplicação entre números racionais satisfaz a propriedade comutativa.

Teorema 3.7 (Comutatividade)**.** *Sejam $r, s \in \mathbb{Q}$. Então, $r \cdot s = s \cdot r$.*

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

$$r \cdot s = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b} = s \cdot r.$$

□

Agora verifiquemos que a multiplicação, assim como em $\mathbb{N}$ e $\mathbb{Z}$, é associativa.

Teorema 3.8 (Associatividade)**.** *Sejam $r, s, t \in \mathbb{Q}$. Então, $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.*

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

$$(r \cdot s) \cdot t = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = r \cdot (s \cdot t).$$

Como queríamos provar. □

Assim como a adição em $\mathbb{Q}$, a multiplicação em $\mathbb{Q}$ tem um único elemento neutro, o qual é dado por $\frac{1}{1}$.

Teorema 3.9 (Elemento Neutro)**.** *$\frac{1}{1} \in \mathbb{Q}$ é o único elemento tal que $r \cdot \frac{1}{1} = r$, para todo $r \in \mathbb{Q}$.*

Demonstração. Seja $r = \frac{a}{b}$. Dessa forma, temos que

$$r \cdot \frac{1}{1} = \frac{a}{b} \cdot \frac{1}{1} = \frac{a1}{b1} = \frac{a}{b} = r.$$

Suponhamos, agora, que existe $s \in \mathbb{Q}$ tal que $r \cdot s = r$, para todo $r \in \mathbb{Q}$. Dessa forma, pelo Teorema 3.7, obtemos

$$\frac{1}{1} = \frac{1}{1} \cdot s = s \cdot \frac{1}{1} = s.$$

Isto conclui a prova do teorema em questão. □

O resultado abaixo mostra que qualquer racional não nulo tem inverso multiplicativo (tal afirmação não é válida em $\mathbb{N}$ e $\mathbb{Z}$).

Teorema 3.10 (Inverso)**.** *Seja $r \in \mathbb{Q}^*$. Então, existe um único $r'' \in \mathbb{Q}$ tal que $r \cdot r'' = \frac{1}{1}$.*

Demonstração. Se $r = \frac{a}{b} \neq \frac{0}{1} \in \mathbb{Q}$, então $a, b \in \mathbb{Q}^*$. Assim, podemos definir $r'' = \frac{b}{a} \in \mathbb{Q}$ em ordem obter

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

Agora, vamos provar a unicidade para r''. Suponhamos a existência de $s \in \mathbb{Q}$ que seja também inverso de r. Daí, $r \cdot s = \frac{1}{1}$. Logo, pelos Teoremas 3.9, 3.8 e 3.7, chegamos a

$$r'' = r'' \cdot \frac{1}{1} = r'' \cdot (r \cdot s) = (r'' \cdot r) \cdot s = (r \cdot r'') \cdot s = \frac{1}{1} \cdot s = s \cdot \frac{1}{1} = s.$$

Daí, concluímos que $r'' = s$.

□

Definição 3.7. O elemento r'' tal que $r \cdot r'' = \frac{1}{1}$ (se $r \neq \frac{0}{1}$), por sua unicidade, é denotado por r^{-1} e é chamado inverso de r.

Exemplo 3.6. É fácil checar que $\frac{3}{1}$ é o inverso de $\frac{1}{3}$, já que $\frac{3}{1} \cdot \frac{1}{3} = \frac{1}{1}$.

Permita-nos enunciar e demonstrar uma propriedade que envolve as operações de adição e multiplicação em $\mathbb{Q}$.

Teorema 3.11 (Distributividade)**.** *Sejam $r, s, t \in \mathbb{Q}$. Então, $r \cdot (s + t) = r \cdot s + r \cdot t$.*

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

$$\begin{aligned}
r \cdot (s + t) &= \frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\left(\frac{cf + de}{df}\right) \\
&= \frac{a(cf + de)}{b(df)} = \frac{acf + ade}{bdf} \\
&= \frac{fac + dae}{dbf} = \frac{b}{b} \cdot \frac{fac + dae}{dbf} \\
&= \frac{b(fac + dae)}{b(dbf)} = \frac{(ac)(bf) + (bd)(ae)}{(bd)(bf)} \\
&= \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} \\
&= r \cdot s + r \cdot t.
\end{aligned}$$

Isto completa aprova do teorema em questão. □

Provaremos, agora, que a lei do cancelamento é válida também para a multiplicação em $\mathbb{Q}$.

Teorema 3.12. *Sejam $r, s, t \in \mathbb{Q}$ tais que $r \neq \frac{0}{1}$. Então, $s \cdot r = t \cdot r \Leftrightarrow s = t$.*

Demonstração. Sejam $s = \frac{a}{b}$, $t = \frac{c}{d}$ e $r = \frac{e}{f} \neq \frac{0}{1}$ em $\mathbb{Q}$. Então, pela lei do cancelamento em $\mathbb{Z}$, chegamos a

$$\begin{aligned} sr = tr &\Leftrightarrow \frac{a}{b} \cdot \frac{e}{f} = \frac{c}{d} \cdot \frac{e}{f} \Leftrightarrow \frac{ae}{bf} = \frac{ce}{df} \\ &\Leftrightarrow aedf = cebf \Leftrightarrow adef = bcef \\ &\Leftrightarrow ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d} \\ &\Leftrightarrow s = t, \end{aligned}$$

pois $e, f \neq 0$. Como queríamos provar. □

A proposição abaixo nos informa que se multiplicarmos qualquer número racional pelo elemento neutro da adição em $\mathbb{Q}$ teremos como resultados este próprio elemento nulo.

Proposição 3.5. *Sejam $r \in \mathbb{Q}$. Então, $r \cdot \frac{0}{1} = \frac{0}{1}$.*

Demonstração. É fácil checar que

$$r \cdot \frac{0}{1} = r \cdot \left(\frac{0}{1} + \frac{0}{1} \right) = r \cdot \frac{0}{1} + r \cdot \frac{0}{1}.$$

Pela lei do cancelamento, chegamos a $r \cdot \frac{0}{1} = \frac{0}{1}$. □

Para finalizar esta subseção, permita-nos mostrar que o conjunto dos números racionais não possui divisores de zero. Mais especificamente, temos a seguinte proposição.

Proposição 3.6. *Sejam $r, s \in \mathbb{Q}$. Então, $r \cdot s = \frac{0}{1} \Rightarrow r = \frac{0}{1}$ ou $s = \frac{0}{1}$*

Demonstração. Considere que $r \neq \frac{0}{1}$ em ordem a obter um $r^{-1} \in \mathbb{Q}$ que satisfaz $r^{-1} \cdot r = \frac{1}{1}$. Com isso, por usar o fato que $r \cdot s = \frac{0}{1}$, inferimos que

$$s = \frac{1}{1} \cdot s = (r^{-1} \cdot r) \cdot s = r^{-1} \cdot (r \cdot s) = r^{-1} \cdot \frac{0}{1} = \frac{0}{1},$$

ver Proposição 3.5. Por fim, $s = \frac{0}{1}$. □

3.3 Relação de Ordem em $\mathbb{Q}$

Nesta seção, provaremos que $\mathbb{Q}$, assim como $\mathbb{N}$ e $\mathbb{Z}$, é um conjunto totalmente ordenado. A relação que caracteriza o conjunto dos números racionais desta forma está definida logo abaixo.

Ressaltamos que, a partir de agora, consideraremos que todos os números racionais $\frac{a}{b}$ satisfazem $b > 0$.

Definição 3.8. Sejam $\frac{a}{b}$ e $\frac{c}{d} \in \mathbb{Q}$ tais que $b, d > 0$. Dizemos que $\frac{a}{b}$ é menor do que ou igual a $\frac{c}{d}$, e escrevemos $\frac{a}{b} \leq \frac{c}{d}$, quando $ad \leq bc$.

Os símbolos $\geq, >$ e $<$ são definidos de forma análoga à estabelecida acima.

Proposição 3.7. *A relação $\leq$, dada na Definição* 3.8*, está bem definida e é uma relação de ordem em $\mathbb{Q}$.*

Demonstração. Mostraremos, inicialmente, que a relação $\leq$ está bem definida, isto é,

$$\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}, \frac{a}{b} \leq \frac{c}{d} \Rightarrow \frac{a'}{b'} \leq \frac{c'}{d'}.$$

Dessa forma, temos que

$$ab' = ba', cd' = dc' \text{ e } ad \leq bc.$$

Logo, multiplicando a desigualdade acima por $d' > 0$, encontramos $add' \leq bcd'$. Deste modo, $add' \leq bdc'$. Multiplicando esta desigualdade por b', obtemos

$$a'bdd' = ab'dd' \leq c'bdb'.$$

Como $b, d > 0$, então, pela lei do cancelamento em $\mathbb{Z}$, obtemos $a'd' \leq c'b'$. Portanto, $\frac{a'}{b'} \leq \frac{c'}{d'}$.

Vejamos, agora, que a relação $\leq$ é, de fato, uma relação de ordem.

i) [Reflexividade]: Sabemos da comutatividade em $\mathbb{Z}$, que $ab = ba$. Logo, $\frac{a}{b} \leq \frac{a}{b}$.

ii) [Antissimetria]: Sejam $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ tais que $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{a}{b}$. Dessa forma, inferimos

$$ad \leq bc = cb \leq da.$$

Donde concluímos, pela tricotomia em $\mathbb{Z}$, que $ad = bc$. Logo, $\frac{a}{b} = \frac{c}{d}$.

iii) [Transitividade]: Sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, tais que $\frac{a}{b} \leq \frac{c}{d}$ e $\frac{c}{d} \leq \frac{e}{f}$. Com isso,

$$ad \leq bc \text{ e } cf \leq de.$$

Multiplicando as desigualdades acima, respectivamente, por f e b, obtemos

$$adf \leq bcf = cfb \leq deb.$$

Assim, $adf \leq deb$. Pela lei do cancelamento em $\mathbb{Z}$, concluímos que $af \leq be$ $(d > 0)$. Por conseguinte, chegamos a $\frac{a}{b} \leq \frac{e}{f}$.

Isto prova que $\leq$ é uma relação de ordem. □

A seguir, provaremos a compatibilidade entre as operações de adição e multiplicação com a relação de ordem em $\mathbb{Q}$.

Teorema 3.13 (Compatibilidade)**.** *Sejam $r, s, t \in \mathbb{Q}$. Então, as seguintes afirmações são válidas:*

i) $r \leq s \Leftrightarrow r + t \leq s + t$;

ii) $r \leq s$, $t \geq \frac{0}{1} \Rightarrow r \cdot t \leq s \cdot t$. *A recíproca desta afirmação é verdadeira, se* $t > \frac{0}{1}$;

iii) $r \leq s$, $t \leq \frac{0}{1} \Rightarrow r \cdot t \geq s \cdot t$. *A recíproca desta implicação vale, se* $t < \frac{0}{1}$;

Demonstração. Sejam $r = \frac{a}{b}$, $s = \frac{c}{d}$ e $t = \frac{e}{f} \in \mathbb{Q}$, como $b, d, f > 0$. Então, é fácil checar que

i)

$$\begin{aligned} r \leq s &\Leftrightarrow \frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc \\ &\Leftrightarrow adf \leq bcf \Leftrightarrow daf + dbe \leq bcf + dbe \\ &\Leftrightarrow d(af + be) \leq b(cf + de) \Leftrightarrow df(af + be) \leq bf(cf + de) \\ &\Leftrightarrow \frac{af + be}{bf} \leq \frac{cf + de}{df} \Leftrightarrow \frac{a}{b} + \frac{e}{f} \leq \frac{c}{d} + \frac{e}{f} \\ &\Leftrightarrow r + t \leq s + t. \end{aligned}$$

ii) Primeiramente, note que

$$r \leq s \Leftrightarrow \frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc$$

e também

$$t \geq \frac{0}{1} \Leftrightarrow \frac{e}{f} \geq \frac{0}{1} \Leftrightarrow e \geq 0.$$

Daí,

$$\begin{aligned} r \leq s \Leftrightarrow ad \leq bc \Rightarrow ade \leq bce \\ \Leftrightarrow adef \leq bcef \Leftrightarrow \frac{ae}{bf} \leq \frac{ce}{df} \\ \Leftrightarrow \frac{a}{b} \cdot \frac{e}{f} \leq \frac{c}{d} \cdot \frac{e}{f} \Leftrightarrow r \cdot t \leq s \cdot t. \end{aligned}$$

É importante notar que se $t > 0$ ($e > 0$), então a implicação acima se torna equivalência. Logo, **ii**) segue.

iii) Primeiramente, note que $r \leq s$ e $t \leq \frac{0}{1}$ é equivalente a $ad \leq bc$ e $e \leq 0$. Segue, daí, que

$$\begin{aligned} r \leq s \Leftrightarrow ad \leq bc \Leftrightarrow adf \leq bcf \\ \Rightarrow adfe \geq bcfe \Leftrightarrow \frac{ae}{bf} \geq \frac{ce}{df} \\ \Leftrightarrow \frac{a}{b} \cdot \frac{e}{f} \geq \frac{c}{d} \cdot \frac{e}{f} \\ \Leftrightarrow r \cdot t \geq s \cdot t. \end{aligned}$$

Note que a implicação acima se torna equivalência se $t < 0$ ($e < 0$). Portanto, **iii**) segue.

Estes argumentos provam que $\leq$ é uma relação de ordem em $\mathbb{Q}$. □

O próximo resultado nos informa que $\leq$ é uma relação de ordem total em $\mathbb{Q}$ e, consequentemente, $\mathbb{Q}$, munido desta relação, é um conjunto totalmente ordenado.

Teorema 3.14 (Tricotomia)**.** *Sejam $r, s \in \mathbb{Q}$. Então, somente uma das situações seguintes ocorre: $r = s$ ou $r < s$ ou $r > s$.*

Demonstração. Sejam $r = \frac{a}{b}, s = \frac{c}{d} \in \mathbb{Q}$, com $b, d > 0$. Comparemos os inteiros ad e bc. Pela tricotomia em $\mathbb{Z}$, ou $ad = bc$, cujo caso ocorre $r = s$, ou $ad < bc$, em cujo caso ocorre $r < s$, ou $ad > bc$, em cujo caso ocorre $r > s$. Além disso, a validade de uma da afirmações exclui a validade das outras duas. □

3.4 Caracterização Usual de $\mathbb{Q}$

Através da caracterização usual de $\mathbb{Z}$, podemos escrever o conjunto dos números racionais como a união disjunta $\mathbb{Q} = \mathbb{Q}^*_- \cup \mathbb{Q}^*_+ \cup \left\{\frac{0}{1}\right\}$, onde $\mathbb{Q}^*_+ = \{\frac{a}{b}/(a,b) \in \mathbb{Z}^*_+ \times \mathbb{Z}^*_+\}$ e $\mathbb{Q}^*_- = \{\frac{a}{b}/(a,b) \in \mathbb{Z}^*_- \times \mathbb{Z}^*_+\}$. Também denotamos, $\mathbb{Q}_- = \mathbb{Q}^*_- \cup \left\{\frac{0}{1}\right\}$, $\mathbb{Q}_+ = \mathbb{Q}^*_+ \cup \left\{\frac{0}{1}\right\}$ e $\mathbb{Q}^* = \{\frac{a}{b}/(a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*\}$.

Permita-nos, agora, identificar o conjunto $\mathbb{Z}$ como um subconjunto de $\mathbb{Q}$.

Teorema 3.15. *Seja $f_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}$ uma aplicação dada por*

$$f_{\mathbb{Z}}(n) = \frac{n}{1}, \forall n \in \mathbb{Z}.$$

Então, são verdadeiras ass seguintes afirmações:

i) *$f_{\mathbb{Z}}$ é injetora;*

ii) *$f_{\mathbb{Z}}(m+n) = f_{\mathbb{Z}}(m) + f_{\mathbb{Z}}(n), \forall n, m \in \mathbb{Z}$;*

iii) *$f_{\mathbb{Z}}(mn) = f_{\mathbb{Z}}(m) \cdot f_{\mathbb{Z}}(n), \forall n, m \in \mathbb{Z}$;*

iv) *$m < n \Leftrightarrow f_{\mathbb{Z}}(m) < f_{\mathbb{Z}}(n), n, m \in \mathbb{Z}$.*

Demonstração. Sejam $n, m \in \mathbb{Z}$. Então,

i) Mostremos que $f_{\mathbb{Z}}$ é injetora. Com efeito,

$$f_{\mathbb{Z}}(m) = f_{\mathbb{Z}}(n) \Leftrightarrow \frac{m}{1} = \frac{n}{1} \Leftrightarrow m \cdot 1 = 1 \cdot n \Leftrightarrow m = n.$$

ii) Agora, vamos provar que $f_{\mathbb{Z}}$ preserva a estrutura algébrica de $\mathbb{Z}$, isto é,

$$f_{\mathbb{Z}}(n) + f_{\mathbb{Z}}(m) = \frac{n}{1} + \frac{m}{1} = \frac{n \cdot 1 + 1 \cdot m}{1 \cdot 1} = \frac{n+m}{1} = f_{\mathbb{Z}}(n+m).$$

iii) Analogamente, temos que

$$f_{\mathbb{Z}}(n) \cdot f_{\mathbb{Z}}(m) = \frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1 \cdot 1} = \frac{nm}{1} = f_{\mathbb{Z}}(nm).$$

iv) Por fim, mostremos que $f_{\mathbb{Z}}$ preserva a relação de ordem de $\mathbb{Z}$. De fato,

$$m < n \Leftrightarrow m \cdot 1 < n \cdot 1 \Leftrightarrow \frac{m}{1} < \frac{n}{1} \Leftrightarrow f_{\mathbb{Z}}(m) < f_{\mathbb{Z}}(n).$$

Isto completa a prova do teorema em questão. □

Assim, o conjunto $f_{\mathbb{Z}}(\mathbb{Z}) = \{\frac{n}{1} / n \in \mathbb{Z}\}$ é uma cópia algébrica de $\mathbb{Z}$ em $\mathbb{Q}$. Essa imersão de $\mathbb{Z}$ em $\mathbb{Q}$ também mostra que $\mathbb{Q}$ é infinito, já que $\mathbb{Z}$ contém uma cópia de $\mathbb{N}$. Além disso, através da identificação $f_{\mathbb{Z}}$, temos que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

3.5 Enumerabilidade de $\mathbb{Q}$

Nesta seção, estamos interessados em provar que o conjunto dos números racionais $\mathbb{Q}$, assim com $\mathbb{N}$ e $\mathbb{Z}$, é enumerável.

Primeiramente, utilizaremos o Teorema 2.18, para provar que qualquer número racional positivo poder ser escrito de modo único como uma fração irredutível. Mais precisamente, temos o seguinte lema.

Lema 3.1. *Seja $\frac{a}{b} \in \mathbb{Q}_+^*$. Então existem únicos $m, n \in \mathbb{N}^*$ tais que $\frac{a}{b} = \frac{m}{n}$, onde m, n são relativamente primos, isto é, m e n não são divisíveis.*

Demonstração. Considere as decomposições em fatores primos de a e de b, dadas pelo Teorema 2.18. Seja k o produto de todos os fatores primos comuns a a e b, de modo que $\frac{a}{b} = \frac{ka'}{kb'}$, onde a' e b' são relativamente primos. Assim, $\frac{a}{b} = \frac{a'}{b'}$. Se houvesse uma fração irredutível $\frac{c}{d}$ igual a $\frac{a'}{b'}$, a propriedade fundamental das frações nos daria $a'd = b'c$, o que, pela unicidade de decomposição de fatores primos, obrigaria d a conter, em sua decomposição (ver Teorema 2.18), os fatores primos de b' e vice-versa, o mesmo ocorrendo para a' e c, ou seja, $a' = c$ e $b' = d$. □

Lema 3.2. *$\mathbb{Q}_+^*$ e $\mathbb{Q}_-^*$ são enumeráveis.*

Demonstração. Consideremos os números racionais escritos na forma irredutível, dada no Lema 3.1. Seja $f : \mathbb{Q}_+^* \to \mathbb{N}$ dada por

$$f\left(\frac{m}{n}\right) = 2^m \cdot 3^n, \forall \frac{m}{n} \in \mathbb{Q}_+^*.$$

Se $f(\frac{m}{n}) = f(\frac{m'}{n'})$, então $2^m \cdot 3^n = 2^{m'} \cdot 3^{n'}$. Daí, pelo Teorema 2.18 e Lema 3.1, concluímos que $2^m = 2^{m'}$ e $3^n = 3^{n'}$, isto é, $m = m'$ e $n = n'$ (ver Corolário 1.15), que implica, $m \cdot n' = n \cdot m'$. Deste modo, $\frac{m}{n} = \frac{m'}{n'}$. Logo, f é injetora e tem como imagem um subconjunto (infinito, pois $\mathbb{Q}_+^*$ é infinito, pelo fato que $\mathbb{N}^* = \mathbb{Z}_+^* \subset \mathbb{Q}_+^*$) de $\mathbb{N}$, o qual, pelo Lema 1.17, é enumerável.

Agora vamos provar que $\mathbb{Q}_-^*$ é enumerável. Basta mostrarmos que a aplicação $f : \mathbb{Q}_-^* \to \mathbb{Q}_+^*$, dada por

$$f\left(-\frac{a}{b}\right) = \frac{a}{b}, \forall a, b \in \mathbb{Z}_+^*,$$

é bijetora (lembre que $-\frac{a}{b} = \frac{-a}{b}$). De fato, f é injetora, pois

$$f\left(-\frac{a_1}{b_1}\right) = f\left(-\frac{a_2}{b_2}\right) \Rightarrow \frac{a_1}{b_1} = \frac{a_2}{b_2} \Rightarrow -\frac{a_1}{b_1} = -\frac{a_2}{b_2}.$$

Temos também que f é sobrejetora, já que se $\frac{c}{d} \in \mathbb{Q}_+^*$ temos que $f(-\frac{c}{d}) = \frac{c}{d}$, com $-\frac{c}{d} \in \mathbb{Q}_-^*$. Portanto, f é bijetora. Usando o fato que $\mathbb{Q}_+^*$ ser enumerável, concluímos que $\mathbb{Q}_-^*$ também o é. □

Agora, estamos prontos para garantir que $\mathbb{Q}$ é enumerável.

Teorema 3.16. *$\mathbb{Q}$ é enumerável.*

Demonstração. Sabemos que $\mathbb{Q}_+^*$ e $\mathbb{Q}_-^*$ são enumeráveis (ver Lema 3.2). Logo, desde que $\mathbb{Q} = \mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^*$, temos, pela Proposição 1.18, que $\mathbb{Q}$ é enumerável ($\{0\}$ é enumerável). □

3.6 O Corpo Ordenado $\mathbb{Q}$

Nesta seção, nossa meta é trabalhar com o conjunto dos números racionais $\mathbb{Q}$ observando sua estrutura de corpo ordenado.

Comecemos assumindo que o conjunto dos números racionais $\mathbb{Q}$ está munido das duas operações, adição e multiplicação, estudadas anteriormente. Podemos definir, a partir destas, a subtração e a divisão (esta não é possível em $\mathbb{N}$ e $\mathbb{Z}$) entre números racionais da seguinte forma:

Definição 3.9. Sejam $r, s \in \mathbb{Q}$, define-se a subtração ($- : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$) e a divisão ($\div : \mathbb{Q}\times\mathbb{Q}^* \to \mathbb{Q}$), respectivamente, entre esses dois elementos por

$$r - s = r + (-s) \text{ e } r \div s = r \cdot s^{-1}.$$

onde, no caso da divisão, $s \neq 0$. (Estritamente falando, a divisão não seria uma operação em $\mathbb{Q}$, uma vez que seu domínio não é $\mathbb{Q} \times \mathbb{Q}$, mas sim $\mathbb{Q} \times \mathbb{Q}^*$).

A proposição a seguir nos permite saber que a definição de divisão, dada acima, pode, na prática, ser representada com a ideia de fração estabelecida no ensino elementar.

Proposição 3.8. *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, então $\frac{a}{1} \div \frac{b}{1} = \frac{a}{b}$. Assim, se identificarmos $\mathbb{Z}$ com sua cópia $f_{\mathbb{Z}}(\mathbb{Z})$ em $\mathbb{Q}$, a igualdade acima se escreve $a \div b = \frac{a}{b}$.*

Demonstração. Como $a, b \in \mathbb{Z}, b \neq 0$, temos que

$$a \div b = \frac{a}{1} \div \frac{b}{1} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a \cdot 1}{1 \cdot b} = \frac{a}{b}$$

□

O resultado abaixo nos mostra que a definição de divisão, dada acima, é, na prática, a mesma da estabelecida no ensino elementar.

Proposição 3.9. *Sejam* $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, *com* $\frac{c}{d} \neq \frac{0}{1}$. *Então,* $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc} = \frac{a}{b} \cdot \frac{d}{c}$.

Demonstração. Observe que

$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}.$$

Como queríamos demonstrar. □

Admitindo a identificação de $\mathbb{Z}$ com $f_{\mathbb{Z}}(\mathbb{Z})$, é possível provar que as regras de sinal, estudadas na ensino básico, são satisfeitas pelos números racionais.

Proposição 3.10. *Sejam* $r, s \in \mathbb{Q}$. *Então, são válidos os seguintes itens:*

i) $rs = 0 \Rightarrow s = 0$ *ou* $r = 0$;

ii) $r > 0, s > 0 \Rightarrow rs > 0$;

iii) $r > 0, s < 0 \Rightarrow rs < 0$;

iv) $r < 0, s < 0 \Rightarrow rs > 0$;

v) $r > 0 \Rightarrow r^{-1} > 0$.

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

i) Suponhamos $r \neq 0$, ou seja, $\frac{a}{b} \neq \frac{0}{1}$ $(a \neq 0)$. Segue, daí, que,

$$\frac{0}{1} = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Logo, $ac = 0$. Isto nos diz que $c = 0$. Portanto, $s = \frac{0}{1} = 0$.

ii) Se $\frac{a}{b} > \frac{0}{1}$ e $\frac{c}{d} > \frac{0}{1}$, então $a > 0$ e $c > 0$. Daí, pelas propriedades de $\mathbb{Z}$, temos que $ac > 0$. Consequentemente, $\frac{ac}{bd} > \frac{0}{1}$, isto é, $rs > 0$.

iii) Se $\frac{a}{b} > \frac{0}{1}$, então $a > 0$. Analogamente, se $\frac{c}{d} < \frac{0}{1}$, temos que $c < 0$. Assim, pelas propriedades de $\mathbb{Z}$, encontramos $ac < 0$. Portanto, $\frac{ac}{bd} < \frac{0}{1}$, ou seja, $rs < 0$.

iv) Se $\frac{a}{b} < \frac{0}{1}$, então $a < 0$. Pelo mesmo motivo $\frac{c}{d} < \frac{0}{1}$ implica que $c < 0$. Logo, pelas propriedades de $\mathbb{Z}$, encontramos $ac > 0$. Portanto, $\frac{ac}{bd} > \frac{0}{1}$. Por fim, $rs > 0$.

v) Se $\frac{a}{b} > 0$, tem-se $a > 0$. Logo, $\frac{b}{a} \in \mathbb{Q}$ é o inverso de $\frac{a}{b}$. Por conseguinte, $\frac{b}{a} > 0$ $(b > 0)$.

□

Ainda considerando a identificação de $\mathbb{Z}$ com $f_{\mathbb{Z}}(\mathbb{Z})$, mostraremos que entre dois números racionais sempre é possível encontrar um outro (este é denominado média aritmética entre os extremos).

Proposição 3.11. *Sejam $r, s \in \mathbb{Q}$. Se $r < s$, então $r < (r + s) \cdot 2^{-1} < s$.*

Demonstração. Note que

$$2r = r + r < r + s < s + s = 2s.$$

Segue que, $2r < r+s < 2s$. Por fim, multiplicando por $2^{-1} \in \mathbb{Q}$, chegamos a $r < (r+s)\cdot 2^{-1} < s$. □

Vimos que os conjuntos $\mathbb{N}$ e $\mathbb{Z}$ são bem ordenados (ver Teoremas 1.16 e 2.13). Porém, o conjunto dos números racionais não verifica tal afirmação. Mais precisamente, temos a seguinte proposição.

Proposição 3.12. *$\mathbb{Q}$ não é bem ordenado, isto é, existem em $\mathbb{Q}$ subconjuntos não vazios e limitados inferiormente que não possuem elemento mínimo.*

Demonstração. Fixe $q_0 \in \mathbb{Q}$. Seja $X = \{\frac{a}{b} \in \mathbb{Q} / q_0 < \frac{a}{b}\}$. É fácil ver que $X \neq \varnothing$ (pois $q_0 + \frac{1}{1} \in X$) e é limitado inferiormente por q_0. Suponhamos que X possua um elemento mínimo, digamos $j \in X$. Assim sendo, $j \leq \frac{a}{b}$, para todo $\frac{a}{b} \in X$. Como q_0 é cota inferior de X, temos que $q_0 < j$ (já que $j \in X$ e $q_0 \notin X$). Daí, pela Proposição 3.11, obtemos $(q_0 + j) \cdot 2^{-1} \in \mathbb{Q}$ tal que

$$q_0 < (q_0 + j) \cdot 2^{-1} < j.$$

Assim sendo, $(q_0 + j) \cdot 2^{-1} \in X$ e $(q_0 + j) \cdot 2^{-1} < j$. Um absurdo, visto que $j = \min X$. Portanto, $\mathbb{Q}$ não é bem ordenado. □

Apesar de $\mathbb{Q}$ não ser bem ordenado, $\mathbb{Q}$ possui todas as propriedades aritméticas de $\mathbb{Z}$, além da propriedade de que todo elemento não nulo possui inverso. Na linguagem algébrica, qualquer conjunto munido de duas operações, usualmente denotadas por $\cdot$ e $+$, com propriedades aritméticas análogas às de $\mathbb{Q}$, chama-se corpo conforme definiremos abaixo.

Definição 3.10. Um conjunto não vazio K é um corpo se em K pudermos definir duas operações, denotadas por $+ : K \times K \to K$ (adição) e $\cdot : K \times K \to K$ (multiplicação), satisfazendo as seguintes propriedades:

(F) $x + y \in \mathbb{K}$ e $x \cdot y \in K$, $\forall x, y \in K$;

(A1) [Comutatividade Adição]: $x + y = y + x$, $\forall x, y \in K$;

(A2) [Associatividade Adição]: $x + (y + z) = (x + y) + z$, $\forall x, y, z \in K$;

(A3) [Elemento Neutro Adição]: Existe um elemento em K, denotado por 0, chamado de elemento neutro da adição, que satisfaz $0 + x = x + 0 = x$, $\forall x \in K$;

(A4) [Simétrico]: Para cada $x \in K$, existe um elemento em K, denotado por $-x$ e chamado de simétrico de x tal que $x + (-x) = (-x) + x = 0$;

(M1) [Comutatividade Multiplicação]: $x \cdot y = y \cdot x$, $\forall x, y \in K$;

(M2) [Associatividade Multiplicação]: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $\forall x, y, z \in K$;

(M3) [Elemento Neutro Multiplicação]: Existe um elemento em $\mathbb{K}$, denotado por 1, chamado de elemento neutro da multiplicação, tal que $1 \cdot x = x \cdot 1 = x$, $\forall x \in K$;

(M4) [Inverso]: Para cada elemento não nulo $x \in K$, existe um elemento em K, denotado por x^{-1}, chamado de inverso multiplicativo de x, tal que $x \cdot x^{-1} = x^{-1} \cdot x = 1$;

(D) [Distributividade]: $(x + y) \cdot z = x \cdot z + y \cdot z$, $\forall x, y, z \in K$.

Além disso, se um corpo tiver munido de uma relação de ordem compatível com sua operações aritméticas, ele é chamado de corpo ordenado. Adotaremos a seguinte notação para os elementos de um corpo ordenado arbitrário K: continuaremos denotando por 0 e por 1 o elemento neutro aditivo e o neutro multiplicativo de K, respectivamente e, para x um natural maior do que 1, denotaremos também por x o elemento $1 + 1 + ... + 1$ (x vezes) (isto nos diz que $\mathbb{N}$ possui uma cópia em K, pois $0 \in K$). Assim, seu simétrico, $-x$, será $-(1 + 1 + 1 + ... + 1) = -1 - 1 - 1 - ... - 1$ (x vezes) (isto nos informa que $\mathbb{Z}$ admite uma cópia em K). O contexto encarrega-se de deixar claro que o elemento 3, por exemplo, refere-se ao natural 3 ou ao $3 \in K$.

É importante ressaltar que tudo o que foi feito neste capítulo nos mostra que $\mathbb{Q}$ é um exemplo de corpo ordenado.

A seguir definiremos potências com bases em um corpo ordenado e expoentes inteiros.

Definição 3.11. Seja K um corpo ordenado. Seja $a \in K$ e $n \in \mathbb{N}$. Definimos a potência a^n recursivamente como sendo 1, se $n = 0$ (neste caso, $a \neq 0$), por a, se $n = 1$; e como sendo $a \cdot a^{n-1}$, para $n > 1$. Se $a \neq 0$ em K, definimos $a^{-n} = (a^{-1})^n$ para todo $n \in \mathbb{N}$.

Precisaremos de algumas propriedades envolvendo potências para provarmos a famosa desigualdade de Bernoulli (ver Proposição 3.19).

Proposição 3.13. *Sejam $a \in K$ e $n, m \in \mathbb{Z}$. Então, $a^n a^m = a^{n+m}$.*

Demonstração. Primeiramente, mostraremos, por indução, que

$$a^n a^m = a^{n+m}, \forall n \in \mathbb{Z}, m \in \mathbb{N}.$$

Fixe $n \in \mathbb{Z}$. Seja $X_n = \{m \in \mathbb{N} / a^n a^m = a^{n+m}\}$. É fácil ver que

$$a^{n+0} = a^n = a^n \cdot 1 = a^n a^0.$$

Suponha, então que $m \in X_n$, isto é, $a^n a^m = a^{n+m}$. Portanto,

$$a^n a^{m+1} := a^n (a^m a) := (a^n a^m) a = a^{n+m} a = a^{(n+m)+1} = a^{n+(m+1)}. \tag{3.7}$$

Logo, $m + 1 \in X$. Por indução, concluímos que $X_n = \mathbb{N}$.

Observe que se $n \in \mathbb{N}$ e $m \in \mathbb{Z}$, então

$$a^{n+m} = a^{m+n} = a^m a^n = a^n a^m.$$

Por fim, se $n < 0$ e $m < 0$, encontramos

$$a^{n+m} = a^{-(-n-m)} := (a^{-1})^{[(-n)+(-m)]} = (a^{-1})^{-n} (a^{-1})^{-m} =: a^{-(-n)} a^{-(-m)} = a^n a^m.$$

Isto conclui a prova do teorema em questão. □

Proposição 3.14. *Sejam $a \in K$ e $n, m \in \mathbb{Z}$. Então, $(a^n)^m = a^{nm}$.*

Demonstração. O caso em que $n, m \in \mathbb{N}$ pode ser provado por indução. Fixe $n \in \mathbb{N}$. Defina $X_n = \{m \in \mathbb{N} : (a^n)^m = a^{nm}\}$. É fácil checar que

$$(a^n)^0 = 1 = a^0 = a^{n \cdot 0}.$$

Assim, $0 \in X_n$. Suponha que $m \in X_n$, isto é, $(a^n)^m = a^{nm}$. Deste modo, podemos escrever, através da Proposição 3.13, que

$$(a^n)^{m+1} = (a^n)^m a^n = a^{nm} a^n = a^{nm+n} = a^{n(m+1)}.$$

Portanto, $m + 1 \in X_n$. Dessa forma, concluímos que $X_n = \mathbb{N}$.

Agora, vamos provar que $(a^n)^{-1} = a^{-n}$, para todo $n \in \mathbb{Z}$. De fato, pela Proposição 3.13, temos que

$$a^n a^{-n} = a^{n+(-n)} = a^0 = 1, \forall n \in \mathbb{Z}.$$

Portanto, pela unicidade de um elemento inverso, chegamos a $(a^n)^{-1} = a^{-n}$, para todo $n \in \mathbb{Z}$.

Sejam $n \in \mathbb{N}$ e $m < 0$. Então, pelo que foi feito acima, encontramos

$$(a^n)^m = (a^n)^{-(-m)} := [(a^n)^{-1}]^{-m} = (a^{-n})^{-m} = a^{(-n)(-m)} = a^{nm}.$$

Por fim, considere que $n, m < 0$. Assim, pelo que já foi estabelecido acima, chegamos a

$$(a^n)^m = (a^{-(-n)})^m := [(a^{-1})^{-n}]^m = (a^{-1})^{(-n)m} = (a^{-1})^{-nm} = [(a^{-1})^{-1}]^{nm} = a^{nm}.$$

A proposição em questão segue. □

A seguir, vamos definir o que significa módulo de um elemento de um corpo ordenado.

Definição 3.12. Num corpo ordenado K, definimos o módulo (ou valor absoluto) de um elemento x, como sendo x, se $x \geq 0$ e $-x$ se $x < 0$. Usaremos o símbolo $|x|$ para indicar o módulo de x, ou seja,

$$|x| = \begin{cases} x, \text{ se } x \geq 0; \\ -x, \text{ se } x < 0. \end{cases}$$

Obs 3.3. A Definição 3.12 é equivalente a $|x| = \max\{x, -x\}$, onde $x \in K$. Por conseguinte, podemos escrever que

$$|x| \geq x, -x, \forall x \in K,$$

isto é,

$$-|x| \leq x \leq |x|, \forall x \in K.$$

Como um resultado, podemos garantir que $|x| \geq 0$, para todo $x \in K$.

Vejamos duas maneiras de caracterizar quando um elemento de um corpo ordenado K tem módulo menor do que ou igual a um outro elemento deste mesmo conjunto.

Proposição 3.15. *Seja K um corpo ordenado. Seja $x, a \in K$. As seguintes afirmações são equivalentes:*

i) $-a \leq x \leq a$;

ii) $x \leq a$ *e* $-x \leq a$;

iii) $|x| \leq a$.

Demonstração. Os três itens acima seguem diretamente das equivalências abaixo:

$$-a \leq x \leq a \Leftrightarrow -a \leq x \text{ e } x \leq a \Leftrightarrow -x \leq a \text{ e } x \leq a \Leftrightarrow |x| \leq a.$$

□

O próximo resultado estabelece algumas propriedades importantes para o módulo de elementos de corpos ordenados.

Teorema 3.17. *Seja K um corpo ordenado. Sejam $x, y, z \in K$. Então, valem as afirmações abaixo:*

i) $|x + y| \leq |x| + |y|$;

ii) $|x \cdot y| = |x| \cdot |y|$;

iii) $|x| - |y| \leq ||x| - |y|| \leq |x - y|$;

iv) $|x - z| \leq |x - y| + |y - z|$.

Demonstração. **i)** Vimos que

$$-|x| \leq x \leq |x| \text{ e } -|y| \leq y \leq |y|.$$

Adicionando estas igualdades, encontramos

$$-(|x| + |y|) \leq x + y \leq |x| + |y|.$$

Pela Proposição 3.15, isto significa que $|x + y| \leq |x| + |y|$.

ii) É fácil checar que $x^2 = |x|^2$, pois $|x|$ é um dos elementos x ou $-x$ e vale $x^2 = (-x)^2$. Logo,

$$|x \cdot y|^2 = (x \cdot y)^2 = x^2 \cdot y^2 = |x|^2 \cdot |y|^2 = (|x| \cdot |y|)^2.$$

Deste modo, chegamos a

$$[|x \cdot y| - |x| \cdot |y|][|x \cdot y| + |x| \cdot |y|] = |x \cdot y|^2 - (|x| \cdot |y|)^2 = 0.$$

Segue que, $|x \cdot y| = \pm|x| \cdot |y|$ (K não possui divisores de zero - a prova deste fato segue os passos da Proposição 3.6). Como $|x \cdot y|$ e $|x| \cdot |y|$ são ambos não negativos, concluímos que $|x \cdot y| = |x| \cdot |y|$.

iii) Em virtude de **i**), temos que

$$|x| = |(x-y)+y| \leq |x-y| + |y|.$$

O que nos fornece, $|x| - |y| \leq |x-y|$. Analogamente, tem-se $|y| \leq |y-x| + |x|$. Logo, $-(|x| - |y|) \leq |x-y|$. Por fim, $||x| - |y|| \leq |x-y|$.

iv) Por **i**), obtemos

$$|x-z| = |(x-y)+(y-z)| \leq |x-y| + |y-z|.$$

Isto completa a prova do teorema em questão. □

Vejamos mais algumas consequências que envolvem elementos de um corpo ordenado.

Proposição 3.16. *Seja K um corpo ordenado. Então, as seguintes afirmações são válidas:*

i) $x \cdot 0 = 0, \forall x \in K$*;*

ii) *se* $0 = 1$*, então K possui um só elemento;*

iii) $x^2 \geq 0, \forall x \in K$*;*

iv) *se* $1 \neq 0$*, então* $1 > 0 > -1$*;*

v) *se* $1 \neq 0$*, então K contém uma cópia de* $\mathbb{N}$*, de* $\mathbb{Z}$ *e de* $\mathbb{Q}$ *e é, portanto, infinito.*

Demonstração. **i)** É fácil checar que

$$x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0,$$

para todo $x \in K$. Segue que,

$$0 = x \cdot 0 + (-x \cdot 0) = [x \cdot 0 + x \cdot 0] + (-x \cdot 0) = x \cdot 0 + [x \cdot 0 + (-x \cdot 0)] = x \cdot 0 + 0 = x \cdot 0,$$

para todo $x \in K$. Portanto, $x \cdot 0 = 0$, para todo $x \in K$

ii) Por hipótese, $0 = 1$. Seja $x \in K$. Daí,

$$x = x \cdot 1 = x \cdot 0 = 0,$$

por **i**). Logo, $K = \{0\}$.

iii) Dado $x \in K$, tem-se que

- $x < 0 \Rightarrow x^2 > 0$;
- $x = 0 \Rightarrow x^2 = 0$;
- $x > 0 \Rightarrow x^2 > 0$.

Portanto, $x^2 \geq 0$, para todo $x \in K$.

iv) Se $1 \neq 0$, então

$$1 = 1 \cdot 1 = 1^2 > 0.$$

v) Já discutimos o fato de $\mathbb{N}$ e $\mathbb{Z}$ possuírem cópias em K ($0 \in K$). Assim sendo, se identificarmos $\mathbb{N}$ e $\mathbb{Z}$ com suas respectivas cópias em K, temos que $\mathbb{N} \subset \mathbb{Z} \subset K$. Por fim, se $\frac{a}{b} \in \mathbb{Q}$, concluímos que

$$\frac{a}{b} = a : b = a \cdot b^{-1} \in K,$$

desde que $a \in \mathbb{Z}$ e $b \in \mathbb{Z}_+^*$. Por fim, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset K$.

□

No que segue, os termos limitado superiormente, inferiormente, cota superior, inferior, elemento máximo e mínimo têm significado análogo àqueles já definidos no contexto dos números inteiros.

Proposição 3.17. *O conjunto* $\mathbb{N}$ *é ilimitado superiormente em* $\mathbb{Q}$.

Demonstração. Suponhamos, por contradição, a existência de $\frac{a}{b} \in \mathbb{Q}$ tal que $\frac{a}{b} \geq x$, para todo $x \in \mathbb{N}$. Como, por convenção, $b > 0$, temos que $a, b \in \mathbb{Z}_+^*$, ou seja, $a, b \in \mathbb{N}^*$. Assim, $b \geq 1$ (ver Proposição 1.9). Logo, $a \geq \frac{a}{b}$ (ver Proposição 1.13). Note que, se $a > \frac{a}{b}$, então chegaríamos a um absurdo, visto que $\frac{a}{b}$ é uma cota superior de $\mathbb{N}$ em $\mathbb{Q}$ ($a \in \mathbb{N}^*$). Dessa forma, $a = \frac{a}{b}$ e, por conseguinte, concluímos que $a + 1 > a = \frac{a}{b}$. De qualquer maneira chegaríamos a outra contradição, pelo fato de $\frac{a}{b}$ ser uma cota superior de $\mathbb{N}$ em $\mathbb{Q}$ ($a+1 \in \mathbb{N}^*$). Portanto, $\mathbb{N}$ é ilimitado superiormente em $\mathbb{Q}$. □

Proposição 3.18. $\mathbb{Q}$ *não possui elemento máximo e nem mínimo.*

Demonstração. Suponhamos que $\mathbb{Q}$ possua um elemento mínimo, digamos, $\min \mathbb{Q} = \frac{a}{b}$, ou seja, $\frac{a}{b} \leq \frac{x}{y}$, para todo $\frac{x}{y} \in \mathbb{Q}$. É fácil ver que, $\frac{a}{b} - 1 = \frac{a-b}{b} \in \mathbb{Q}$; além disso, $\frac{a-b}{b} < \frac{a}{b}$ ($b > 0$), o que contradiz a minimalidade de $\frac{a}{b}$. Logo, $\mathbb{Q}$ não possui elemento mínimo. De forma análoga, suponhamos que $\mathbb{Q}$ possua um elemento máximo, digamos, $\max \mathbb{Q} = \frac{c}{d}$, isto é, $\frac{x}{y} \leq \frac{c}{d}$, para todo

$\frac{x}{y} \in \mathbb{Q}$. Claramente, $\frac{c}{d} + 1 = \frac{c+d}{d} \in \mathbb{Q}$; além disso, $\frac{c}{d} < \frac{c+d}{d}$ $(d > 0)$, o que contradiz a maximalidade de $\frac{c}{d}$. Portanto, $\mathbb{Q}$ também não possui elemento máximo, como queríamos. □

Definição 3.13. Os corpos ordenados para os quais sua cópia de naturais é ilimitada superiormente são chamados corpos Arquimedianos.

Exemplo 3.7. Através da Proposição 3.17, podemos concluir que $\mathbb{Q}$ é um exemplo de corpo Arquimediano.

Vejamos mais duas maneiras de caracterizar corpos ordenados não triviais como Arquimedianos. Mais precisamente, temos o seguinte teorema.

Teorema 3.18. *Seja $K \neq \{0\}$ um corpo ordenado. Então, as seguintes afirmações são equivalentes:*

i) *K é Arquimediano;*

ii) *dados $a, b \in K$, com $a > 0$, existe $n \in \mathbb{N}$, tal que $na > b$;*

iii) *dado $a > 0 \in K$, existe $n \in \mathbb{N}$ $(\subset K)$ tal que $n^{-1} < a$.*

Demonstração. **i)** $\Rightarrow$ **ii)**: Como $\mathbb{N}$ é ilimitado superiormente (K é Arquimediano), então dados $a > 0$ e b em K, existe $n \in \mathbb{N}$ tal que $b \cdot a^{-1} < n$ e, portanto, $b < n \cdot a$.

ii) $\Rightarrow$ **iii)**: Dado $a > 0$ em K, existe, em virtude de **ii)**, um $n \in \mathbb{N}$ tal que $n = n \cdot 1 > a^{-1}$ $(1 > 0)$. Logo, $n \cdot a > 1$. Então, $n^{-1} < a$.

iii) $\Rightarrow$ **i)**: Dado qualquer $b > 0$ em K, existe, por **iii)**, um $n \in \mathbb{N}$ tal que $n^{-1} < b^{-1}$ $(b^{-1} > 0)$, ou seja, $n > b$. Assim, nenhum elemento positivo de K pode ser cota superior de $\mathbb{N}$. Por outro lado, qualquer elemento não positivo de K é limitado por $1 \in \mathbb{N}$ $(1 > 0)$. Por fim, K é Arquimediano. □

Apresentaremos abaixo uma desigualdade, conhecida como desigualdade de Bernoulli, que desempenhará papel importante na construção dos números reais.

Proposição 3.19 (Desigualdade de Bernoulli)**.** *Sejam K um corpo ordenado e $x \in K$ tal que $x \geq -1$. Assuma que $n \in \mathbb{N}^*$. Então, $(1 + x)^n \geq 1 + nx$.*

Demonstração. Mostraremos o resultado por indução em n. Seja $X = \{n \in \mathbb{N}^* / (1+x)^n \geq 1+nx\}$. É fácil ver que

$$(1 + x)^1 = 1 + x \geq 1 + 1 \cdot x.$$

Logo $1 \in X$. Agora suponha que $n \in X$, ou seja, $(1+x)^n \geq 1+nx$. Consequentemente,

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n \cdot (1+x) \geq (1+nx) \cdot (1+x) \\ &= 1+nx+x+nx^2 = 1+(n+1)x+nx^2 \\ &\geq 1+(n+1)x,\end{aligned}$$

pois $x+1 \geq 0$. Portanto, $n+1 \in X$. Isto nos diz que $X = \mathbb{N}^*$. Como queríamos mostrar. □

Em ordem a motivarmos a construção do conjunto dos números reais, provamos abaixo que é possível mostrar a existência de um número que não é racional (no próximo capítulo construiremos tal conjunto, o qual contém tal elemento). Mais precisamente, temos a seguinte proposição.

Proposição 3.20. *A equação $x^2 = 2$ não tem solução em $\mathbb{Q}$.*

Demonstração. Suponhamos que a equação $x^2 = 2$ admite solução em $\mathbb{Q}$, digamos $x = \frac{a}{b} \in \mathbb{Q}$ (irredutível) soluciona a equação anterior. Assim sendo,

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

O que implica que $a^2 = 2 \cdot b^2$, isto é, $a = 2k$, com $k \in \mathbb{Q}$. Daí,

$$2 \cdot b^2 = a^2 = (2k)^2 = 4k^2.$$

Logo, $b^2 = 2k^2$. Por conseguinte, $b = 2k_1$, com $k_1 \in \mathbb{Q}$. O que nos diz que $\frac{a}{b}$ é redutível, uma contradição pela suposição feita. Portanto, a equação $x^2 = 2$ não tem solução em $\mathbb{Q}$. □

3.7 Sequências em $\mathbb{Q}$

Nesta seção, nossa meta é definir sequências em $\mathbb{Q}$ e apresentar algumas propriedades satisfeitas por estas mesmas aplicações em ordem a construir o conjunto dos números reais no próximo capítulo.

3.7.1 Limites de Sequências em $\mathbb{Q}$

Nesta subseção, estamos interessados em definir limites de sequências envolvendo números racionais. É importante destacar aqui que o processo de construção do conjunto dos números reais através destas sequências remete a Cantor.

Definição 3.14. Uma sequência de números racionais é uma aplicação $x : \mathbb{N}^* \to \mathbb{Q}$, que associa a cada número natural não nulo n um número racional definido por $x(n) = x_n$ (chamado termo geral), denotada por $x = (x_n)_{n\in\mathbb{N}^*} = (x_1, x_2, ...)$, onde $x_n \in \mathbb{Q}$, para todo $n \in \mathbb{N}^*$.

Gostaríamos de ressaltar que, quando não houver possibilidade de confusão, denotaremos a sequência, definida acima, simplesmente por (x_n).

Abaixo definimos quando uma sequência de números racionais converge.

Definição 3.15. Dizemos que uma sequência (x_n) converge para $a \in \mathbb{Q}$ e indicamos por $x_n \to a$, ou ainda, $\lim\limits_{n\to\infty} x_n = a$, se para um dado $\varepsilon \in \mathbb{Q}_+^*$ existe $n_0 \in \mathbb{N}^*$ tal que, $\forall n \geq n_0$, com $n \in \mathbb{N}^*$, tem-se $|x_n - a| < \varepsilon$.

Permita-nos exibir alguns exemplos de sequências convergentes.

Exemplo 3.8. Considere uma sequência constante (x_n), isto é, $x_n = c \in \mathbb{Q}$, para todo $n \in \mathbb{N}^*$. Logo, dado $\varepsilon \in \mathbb{Q}_+^*$, temos que

$$|x_n - c| = |c - c| = 0 < \varepsilon, \forall n \in \mathbb{N}^*.$$

Neste caso, $n_0 = 1 \in \mathbb{N}^*$. Dessa forma, toda sequência $(c)_{n\in\mathbb{N}^*}$ constante, com $c \in \mathbb{Q}$ é convergente e converge para c.

Exemplo 3.9. Considere a sequência $\left(\frac{1}{n}\right)$. Afirmamos que $\lim\limits_{n\to\infty} \frac{1}{n} = 0$. Com efeito, dado $\varepsilon \in \mathbb{Q}_+^*$, por $\mathbb{Q}$ ser Arquimediano, $\exists n_0 \in \mathbb{N}^*$ tal que $\frac{1}{\varepsilon} < n_0$. Portanto, $\forall n \geq n_0$, obtemos

$$\left|\frac{1}{n} - 0\right| = \frac{1}{n} \leq \frac{1}{n_0} < \varepsilon.$$

Proposição 3.21. *O limite de uma sequência, quando existe, é único.*

Demonstração. Suponhamos que $a \neq b$, de forma que $x_n \to a$ e $x_n \to b$. Tomando $\varepsilon = |b - a| > 0$, temos que $\varepsilon \in \mathbb{Q}_+^*$. Mas, como $x_n \to a$, então

$$\exists n_1 \in \mathbb{N}^* \text{ tal que } n \geq n_1 \Rightarrow |x_n - a| < \tfrac{\varepsilon}{2}.$$

E, por outro lado $x_n \to b$, assim

$$\exists n_2 \in \mathbb{N}^* \text{ tal que } n \geq n_2 \Rightarrow |x_n - b| < \tfrac{\varepsilon}{2}.$$

Seja $n_0 = \max\{n_1, n_2\}$, assim temos que para todo $n \geq n_0$, encontramos

$$\varepsilon = |b - a| = |b - x_n + x_n - a| \leq |b - x_n| + |x_n - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

O que é um absurdo. Portanto $a = b$. □

Agora, estabelecemos a seguinte definição de sequências limitadas.

Definição 3.16. Uma sequência (x_n) de números racionais diz-se limitada se existe $c \in \mathbb{Q}_+^*$ tal que $|x_n| \leq c$, para todo $n \in \mathbb{N}^*$.

Obs 3.4. Esta definição pode ser dada de forma equivalente da seguinte maneira: Uma sequência de (x_n) de números racionais, diz-se limitada se existem $a, b \in \mathbb{Q}$, de forma que $a \leq x_n \leq b$ para todo $n \in \mathbb{N}^*$. De fato, se $a \leq x_n \leq b$ então c pode ser tomado de forma que $c > \max\{|a|, |b|\}$ e, reciprocamente, se $|x_n| \leq c$, então $a = -c$ e $b = c$.

Teorema 3.19. Se $\lim_{n\to\infty} x_n = 0$ e (y_n) é uma sequência limitada, então $\lim_{n\to\infty} x_n y_n = 0$.

Demonstração. Existe $c \in \mathbb{Q}_+^*$ tal que $|y_n| \leq c$ para todo $n \in \mathbb{N}^*$. Dado $\varepsilon \in \mathbb{Q}_+^*$, como $\lim_{n\to\infty} x_n = 0$, podemos encontrar $n_0 \in \mathbb{N}^*$ tal que $n \geq n_0 \Rightarrow |x_n| < \frac{\varepsilon}{c}$. Logo, para todo $n \geq n_0$, obtemos

$$|x_n y_n| = |x_n||y_n| < \frac{\varepsilon}{c} \cdot c = \varepsilon.$$

Isto mostra que $\lim_{n\to\infty} x_n y_n = 0$. □

A seguir, apresentamos algumas propriedades básicas que envolvem limites de sequências.

Teorema 3.20. *Sejam (x_n) e (y_n) sequências em $\mathbb{Q}$. Se $\lim_{n\to\infty} x_n = a$ e $\lim_{n\to\infty} y_n = b$, então são válidas as seguintes afirmações:*

i) $\lim_{n\to\infty} (x_n \pm y_n) = a \pm b$;

ii) $\lim_{n\to\infty} x_n y_n = ab$;

ii) $\lim_{n\to\infty} \frac{x_n}{y_n} = \frac{a}{b}$, *se* $b \neq 0$.

Demonstração. **i)** Dado $\varepsilon \in \mathbb{Q}_+^*$, existem n_1 e n_2 em $\mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow |x_n - a| < \frac{\varepsilon}{2} \text{ e } n \geq n_2 \Rightarrow |y_n - b| < \frac{\varepsilon}{2}.$$

Tomando $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$, encontramos, para todo $n \geq n_0$,

$$|(x_n + y_n) - (a + b)| = |(x_n - a) + (y_n - b)| \leq |x_n - a| + |y_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Isto prova que $\lim_{n\to\infty}(x_n + y_n) = a + b$.

Analogamente ao caso acima, tem-se que dado $\varepsilon \in \mathbb{Q}_+^*$, existem n_3 e n_4 em $\mathbb{N}^*$ tais que

$$n \geq n_3 \Rightarrow |x_n - a| < \frac{\varepsilon}{2} \text{ e } n \geq n_4 \Rightarrow |y_n - b| < \frac{\varepsilon}{2}.$$

Assumindo $n_5 = \max\{n_3, n_4\} \in \mathbb{N}^*$, chegamos, para todo $n \geq n_5$, a

$$|(x_n - y_n) - (a - b)| = |(x_n - a) + [-(y_n - b)]| \leq |x_n - a| + |y_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Portanto, $\lim_{n\to\infty}(x_n - y_n) = a - b$.

ii) Primeiramente, note que

$$x_n y_n - ab = x_n y_n - x_n b + x_n b - ab = x_n(y_n - b) + (x_n - a)b, \forall n \in \mathbb{N}^*.$$

Ora (x_n) é uma sequência limitada e $\lim_{n\to\infty}(y_n - b) = 0$. Logo, pelo Teorema 3.19, $\lim_{n\to\infty}[x_n(y_n - b)] = 0$. Por motivo semelhante, $\lim_{n\to\infty}[(x_n - a)b] = 0$. Assim, temos que

$$\lim_{n\to\infty}(x_n y_n - ab) = \lim_{n\to\infty}[x_n(y_n - b)] + \lim_{n\to\infty}[(x_n - a)b] = 0,$$

donde $\lim_{n\to\infty} x_n y_n = ab$.

iii) Notemos que, como $y_n b \to b^2$, existe $n_0 \in \mathbb{N}^*$ tal que $n \geq n_0 \Rightarrow y_n b > \frac{b^2}{2}$ (basta tomar $\varepsilon = \frac{b^2}{2} \in \mathbb{Q}_+^*$ e achar o n_0 correspondente). Segue que para todo $n \geq n_0$, $\frac{1}{y_n b}$ é um número inferior a $\frac{2}{b^2}$. Logo, a sequência $\left(\frac{1}{y_n b}\right)$ é limitada. Ora, é fácil notar que

$$\frac{x_n}{y_n} - \frac{a}{b} = \frac{bx_n - ay_n}{y_n b} = (bx_n - ay_n)\frac{1}{y_n b}.$$

Como

$$\lim_{n\to\infty}(bx_n - ay_n) = ab - ab = 0,$$

segue, do Teorema 3.19, que $\lim_{n\to\infty}\left(\frac{x_n}{y_n} - \frac{a}{b}\right) = 0$. Portanto, $\lim_{n\to\infty}\frac{x_n}{y_n} = \frac{a}{b}$.

□

O resultado abaixo nos mostra que o limite é compatível com a relação de ordem em $\mathbb{Q}$.

Teorema 3.21. *Sejam (x_n), (y_n) sequências de números racionais tais que $x_n \leq y_n$, para todo $n \in \mathbb{N}^*$. Se $\lim_{n\to\infty} x_n = a$ e $\lim_{n\to\infty} y_n = b$, então $a \leq b$.*

Demonstração. Suponhamos $a > b$. Como $x_n \to a$ e $y_n \to b$, podemos tomar $\varepsilon = \frac{a-b}{2} \in \mathbb{Q}_+^*$ para obter $n_1 \in \mathbb{N}$ tal que para todo $n \geq n_1$, tem-se $|x_n - a| < \varepsilon$, isto é, $a - \varepsilon < x_n$, ou seja, $\frac{a+b}{2} < x_n$.

Analogamente, obtém-se $n_2 \in \mathbb{N}$ tal que para todo $n \geq n_2$, chega-se a $|y_n - b| < \varepsilon$, isto é, $y_n < b + \varepsilon$, ou seja, $y_n < \frac{a+b}{2}$. Tomando $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$, temos

$$y_n < \frac{a+b}{2} < x_n, \forall n \geq n_0^*.$$

Isto contraria a hipótese $x_n \leq y_n, \forall n \in \mathbb{N}^*$. Por fim, $a \leq b$. □

Um caso particular para o Teorema 3.21 pode ser enunciado como segue.

Corolário 3.22. *Sejam $c \in \mathbb{Q}$ e (x_n) uma sequência de números racionais. Se $x_n \leq b$ para todo $n \in \mathbb{N}^*$ e $\lim_{n\to\infty} x_n = a$, então $a \leq b$.*

Demonstração. Basta usarmos o Teorema 3.21 e tomarmos $y_n = b, \forall n \in \mathbb{N}$. □

Obs 3.5. Se $x_n \leq 0$, $\forall n \in \mathbb{N}^*$, então $\lim_{n\to\infty} x_n$, caso exista, é menor do que ou igual a 0 (basta usar o Teorema 3.21 com $y_n = 0, \forall n \in \mathbb{N}^*$).

Obs 3.6. Se $y_n \geq 0$, $\forall n \in \mathbb{N}^*$, então $\lim_{n\to\infty} y_n$, caso exista, é maior do que ou igual a 0 (basta usar o Teorema 3.21 com $x_n = 0, \forall n \in \mathbb{N}^*$).

Obs 3.7. Observe que se $x_n > 0$, $\forall n \in \mathbb{N}^*$ não significa que $\lim_{n\to\infty} x_n > 0$ (mesmo que este elemento exista). Considere, por exemplo, a sequência $x_n = \frac{1}{n}$, a qual satisfaz $\lim_{n\to\infty} x_n = 0$.

3.7.2 Sequências de Cauchy em $\mathbb{Q}$

Nesta subseção, nossa meta é definir sequências de Cauchy em $\mathbb{Q}$ e apresentar algumas propriedades satisfeitas por estas mesmas aplicações em ordem a construir o conjunto dos números reais no próximo capítulo.

Definição 3.17. Uma sequência (x_n) de elementos em $\mathbb{Q}$ é chamada sequência de Cauchy, se dado $\varepsilon \in \mathbb{Q}_+^*$, existe $n_0 \in \mathbb{N}$ tal que, $\forall m, n \in \mathbb{N}^*$, com $m, n \geq n_0$, tem-se $|x_n - x_m| < \varepsilon$.

A proposição abaixo nos diz que toda sequência de Cauchy de números racionais é limitada.

Proposição 3.22. *Seja (x_n) uma sequência de Cauchy de números racionais. Então, (x_n) é limitada.*

Demonstração. Para $\varepsilon = 1 > 0$, existe $n_0 \in \mathbb{N}^*$ tal que,

$$\forall m, n \in \mathbb{N}^*, \text{ com } m, n \geq n_0 \Rightarrow |x_n - x_m| < 1.$$

Em particular, $|x_m - x_{n_0}| < 1$ para todo $m \geq n_0$. Mas, para todo $m \geq n_0$, temos

$$|x_m| = |x_m - x_{n_0} + x_{n_0}| \leq |x_m - x_{n_0}| + |x_{n_0}| < 1 + |x_{n_0}|.$$

Sendo $c = \max\{|x_1|, |x_2|, ..., |x_{n_0-1}|, 1 + |x_{n_0}|\} \in \mathbb{Q}$, então, para todo $n \in \mathbb{N}^*$, temos que $|x_n| \leq c$. Portanto, (x_n) é limitada. □

A proposição a seguir nos mostra como provar que a soma de duas sequências de Cauchy em $\mathbb{Q}$ é, novamente, uma sequência do mesmo tipo.

Teorema 3.23. *Sejam (x_n), (y_n) sequências de Cauchy de números racionais, então $(x_n) \pm (y_n) := (x_n \pm y_n)$ também o é.*

Demonstração. Como (x_n), (y_n) são sequências de Cauchy de números racionais, então dado $\varepsilon \in \mathbb{Q}_+^*$, existem $n_1, n_2 \in \mathbb{N}^*$ tais que, $\forall m, n \in \mathbb{N}^*$, tem-se

$$m, n \geq n_1 \Rightarrow |x_n - x_m| < \frac{\varepsilon}{2} \text{ e } m, n \geq n_2 \Rightarrow |y_m - y_n| < \frac{\varepsilon}{2}.$$

Seja $n_0 = \max\{n_1, n_2\}$, então, para todo $m, n \in \mathbb{N}^*$, com $m, n \geq n_0$, obtém-se

$$|(x_m + y_m) - (x_n + y_n)| = |(x_m - x_n) \pm (y_m - y_n)| \leq |(x_m - x_n)| + |(y_m - y_n)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Portanto, $(x_n) \pm (y_n)$ é sequência de Cauchy de números racionais. □

Não só a adição, mas a multiplicação, definida de maneira usual, de sequências de Cauchy em $\mathbb{Q}$ gera uma sequência do mesma categoria.

Teorema 3.24. *Sejam (x_n), (y_n) sequências de Cauchy de números racionais, então $(x_n) \cdot (y_n) := (x_n y_n)$ também o é.*

Demonstração. É fácil checar que

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n y_n - x_m y_n + x_m y_n - x_m y_m| \\ &\leq |y_n||x_n - x_m| + |x_m||y_n - y_m|, \forall n, m \in \mathbb{N}. \end{aligned}$$

Como (x_n), (y_n) são sequências de Cauchy de números racionais, então, pela Proposição 3.22, temos que (x_n), (y_n) são limitadas e, assim, existem $c, d \in \mathbb{Q}_+^*$ tais que $|x_n| \leq c$, $|y_n| \leq d$ para todo $n \in \mathbb{N}^*$. Tomando $k = \max\{c, d\} \in \mathbb{Q}_+^*$, obtemos que

$$|x_n| \leq k \text{ e } |y_n| \leq k, \forall n \in \mathbb{N}^*.$$

E daí,

$$|x_n y_n - x_m y_m| \leq |y_n||x_n - y_m| + |x_m||y_n - y_m| \leq k|x_n - x_m| + k|y_n - y_m|, \forall n \in \mathbb{N}.$$

Ainda pelo fato de (x_n), (y_n) serem sequências de Cauchy de números racionais, dado $\varepsilon \in \mathbb{Q}_+^*$, temos que existem $n_1, n_2 \in \mathbb{N}^*$, de modo que, para todo $m, n \in \mathbb{N}^*$, encontramos

$$m, n \geq n_1 \Rightarrow |x_n - x_m| < \frac{\varepsilon}{2k} \text{ e } m, n \geq n_2 \Rightarrow |y_n - y_m| < \frac{\varepsilon}{2k}.$$

Seja $n_0 = \max\{n_1, n_2\}$, então, para todo $m, n \in \mathbb{N}^*$, com $m, n \geq n_0$, temos que

$$|x_m y_m - x_n y_n| < k \cdot \frac{\varepsilon}{2k} + k \cdot \frac{\varepsilon}{2k} = \varepsilon.$$

Portanto $(x_n) \cdot (y_n)$ é sequência de Cauchy de números racionais. □

Além da adição e da multiplicação, se considerarmos o módulo em cada termo de uma sequência de Cauchy em $\mathbb{Q}$, então encontramos outra sequência do mesmo tipo.

Proposição 3.23. *Seja (x_n) uma sequência de Cauchy de números racionais. Então, $(|x_n|)$ é uma sequência de Cauchy.*

Demonstração. Dado $\varepsilon \in \mathbb{Q}_+^*$, existe $n_0 \in \mathbb{N}^*$ tal que, para todo $m, n \in \mathbb{N}^*$, tem-se

$$m, n \geq n_0 \Rightarrow |x_n - x_m| < \varepsilon.$$

Por outro lado, para todo $m, n \geq n_0$, obtém-se

$$||x_n| - |x_m|| \leq |x_n - x_m| < \varepsilon.$$

Portanto, $(|x_n|)$ é uma sequência de Cauchy de números racionais. □

A proposição abaixo nos garante que se tivermos uma sequência, constituída de termos não nulos, que não converge para zero, então é possível definir uma outra sequência com os inversos dos termos da sequência original. O resultado obtido será novamente uma sequência de Cauchy.

Proposição 3.24. *Seja (x_n) uma sequência de Cauchy de números racionais tal que $\lim_{n\to\infty} x_n \neq 0$ e $x_n \neq 0$, para todo $n \in \mathbb{N}^*$. Então, $\left(\frac{1}{x_n}\right)$ é uma sequência de Cauchy.*

Demonstração. Primeiramente observe que

$$\Big|\frac{1}{x_m} - \frac{1}{x_n}\Big| = \Big|\frac{x_n - x_m}{x_n x_m}\Big| = \frac{|x_n - x_m|}{|x_n||x_m|}, \forall n \in \mathbb{N}^*.$$

Por outro lado, como $x_n \nrightarrow 0$, então $\exists \varepsilon_0 \in \mathbb{Q}_+^*$ tal que $\forall y \in \mathbb{N}^*$ podemos encontrar $n_y \in \mathbb{N}^*$ de forma que $n_y \geq y$ e $|x_{n_y}| \geq \varepsilon_0$.

Como (x_n) é uma sequência de Cauchy, então, pela Proposição 3.23, $(|x_n|)$ também o é. Portanto, $\exists m_1 \in \mathbb{N}^*$ tal que para todo $m, n \geq m_1$, tem-se que $||x_m| - |x_n|| < \frac{\varepsilon_0}{2}$. Deste modo, infere-se $||x_m| - |x_{n_{m_1}}|| < \frac{\varepsilon_0}{2}$, para todo $m \geq m_1$. Então,

$$\frac{-\varepsilon_0}{2} < |x_m| - |x_{m_1}| \leq |x_m| - \varepsilon_0, \forall m \geq m_1,$$

ou equivalentemente,

$$\frac{1}{|x_m|} < \frac{2}{\varepsilon_0} =: k, \forall m \geq m_1.$$

Novamente, usando o fato que (x_n) é uma sequência de Cauchy, temos que existe $n_2 \in \mathbb{N}^*$ de modo que

$$\forall m, n \in \mathbb{N}^*, \text{ com } m, n \geq n_2 \Rightarrow |x_n - x_m| < \frac{\varepsilon}{k^2}.$$

Tomando $n_0 = \max\{m_1, n_2\} \in \mathbb{N}^*$ temos, para todo $n, m \in \mathbb{N}^*$, com $n, m \geq n_0$, que

$$\Big|\frac{1}{x_m} - \frac{1}{x_n}\Big| = \frac{|x_n - x_m|}{|x_n||x_m|} < \frac{\varepsilon}{k^2} \cdot k^2 = \varepsilon.$$

Isto completa a prova da proposição em questão. □

A seguir, provaremos que toda sequência convergente de números racionais é uma sequência de Cauchy.

Teorema 3.25. *Seja (x_n) uma sequência convergente de números racionais. Então, (x_n) é também uma sequência de Cauchy em $\mathbb{Q}$.*

Demonstração. Suponha que $x_n \to a \in \mathbb{Q}$. Então, dado $\varepsilon \in \mathbb{Q}_+^*$, existe $n_0 \in \mathbb{N}^*$ tal que

$$\forall n \in \mathbb{N}^*, n \geq n_0 \Rightarrow |x_n - a| < \frac{\varepsilon}{2}.$$

Desse modo, para todo $m, n \in \mathbb{N}^*$, com $m, n \geq n_0$, tem-se que

$$|x_n - x_m| = |x_n - a + a - x_m| \leq |x_n - a| + |x_m - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Consequentemente, (x_n) é uma sequência de Cauchy em $\mathbb{Q}$. □

Toda sequência convergente de números racionais são sequências de Cauchy em $\mathbb{Q}$, então ser sequência de Cauchy é uma condição necessária de convergência; porém, não é condição suficiente. Na verdade, existem sequências de Cauchy em $\mathbb{Q}$ que não converge em $\mathbb{Q}$, como mostra o exemplo a seguir.

Exemplo 3.10. Consideremos (x_n) a sequência das raízes aproximadas de 2, construída como se segue:

Seja x_1 o maior inteiro tal que $x_1^2 \leq 2$. Substituindo os possíveis valores para x_1 descobrimos que $x_1 = 1$.

Seja x_2 o maior racional da forma $1 + \frac{b_1}{10}$, onde b_1 pode ser $0, 1, 2, ...$ ou 9, determinado por substituição direta de modo que $x_2^2 \leq 2$. Fazendo os cálculos obtemos $b_1 = 4$.

Assuma x_3 o maior racional da forma $1 + \frac{b_1}{10} + \frac{b_2}{10^2}$, onde b_2 pode ser $0, 1, 2, ...$ ou 9, determinado por substituição direta de modo que $x_3^2 \leq 2$. Fazendo os cálculos obtemos $b_2 = 1$. E assim sucessivamente. Logo, o termo geral da sequência (x_n) para todo $n \in \mathbb{N}^*$ é dado por

$$x_n = 1 + \frac{4}{10} + \frac{1}{10^2} + ... + \frac{b_n}{10^n}, \forall \in \mathbb{N}^*.$$

Mostraremos que (x_n) não converge para nenhum número racional. Com esta finalidade vamos inicialmente provar que $x_n^2 \longrightarrow 2$. Sabemos, através da construção acima, que $x_n^2 \leq 2$ para todo $n \in \mathbb{N}$ e também que

$$\left(1 + \frac{4}{10} + \frac{1}{10^2} + ... + \frac{b_n + 1}{10^n}\right)^2 > 2.$$

Logo,

$$\begin{aligned} \left(1 + \frac{4}{10} + \frac{1}{10^2} + ... + \frac{b_n}{10^n} + \frac{1}{10^n}\right)^2 > 2 \quad &\Rightarrow \quad \left(x_n + \frac{1}{10^n}\right)^2 > 2 \\ &\Rightarrow \quad x_n^2 + \frac{2x_n}{10^n} + \frac{1}{10^{2n}} > 2 \\ &\Rightarrow \quad 2 - x_n^2 < \frac{2x_n}{10^n} + \frac{1}{10^{2n}}. \end{aligned}$$

Mas, $\frac{1}{10^{2n}} < \frac{1}{10^n}$ e $x_n < 2$ implicam

$$2 - x_n^2 < \frac{4}{10^n} + \frac{1}{10^n} = \frac{5}{10^n}.$$

Como $2 - x_n^2 \geq 0$, então

$$|x_n^2 - 2| = 2 - x^2 < \frac{5}{10^n}.$$

Assim, dado $\varepsilon \in \mathbb{Q}_+^*$ existe $n_0 \in \mathbb{N}^*$ tal que $n_0 > \frac{5}{9\varepsilon} - \frac{1}{9}$ ($\mathbb{Q}$ é Arquimediano). Assim sendo, temos que

$$\forall n \in \mathbb{N}, n \geq n_0 \Rightarrow |x_n^2 - 2| < \frac{5}{10^n} < \varepsilon,$$

basta usar a desigualdade de Bernoulli. Portanto, $x_n^2 \to 2$. Agora vamos provar que (x_n) é uma sequência de Cauchy.

Acabamos de provar que (x_n^2) é convergente. Assim sendo, em consequência do Teorema 3.25, segue que (x_n^2) é uma sequência de Cauchy. Então, dado $\varepsilon \in \mathbb{Q}_+^*$ existe $n_0 \in \mathbb{N}^*$ tal que

$$\forall n, m \in \mathbb{N}, n, m \geq n_0 \Rightarrow |x_m^2 - x_n^2| < 2\varepsilon.$$

Mas, por distributividade, podemos concluir que

$$|x_m - x_n||x_m + x_n| = |x_m^2 - x_n^2| < 2\varepsilon \Rightarrow |x_m - x_n| < \frac{2\varepsilon}{|x_m + x_n|}.$$

Como $|x_m + x_n| > 2$ (ver construção de (x_n)), então, para todo $m, n \geq n_0$, temos

$$|x_m - x_n| < \frac{2\varepsilon}{|x_m + x_n|} < \frac{2\varepsilon}{2} = \varepsilon.$$

Isto nos mostra que (x_n) é de Cauchy em $\mathbb{Q}$.

Suponhamos, finalmente, que existe um número racional $\frac{a}{b}$ tal que $x_n \to \frac{a}{b}$, então, pelo Teorema 3.20, chegamos a $x_n^2 \to \left(\frac{a}{b}\right)^2$. Porém, já provamos que $x_n^2 \to 2$. Como o limite de uma sequência de números racionais é único, de acordo com a Proposição 3.21, então $\left(\frac{a}{b}\right)^2 = 2$. Já provamos que isto é um absurdo. Logo, (x_n) não converge para nenhum número racional.

3.8 Aplicação dos racionais (Método de Sylvester)

Nossa aplicação neste capítulo, inicialmente, será uma aplicação de um método proposto pelo matemático James Joseph Sylvester (1814 - 1897). Sylvester propôs escrever um número racional a, $0 < a < 1$, como soma de frações unitárias. Vamos chamar de frações unitárias as frações de numerador 1. Toda fração unitária pode ser desdobrada como soma de duas frações unitárias.

James Joseph Sylvester

Professor e matemático inglês nascido em Londres, um dos criadores da álgebra moderna e publicou numerosos trabalhos, notadamente sobre polinômios. Contribuiu fundamentalmente no desenvolvimento da teoria matricial, teoria dos invariantes, teoria dos números e análise combinatória. Desempenhou papel fundamental no desenvolvimento da matemática nos Estados Unidos na segunda metade do século XIX, quando professor da Universidade Johns Hopkins e fundador do American Journal of Mathematics. Criou a palavra totiente, pela qual é reconhecida a Função totiente de Euler, usada em teoria dos números e criptografia RSA, a qual foi usada por Leonhard Euler para provar o Pequeno Teorema de Fermat.

Freqüentou duas escolas primárias em Londres, e teve a instrução secundária na Royal Institution em Liverpool. Entrou (1833) e fez graduação no St. John's College, em Cambridge e teve como colegas dois outros matemáticos famosos: Duncan Gregory e George Green. Para obter o grau era necessário para um estudante assinar um juramento religioso para a Igreja de Inglaterra, mas como ele era judeu, e de temperamento irrequieto e irreverente, recusou-se a fazer o juramento necessário e, assim, não pôde se formar e, assim, também não pode ganhar o Smith's prize nem o Fellowship. Foi ensinar física na University of London (1838) onde seu professor De Morgan também ensinava, um dos poucos lugares que não o vetaram por causa da sua religião, lá permanecendo durante três anos. Eleito Fellow da Royal Society (1839), foi ensinar na Universidade da Virgínia (1841), onde ficou apenas três meses, fugindo para Nova Iorque depois de bater em um estudante que o tinha insultado, e voltando para a Inglaterra. No período seguinte (1841-1850), formou-se em direito e trabalhou como atuário e advogado, mas deu instrução de matemática. Então, conheceu Cayley, que também era um advogado, opostamente um sujeito de temperamento dócil. Ambos trabalharam nos tribunais da Pousada de Lincoln em Londres e tornaram-se grandes amigos e resolveram abandonar as leis para se dedicarem a matemática. Desenvolveram importante trabalho em teoria de matrizes para estudos de geometria (1851) e editaram várias publicações conjuntas sobre a teoria das invariantes, chegando a serem chamados de gêmeos invariantes. Tornou-se professor de matemática na Royal Military Academy em Woolwich (1854) e ganhou a Royal Society Royal Medal (1861). Aposentado compulsoriamente da academia militar aos 55 anos, publicou The Laws of Verse, um texto matemático em versos do qual muito se envaidecia, ponto de às vezes se assinar "J. J. Sylvester, autor de As Leis de Verso". Tornou-se o segundo presidente London Mathematical Society (1866-1868), substituindo De Morgan. Voltou aos Estados Unidos (1876), desta vez para a então recém-fundada Johns Hopkins University, onde ficou (1876-1883), e fundou (1878) o American Journal of Mathematics, a primeira revista de matemática dos EEUU. Voltou a Inglaterra para

ensinar na Universidade de Oxford, convidado para a cadeira de Savilian Professor of Geometry (1883). Foi agraciado com Royal Society Copley Medal (1880) e foi o primeiro ganhador da medalha de ouro que a Sociedade premiou em honra a De Morgan, a De Morgan Medal (1887). Com atritos com os estudantes e sofrendo de perda de memória, voltou a Londres (1892) onde dedicou seus últimos anos ao Athenaeum.

O método

Vejamos a descrição do método:

i) achar a maior fração unitária que seja menor que a fração dada
ii) subtrair essa fração unitária da fração dada
iii) achar a maior fração unitária menor que a diferença obtida em ii
iv) subtrair desta diferença, a fração unitária obtida em iii
v) continuar o processo até que uma das diferenças seja fração unitária.

Aplicação do método

Agora iremos aplicar esse processo à seguinte fração: $\frac{13}{20}$

Resolução:

$$\frac{1}{a} < \frac{13}{20} \Rightarrow 20 < 13a$$

Logo $a = 2$ é o menor natural para o qual a desigualdade se verifica.

Como $\frac{3}{20} - \frac{1}{7} = \frac{1}{140}$ é unitária, então $\frac{13}{20} = \frac{1}{2} + \frac{3}{20} = \frac{1}{2} + \frac{1}{7} + \frac{1}{140}$.

Uma outra aplicação

Seja K um corpo. Uma aplicação bijetora $f : K \to K$ se diz um *automorfismo* de K se: $f(x+y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$, para todo par de elementos $x, y \in K$. Mostre, através das etapas seguintes, que o único automorfismo f de $\mathbb{Q}$ é a aplicação idêntica: i) $f(1) = 1$; ii) $f(-a) = -f(a), \forall a \in \mathbb{Q}$; iii) $f(m) = m, \forall m \in \mathbb{Z}$; iv) $f(\frac{1}{n}) = (\frac{1}{n}), \forall n \in \mathbb{N}^*$; v) $f(\frac{m}{n}) = \frac{m}{n}, \forall m, n \in \mathbb{Z}, n \neq 0$.

Resolução: ii) Como $f(0) = f(0+0) = f(0) + f(0)$, então, pela lei do cancelamento da adição, $f(0) = 0$. Assim, $\forall a \in \mathbb{Q}$: $f(-a) + f(a) = f((-a) + a) = f(0) = 0$; então, $f(-a) = -f(a)$. iv) $1 = f(1) = f(\frac{n}{n}) = f(n.\frac{1}{n}) = f(\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}) = f(\frac{1}{n}) + f(\frac{1}{n}) + \ldots + f(\frac{1}{n}) = nf(\frac{1}{n}) \Longrightarrow f(\frac{1}{n}) = \frac{1}{n}$. v) Admitindo $n > 0$, o que sempre é possível, $f(\frac{m}{n}) = f(m.\frac{1}{n}) = f(m)f(\frac{1}{n}) = m.\frac{1}{n} = \frac{m}{n}$.

Capítulo 4

Construção do Números Reais

Neste capítulo, estudaremos a construção dos chamados números reais a partir dos números racionais através de dois métodos diferentes: Cortes de Dedekind e Sequências de Cauchy (referimos a [6, 7, 8, 9, **?**]).

4.1 Construção por Cortes de Dedekind

Permita-nos começarmos a construção dos números reais pelos famosos cortes de Dedekind. É importante ressaltar que a teoria desenvolvida no capítulo anterior é imprescindível para o entendimento desta seção.

4.1.1 Conjunto dos Cortes

Nesta subseção, definiremos qual é significado matemático para cortes e classificaremos quais cortes admitem cota superior mínima.

Definição 4.1. Um conjunto α de números racionais diz-se um corte se satisfizer as seguintes condições:

i) $\alpha \neq \emptyset$ e $\alpha \neq \mathbb{Q}$;

ii) se $r \in \alpha$ e $s < r$, $s \in \mathbb{Q}$, então $s \in \alpha$;

iii) α não admite elemento máximo.

Vejamos um exemplo de conjunto que é um corte e outros que não satisfazem a definição acima.

Exemplo 4.1. O conjunto $\alpha = \{x \in \mathbb{Q}/x < \frac{3}{5}\}$ é um corte.

i) Como $0 \in \alpha$ temos que $\alpha \neq \emptyset$. Além disso, $\alpha \neq \mathbb{Q}$, pois $1 \in \mathbb{Q}$ e $1 \notin \alpha$;

ii) Seja $r \in \alpha$ e $s < r$ (com $s \in \mathbb{Q}$); assim, $s < r < \frac{3}{5}$. Daí, temos $s < \frac{3}{5}$. Logo, $s \in \alpha$;

iii) Suponhamos que exista um elemento máximo em α, digamos $x = \max \alpha$. Daí, segue que $r \leq x$ para todo $r \in \alpha$, então $x < \frac{3}{5}$. Através da Proposição 3.11, concluímos que

$$x < 2^{-1}(x + \frac{3}{5}) < \frac{3}{5}.$$

O que é um contradição, visto que $x = \max \alpha$. Logo, α não possui elemento máximo.

Portanto, α é um corte.

Exemplo 4.2. O conjunto $\beta = \{x \in \mathbb{Q}/x > \frac{3}{5}\}$ não é um corte. Note que $1 \in \beta$, $0 \notin \beta$ e $0 < 1$. Portanto, β não é um corte.

Exemplo 4.3. O conjunto $\gamma = \{x \in \mathbb{Q}/x \leq \frac{3}{5}\}$ não é um corte. Observe que $\frac{3}{5}$ é o elemento máximo de γ. Este fato contraria o item **iii)** da Definição 4.1. Portanto, γ não é um corte.

Exemplo 4.4. O conjunto $\delta = \{x \in \mathbb{Q}/ -3 < x < \frac{8}{5}\}$ não é um corte. De fato, seja $r = 1 \in \delta$ e $s = -4 \in \mathbb{Q}$; logo, $-4 \notin \delta$. Portanto, δ não é um corte.

Exemplo 4.5. $\theta = \mathbb{Q}^*$ não é um corte. Qualquer que seja $r > 0$ temos que $r \in \theta$. Mas $s = 0 \in \mathbb{Q}$, satisfaz $s < r$ e $s \notin \theta$. Portanto, θ não é um corte.

Exemplo 4.6. $\omega = \{1, 4, \frac{3}{5}\}$ não é um corte. Note que $r = 4 \in \omega$ e $s = 2 \in \mathbb{Q}$ (com $s < r$). Todavia, $2 \notin \omega$. Portanto, ω não é um corte.

A seguir provaremos que todo corte é limitado superiormente em $\mathbb{Q}$.

Proposição 4.1. *Seja γ um corte. Então, γ é limitado superiormente.*

Demonstração. Seja γ um corte. Suponhamos, por absurdo, que γ é ilimitado superiormente em $\mathbb{Q}$, i.e, que para cada $a \in \mathbb{Q}$ $\exists r_a \in \gamma$, tal que $a < r_a$. Assim, do fato que $\emptyset \neq \gamma \neq \mathbb{Q}$ (item **i**) da Definição 4.1), temos que $\exists a_0 \in \mathbb{Q}$ com $a_0 \notin \gamma$. Para $a_0 \in \mathbb{Q}$, $\exists r_{a_0} \in \gamma$ tal que $a_0 < r_{a_0}$. Logo, $a_0 \in \gamma$ pelo item **ii**) da Definição 4.1. Isto é um absurdo ($a_0 \notin \gamma$). Portanto, todo corte é limitado superiormente em $\mathbb{Q}$. □

O resultado abaixo nos mostra como caracterizar todas as cotas superiores de um corte.

Proposição 4.2. *Seja α um corte e $r \in \mathbb{Q}$. Então, r é cota superior de α se, e somente se, $r \in \mathbb{Q}\backslash\alpha$.*

Demonstração. ($\Rightarrow$) Se r é cota superior de α, então r não pode pertencer a α, caso contrário r seria elemento máximo de α. Isto contradiz o item **iii)** da definição de corte.

($\Leftarrow$) Se $r \in \mathbb{Q}\backslash\alpha$, então r é cota superior de α, pois, caso contrário, haveria $s \in \alpha$ tal que $r < s$, o que, pelo item **ii)** da definição de corte, obrigaria r a pertencer a α. Isto é uma contradição. □

A proposição abaixo nos mostra como exemplificar alguns cortes que admitem cota superior mínima.

Proposição 4.3. *Se $r \in \mathbb{Q}$ e $\alpha = \{x \in \mathbb{Q}/x < r\}$, então α é um corte e r é a menor cota superior de α.*

Demonstração. Vejamos como justificar cada item da definição de corte para α.

i) $\alpha \neq \emptyset$, pois $x = r - 1 \in \alpha$. Além disso, $\alpha \neq \mathbb{Q}$, pois $r \notin \alpha$ e $r \in \mathbb{Q}$.

ii) Sejam $s \in \alpha$, $t \in \mathbb{Q}$ e $t < s$. Assim, $t < s < r$. Consequentemente, $t < r$. Portanto $t \in \alpha$;

iii) Suponha, por absurdo, que exista um elemento $s = \max \alpha$. Daí teríamos $s < r$ ($s \in \alpha$) e, portanto $s < 2^{-1}(s + r) < r$. Contrariando a maximalidade de s ($2^{-1}(s + r) \in \alpha$ e $s < 2^{-1}(s + r)$). Logo, temos que α não possui elemento máximo.

Portanto α é um corte. Agora mostraremos que r é a menor cota superior de α. De fato, pela Proposição 4.2, concluímos que r é cota superior de α, já que $r \in \mathbb{Q}\backslash\alpha$. Além disso, se $s \in \mathbb{Q}$ é cota superior de α e $s < r$, teríamos $s \in \alpha$ (α é um corte). Assim, s seria o elemento máximo de α, contradizendo assim o fato de α ser corte. Portanto, $r \leq s$ para toda cota superior $s \in \alpha$, isto é, r é a menor cota superior de α. □

Definição 4.2. Os cortes do tipo da Preposição 4.3 são denominados cortes racionais e são representados por r^*, i.e.,

$$r^* = \{x \in \mathbb{Q}/x < r\},$$

onde $r \in \mathbb{Q}$.

O resultado abaixo comprova que a recíproca da Proposição 4.3 é verdadeira.

Proposição 4.4. *Todo corte que possui cota superior mínima é racional.*

Demonstração. Seja γ um corte com cota superior mínima, digamos r. Assim, $x \leq r$, $\forall x \in \gamma$. Note que $r \notin \gamma$; caso contrário $r \in \gamma$, teríamos que r seria um máximo para γ. Isto é um absurdo de acordo com a definição de corte. Logo, $x < r$, $\forall x \in \gamma$.

Afirmamos que $\gamma = r^*$. De fato, seja $s \in r^*$, então $s \in \mathbb{Q}$ e $s < r$. Pela minimalidade de r, temos que s não é cota superior de γ. Dessa forma, $\exists x_0 \in \gamma$ tal que $s < x_0$. Como γ é um corte, então $s \in \gamma$. Logo, $r^* \subseteq \gamma$. Reciprocamente, se $x \in \gamma$ então $x < r$ (pelo que já foi feito acima). Isto nos diz que $x \in r^*$. Portanto, $\gamma \subseteq r^*$. Por fim, $\gamma = r^*$, i.e., γ é um corte racional.

□

Vejamos um exemplo de um corte que não é racional

Teorema 4.1. Seja $\alpha = \mathbb{Q}_-^* \cup \{x \in \mathbb{Q}_+ / x^2 < 2\}$. Então α é um corte que não é racional.

Demonstração. Primeiramente vamos mostrar que α é um corte.

i) $\alpha \neq \emptyset$, pois $0 \in \alpha$. Além disso, $\alpha \neq \mathbb{Q}$, pois $3 \in \mathbb{Q}$ e $3 \notin \alpha$;

ii) Sejam $r \in \alpha$ e $s \in \mathbb{Q}$, com $s < r$. Daí,

- se $s \in \mathbb{Q}_-^*$, então $s \in \alpha$;
- se $s > 0$, então $s^2 < r^2 < 2$ ($r \in \alpha$), ou seja, $s \in \alpha$;

iii) Para cada $r \in \alpha$ é possível encontrar um racional s tal que $r < s$ (isto significa que α não possui máximo). De fato, suponhamos que $r \in \alpha$. Dessa forma,

- se $r \in \mathbb{Q}_-^*$, então $s = 1 \in \alpha$ e $r < s$;
- se $r > 0$ e $r^2 < 2$, tomemos $h \in \mathbb{Q}$ com $0 < h < \min\{1, \frac{2-r^2}{2r+1}\}$ (use a média aritmética para garantir a existência de h). Seja $s = r + h$. Logo, $s \in \mathbb{Q}$ e $r < s$. Além disso,

$$s^2 = r^2 + 2rh + h^2 = r^2 + (h + 2r)h.$$

Como $0 < h < 1$, temos que

$$s^2 < r^2 + (1 + 2r)h.$$

Por outro lado, como $h < \frac{2-r^2}{2r+1}$, chegamos a

$$s^2 < r^2 + (1 + 2r)\frac{2 - r^2}{2r + 1} < r^2 + 2 - r^2 = 2.$$

Portanto, $s \in \alpha$. Donde, concluímos que α é um corte.

Mostraremos agora que α não possui cota superior mínima (a Proposição 4.4 nos diz que α não é racional). Os racionais que não pertencem a α são os positivos que têm quadrado maior ou igual a 2. Além disso, sabemos que não existe racional cujo quadrado é igual a 2 (ver Proposição 3.20). Sendo assim, q é uma cota superior de α se $q \in \mathbb{Q}_+^*$ e $q^2 > 2$. Mostraremos que, para cada cota superior p, encontraremos outra cota superior q tal que $q < p$. De fato, seja p uma cota superior de α, ou seja, $p \in \mathbb{Q}_+^*$ e $p^2 > 2$. Seja $q = p - \frac{p^2-2}{2p}$. Assim, $0 < q < p$, pois $p^2 - 2 > 0$ e

$$q^2 = p^2 - 2p\frac{p^2-2}{2p} + \left(\frac{p^2-2}{2p}\right)^2 = 2 + \left(\frac{p^2-2}{2p}\right)^2 > 2.$$

Logo, $q < p$ e $q^2 > 2$. Como queríamos demonstrar. □

Para finalizar esta subseção acrescentaremos um notação para o conjunto de todos os cortes.

Definição 4.3. Denotaremos por $\mathbb{R}$ o conjunto de todos os cortes, i.e.,

$$\mathbb{R} = \{\alpha \subset \mathbb{Q} / \alpha \text{ é um corte}\}.$$

4.1.2 Relação de Ordem Envolvendo Cortes

Nesta subseção, definiremos uma relação de ordem em $\mathbb{R}$. Mais precisamente, esclareceremos quando um corte é menor do que ou igual a outro.

Definição 4.4. Sejam $\alpha, \beta \in \mathbb{R}$. Dizemos que α é menor do que β, e escrevemos $\alpha < \beta$, quando $\beta \backslash \alpha \neq \emptyset$.

Os símbolos $\leq, >, \geq$ podem ser definidos de maneira natural, através da definição de $<$ dada acima.

Exemplo 4.7. Vejamos alguns exemplos para a definição acima.

1) $(\frac{3}{5})^* < 4^*$, pois $2 \in 4^* \backslash (\frac{3}{5})^*$;

2) $0^* < 1^*$, pois $\frac{1}{2} \in 1^* \backslash 0^*$;

3) $(-3)^* < 0^*$, pois $-1 \in 0^* \backslash (-3)^*$;

4) Seja α o corte do Teorema 4.1. Então $\alpha < 2^*$, pois $\frac{18}{10} \in 2^* \backslash \alpha$.

Vejamos abaixo como definir os sinais dos cortes, através da definição dada acima.

Definição 4.5. Dizemos que $\alpha \in \mathbb{R}$ é um corte positivo se $\alpha > 0^*$. Analogamente, chamamos α corte negativo se $\alpha < 0^*$. α é dito corte não negativo se $\alpha \leq 0^*$. Se escrevermos $\alpha \geq 0^*$, então dizemos que α é um corte não positivo.

Exemplo 4.8. O corte 1^* é positivo, pois $1^* > 0^*$. Já $(-3)^*$ é negativo, fornecido que $(-3)^* < 0^*$.

A seguir, daremos mais duas propriedades envolvendo cortes racionais.

Proposição 4.5. *Sejam $p, q \in \mathbb{Q}$. Então valem as seguintes equivalências:*

i) $p^* = q^* \Leftrightarrow p = q$;

ii) $p^* < q^* \Leftrightarrow p < q$.

Demonstração. **i)** ($\Rightarrow$) Suponha que $p^* = q^*$. Então se $x \in p^*$, temos que $x < q$ (pois $x \in q^*$). Então, q é uma cota superior para p^*. Assim, $q \notin p^*$. Logo, $p \leq q$. Por outro lado, se $x \in q^*$, temos que $x < p$. Daí, p é cota superior de q^*, Deste modo $p \notin q^*$. Assim $q \leq p$. Portanto, $p = q$.
($\Leftarrow$) Trivial.

ii) ($\Rightarrow$) Como $p^* < q^*$, temos que $\exists x \in q^*$, tal que $x \notin p^*$, ou seja, $x < q$ e $p \leq x$. Daí $p \leq x < q$. Logo, $p < q$.
($\Leftarrow$) Se $p < q$, então $p \in q^*$. E por definição temos que $p \notin p^*$. Portanto $p^* < q^*$.

□

O resultado abaixo mostra como caracterizar as relações $<$ e $\leq$, por utilizar a inclusão entre conjuntos.

Proposição 4.6. Sejam $\alpha, \beta \in \mathbb{R}$. Então são válidas as equivalências abaixo:

i) $\alpha < \beta \Leftrightarrow \alpha \subset \beta$ e $\alpha \neq \beta$;

ii) $\alpha \leq \beta \Leftrightarrow \alpha \subset \beta$.

Demonstração. **i)** ($\Rightarrow$) Se $\alpha < \beta$, então $\exists x_0 \in \beta \backslash \alpha$ (pois $\beta \backslash \alpha \neq \varnothing$). Logo, $x_0 \in \beta$ e $x_0 \notin \alpha$ (isto já garante que $\alpha \neq \beta$). Agora, seja $r \in \alpha$, então r não pode ser maior do que x_0; caso contrário, $x_0 < r$, teríamos, pela definição de corte, $x_0 \in \alpha$. Isto é uma contradição! ($x_0 \notin \alpha$). Portanto, $r \leq x_0$. Como $x_0 \in \beta$ e β é um corte, então $r \in \beta$. Dessa forma, $\alpha \subset \beta$.

($\Leftarrow$) Suponha que $\alpha \subset \beta$ e $\alpha \neq \beta$. Então, $\exists x_0 \in \beta$ tal que $x_0 \notin \alpha$. Logo, $x_0 \in \beta \backslash \alpha$. Portanto, $\alpha < \beta$.

ii) ($\Rightarrow$) Se $\alpha < \beta$, então, pelo item anterior, tem-se que $\alpha \subset \beta$. Se $\alpha = \beta$, então, trivialmente, temos que $\alpha \subset \beta$.

($\Leftarrow$) Se $\alpha \subset \beta$ e $\alpha \neq \beta$, então, pelo item anterior, concluímos que $\alpha < \beta$. Se $\alpha = \beta$, então $\alpha \leq \beta$.

□

O teorema a seguir mostra que os elementos de C satisfazem a tricotomia.

Teorema 4.2 (Tricotomia)**.** *Sejam $\alpha, \beta \in \mathbb{R}$. Então, ou $\alpha = \beta$ ou $\alpha < \beta$ ou $\alpha > \beta$.*

Demonstração. É claro que $\alpha = \beta$ exclui as outras duas possibilidades (pela definição de igualdade de conjuntos). De modo análogo, as outras possibilidades $\alpha < \beta$ ou $\alpha > \beta$ claramente excluem $\alpha = \beta$. Mostremos que as desigualdades se excluem mutuamente. Suponhamos o contrário, ou seja, que $\alpha < \beta$ e $\alpha > \beta$ ocorram simultaneamente. Então, existem $r \in \beta \backslash \alpha$ e $s \in \alpha \backslash \beta$. Como $r \in \beta$ e $s \notin \beta$ encontramos $r < s$. Caso contrário, $s \leq r$, teríamos $s \in \beta$, pela definição de corte. Analogamente, temos $s < r$ (usando o fato que $s \in \alpha$ e $r \notin \alpha$), contradizendo a lei da tricotomia em $\mathbb{Q}$. Concluímos que no máximo uma das três possibilidades ocorre. Para mostrar que uma delas necessariamente ocorre, temos que $\alpha = \beta$ ou $\alpha \neq \beta$. Se $\alpha = \beta$, não há nada a provar. Suponhamos $\alpha \neq \beta$. Então $\alpha \backslash \beta \neq \emptyset$ ou $\beta \backslash \alpha \neq \emptyset$. No primeiro caso, $\beta < \alpha$ e, no segundo caso, chegamos a $\alpha < \beta$. □

agora estamos prontos para estabelecermos uma relação de ordem em $\mathbb{R}$.

Teorema 4.3. *A relação $\leq$ é uma relação de ordem em $\mathbb{R}$.*

Demonstração. **i)** [Reflexiva]: Seja $\alpha \in \mathbb{R}$. Claramente $\alpha \subset \alpha$, daí $\alpha \leq \alpha$;

ii) [Antissimetria]: Sejam $\alpha, \beta \in \mathbb{R}$, com $\alpha \leq \beta$ e $\beta \leq \alpha$, pela tricotomia em $\mathbb{R}$, temos que $\alpha = \beta$;

iii) [Transitividade]: Sejam $\alpha, \beta, \gamma \in \mathbb{R}$, com $\alpha \leq \beta$ e $\beta \leq \gamma$. Da Proposição 4.6, tiramos que $\alpha \subset \beta$ e $\beta \subset \gamma$ e, das propriedades de conjuntos, concluímos que $\alpha \subset \gamma$, ou seja, $\alpha \leq \gamma$.

Portanto, $\leq$ é uma relação de ordem em $\mathbb{R}$. □

4.1.3 Operações Elementares Envolvendo Cortes

Nesta subseção, vamos estabelecer a definição das operações de adição e multiplicação em $\mathbb{R}$. Além disso, mostraremos as propriedades mais elementares provenientes destas operações.

Definição 4.6. Sejam $\alpha, \beta \in \mathbb{R}$. Denotamos por $\alpha + \beta$, e chamamos adição entre α e β, o seguinte conjunto:

$$\alpha + \beta := \{r + s \in \mathbb{Q} / r \in \alpha, s \in \beta\}.$$

A proposição a seguir nos mostra que a adição entre dois cortes é novamente um corte. Portanto, a adição é uma aplicação da forma $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

Proposição 4.7. *Sejam $\alpha, \beta \in \mathbb{R}$. Então $\alpha + \beta \in \mathbb{R}$.*

Demonstração. Mostraremos que $\alpha + \beta$ satisfaz as três condições da definição de corte.

i) Como $\alpha, \beta \in \mathbb{R}$, então $\alpha + \beta \neq \emptyset$ (desde que $\alpha \neq \emptyset$ e $\beta \neq \emptyset$). Além disso, existem $t \in \mathbb{Q} \backslash \alpha$ e $u \in \mathbb{Q} \backslash \beta$ (pois $\alpha \neq \mathbb{Q}$ e $\beta \neq \mathbb{Q}$). Consequentemente, t e s são cotas superiores de α e β, respectivamente. Daí,

$$t > r, \forall r \in \alpha \text{ e } u > s, \forall s \in \beta.$$

Por conseguinte,

$$t + u > r + s, \forall r \in \alpha, \forall s \in \beta,$$

ou seja, $t + u \notin \alpha + \beta$. Logo $\alpha + \beta \neq \mathbb{Q}$;

ii) Sejam $r \in \alpha + \beta$ e $s < r$ ($s \in \mathbb{Q}$). Mostremos que $s \in \alpha + \beta$. Lembre que $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Então, $s < p + q$. Podemos escrever $s = p + q'$ com $q' < q$ ($q' = s - p \in \mathbb{Q}$). Note que $q' \in \beta$ (pela definição de corte). Logo, $s = p + q'$, com $p \in \alpha$ e $q' \in \beta$, ou seja, $s \in \alpha + \beta$;

iii) Vamos mostrar que em $\alpha + \beta$ não há elemento máximo, ou seja, dado $r \in \alpha + \beta$, existe $s \in \alpha + \beta$ com $s > r$. Com efeito, seja $r = p + q$, com $p \in \alpha$ e $q \in \beta$. Sabemos que existe $p' \in \alpha$ com $p' > p$ (ver item **iii)** da Definição 4.1). Portanto, o racional $s = p' + q \in \alpha + \beta$ é maior do que r.

□

Vejamos, abaixo, que a adição de cortes racionais resulta em outro corte racional.

Proposição 4.8. *Se $p, q \in \mathbb{Q}$, então $p^* + q^* = (p + q)^*$.*

Demonstração. Primeiramente, vamos provar que $p^* + q^* \subset (p+q)^*$. Seja $x \in p^* + q^*$, então $x = a + b$ com $a \in p^*$ e $b \in q^*$. Daí, $a < p$ e $b < q$. Assim,

$$x = a + b < p + q,$$

isto é, $x \in (p+q)^*$. Reciprocamente, vamos mostrar que $(p+q)^* \subset p^* + q^*$. Seja $y \in (p+q)^*$, então $y < p + q$. Seja $y = c + d$, com

$$c = \frac{y}{2} + \frac{p}{2} - \frac{q}{2} \text{ e } d = \frac{y}{2} + \frac{q}{2} - \frac{p}{2}.$$

É fácil ver que $c < p$, pois

$$c = \frac{y}{2} + \frac{p}{2} - \frac{q}{2} < p \Leftrightarrow y < p + q$$

e também $d < q$, já que

$$d = \frac{y}{2} + \frac{q}{2} - \frac{p}{2} < q \Leftrightarrow y < p + q,$$

isto é, $c \in p^*$ e $d \in q^*$. Portanto, $y = c + d \in p^* + q^*$. Por fim, $p^* + q^* = (p+q)^*$. □

o teorema abaixo no mostra que os elementos de $\mathbb{R}$ satisfazem a propriedade comutativa.

Teorema 4.4 (Comutatividade)**.** *Sejam $\alpha, \beta \in \mathbb{R}$. Então, $\alpha + \beta = \beta + \alpha$.*

Demonstração. É fácil checar que

$$\alpha + \beta = \{r + s \in \mathbb{Q} / r \in \alpha, s \in \beta\} = \{s + r \in \mathbb{Q} / s \in \beta, r \in \alpha\} = \beta + \alpha.$$

Isto completa a prova em questão. □

Agora, provemos a associatividade em $\mathbb{R}$.

Teorema 4.5 (Associatividade)**.** *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Então, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.*

Demonstração. Note que

$$\begin{aligned}
(\alpha + \beta) + \gamma &= \{r + s \in \mathbb{Q} / r \in \alpha + \beta, s \in \gamma\} \\
&= \{(a + b) + s \in \mathbb{Q} / a \in \alpha, b \in \beta, s \in \gamma\} \\
&= \{a + (b + s) \in \mathbb{Q} / a \in \alpha, b + s \in \beta + \gamma\} \\
&= \{a + c \in \mathbb{Q} / a \in \alpha, c \in \beta + \gamma\} \\
&= \alpha + (\beta + \gamma).
\end{aligned}$$

□

O elemento neutro da adição em $\mathbb{R}$ é dado por 0^*.

Teorema 4.6 (Elemento Neutro)**.** *Seja $\alpha \in \mathbb{R}$. Então, $\alpha + 0^* = \alpha$. Além disso, 0^* é o único elemento de $\mathbb{R}$ que satisfaz esta igualdade.*

Demonstração. Desejamos verificar as duas inclusões: $\alpha + 0^* \subset \alpha$ e $\alpha \subset \alpha + 0^*$.

($\alpha + 0^* \subset \alpha$): Seja $r \in \alpha + 0^*$. Então $r = p + q$, com $p \in \alpha$ e $q \in 0^*$. Assim, $q < 0$. Dessa forma, $r < p$ e, portanto, a partir do item **ii**) da Definição 4.1, temos que $r \in \alpha$.

($\alpha \subset \alpha + 0^*$): Seja agora $r \in \alpha$. Sabendo que existe $s \in \alpha$ com $s > r$ (ver item **iii**) da Definição 4.1), podemos expressar r como $r = s + (r - s)$, onde $r - s \in 0^*$. Por fim, $r \in \alpha + 0^*$. Deste modo, $\alpha \subset \alpha + 0^*$.

Suponha que $\gamma \in \mathbb{R}$ é tal que $\alpha + \gamma = \alpha$ para todo $\alpha \in \mathbb{R}$. Então,

$$\gamma = \gamma + 0^* = 0^* + \gamma = 0^*.$$

Isto conclui a prova do teorema em questão. □

O lema a seguir será útil na busca por um simétrico para cada elemento de $\mathbb{R}$.

Lema 4.1. *Sejam $\alpha \in \mathbb{R}$ e $r \in \mathbb{Q}_+^*$. Então, existem $p, q \in \mathbb{Q}$, tais que $p \in \alpha$, $q \notin \alpha$, q não é cota superior mínima de α e $q - p = r$.*

Demonstração. Como α é um corte $\alpha \neq \varnothing$. Logo, $\exists s \in \alpha$. Assim sendo, seja $Y = \{n \in \mathbb{N} / s_n \in \alpha\}$, onde

$$s_n = s + nr, \forall n \in \mathbb{N}.$$

É fácil ver que

$$s_0 = s + 0 \cdot r = s \in \alpha.$$

Logo, $0 \in Y$. Isto nos diz que $Y \neq \varnothing$. Por outro lado, como α é um corte, então $\exists q_0 \in \mathbb{Q} \backslash \alpha$. Dessa forma, q_0 é uma cota superior de α. Isto nos diz que $x < q_0$, para todo $x \in \alpha$. Consequentemente, $s_n < q_0$, para todo $n \in Y$, ou equivalentemente,

$$n < \frac{q_0 - s}{r}, \forall n \in Y,$$

onde $s < q_0$ ($s \in \alpha$) e $r \in \mathbb{Q}_+^*$. Com isso, podemos concluir que Y é finito. Dessa forma, existe $m \in Y$ tal que $m + 1 \notin Y$. Isto nos informa que

$$s + mr \in \alpha \text{ e } s + (m+1)r \notin \alpha.$$

Deste modo, temos que $s + (m+1)r$ é cota superior de α.

Suponhamos que $s + (m+1)r$ é uma cota superior mínima de α, então assuma que

$$p = s + (m + \frac{1}{2})r \text{ e } q = s + (m+1)r + \frac{r}{2}.$$

É fácil ver que $q - p = r$. Além disso, $p \in \alpha$; caso contrário, p seria uma cota superior de α ($p \in \mathbb{Q}\backslash\alpha$) e $p < s + (m+1)r$ ($r \in \mathbb{Q}_+^*$). Isto contradiz a minimalidade de $s + (m+1)r$. Por fim, q é uma cota superior, a qual não é mínima, de α (já que $q > s + (m+1)r$). Logo, $q \in \mathbb{Q}\backslash\alpha$.

Agora considere que $s + (m+1)r$ não é cota superior mínima de α, então assuma que

$$p = s + mr \text{ e } q = s + (m+1)r.$$

Vimos acima que $p \in \alpha$ e que $q \in \mathbb{Q}\backslash\alpha$ não é uma cota superior mínima de α. Além disso, $q - p = r$. □

O teorema abaixo nos mostra como representar o simétrico, com relação a adição, para cada elemento de $\mathbb{R}$.

Teorema 4.7 (Simétrico)**.** *Seja $\alpha \in \mathbb{R}$. Então, existe um único $\beta \in \mathbb{R}$ tal que $\alpha + \beta = 0^*$.*

Demonstração. De início, mostremos a unicidade de tal β. Suponhamos que $\alpha + \beta_1 = \alpha + \beta_2 = 0^*$. Dessa forma, obtemos

$$\beta_2 = \beta_2 + 0^* = \beta_2 + (\alpha + \beta_1) = (\beta_2 + \alpha) + \beta_1 = 0^* + \beta_1 = \beta_1.$$

Provemos agora a existência de um corte β que satisfaça $\alpha + \beta = 0^*$. Assim sendo, seja

$$\beta = \{p \in \mathbb{Q} / -p \notin \alpha \text{ não é cota superior mínima de } \alpha\}.$$

Vamos provar que β é um corte.

i) Para mostrar que $\beta \neq \emptyset$, consideremos dois casos:

- α não possui cota superior mínima:

  Como α é um corte, então $\alpha \neq \mathbb{Q}$ e, portanto, $\exists q \in \mathbb{Q}$ tal que $q \notin \alpha$. Assim, basta tomar $p = -q \in \mathbb{Q}$. Consequentemente, $-p = q \notin \alpha$. Logo, $p \in \beta$ (α não possui cota superior

mínima) e, assim, $\beta \neq \emptyset$.

• α possui cota superior mínima m:

Como m é cota superior mínima de α, então $m \notin \alpha$ (caso contrário, m seria elemento máximo de α, contrariando o item **iii**) da Definição 4.1). Com isso, $m+1 \notin \alpha$. Seja $p = -m-1 \in \mathbb{Q}$. Então, $-p = m+1 \notin \alpha$; além disso, $-p = m+1 \neq m$. Portanto, $p \in \beta$ e consequentemente, $\beta \neq \emptyset$.

Para mostrar que $\beta \neq \mathbb{Q}$, consideremos os mesmos dois casos:

• α não possui cota superior mínima:

Como α é um corte, então $\alpha \neq \emptyset$, daí $\exists r \in \alpha$ $(r \in \mathbb{Q})$. Tomemos $p = -r \in \mathbb{Q}$. Assim, $-p = r \in \alpha$. Logo, $p \notin \beta$ e $p \in \mathbb{Q}$.

• α possui cota superior mínima m:

Como m é cota superior mínima de α, então $m-1 \in \alpha$ (caso contrário, $m-1$ seria cota superior de α menor do que m). Seja $p = -m+1 \in \mathbb{Q}$, então $-p = m-1 \in \alpha$. Portanto, $p \notin \beta$ e $p \in \mathbb{Q}$.

ii) Sejam $p \in \beta$ e $q \in \mathbb{Q}$ tais que $q < p$. Mostremos que $q \in \beta$. Como $p \in \beta$, então $-p \notin \alpha$ (isto significa que $-p$ é cota superior de α) e $-p$ não é cota superior mínima de α. Como $q < p$, então $-p < -q$. Daí, $-q \notin \alpha$ (pois, $-p \notin \alpha$). Além disso, concluímos que $-q$ é cota superior de α. Temos também que $-q$ não é cota superior mínima de α (pois do contrário, $-q \leq -p$). Como $q \in \mathbb{Q}$, $-q \notin \alpha$ e $-q$ não é cota superior mínima de α, concluímos que $q \in \beta$.

iii) Seja $p \in \beta$, queremos mostrar que $\exists q \in \beta$ tal que $p < q$. Dividiremos a prova desta afirmação em dois casos:

• α não possui cota superior mínima:

Como $-p \notin \alpha$ e $-p$ não é cota superior mínima de α, então existe uma cota superior r de α $(r \notin \alpha)$, tal que $r < -p$. Assim, $q = -r \in \beta$ (desde que α não possui cota superior mínima) e $p < -r = q$. Logo, β não possui elemento máximo.

• α possui cota superior mínima m:

Seja $q = \frac{-m+p}{2} \in \mathbb{Q}$. Como $p \in \beta$ temos que $-p$ é uma cota superior de α (pois $-p \notin \alpha$), mas não a mínima de α; portanto, $m < -p$. Daí, $p < -m$. Sendo assim,

$$q = \frac{-m+p}{2} = -\frac{m}{2} + \frac{p}{2} > \frac{p}{2} + \frac{p}{2} = p.$$

Por outro lado,

$$-q = \frac{m-p}{2} = \frac{m}{2} - \frac{p}{2} > \frac{m}{2} + \frac{m}{2} = m.$$

Então, $-q \notin \alpha$ (caso contrário, $-q \leq m$) . Finalmente, como $q \in \mathbb{Q}$, $-q \notin \alpha$ e $-q$ não é cota superior mínima de α ($-q \neq m$), temos que $q \in \beta$ e $p < q$. Logo, β não possui elemento máximo.

Portanto, β é um corte.

Para finalizar, basta mostra que $\alpha + \beta = 0^*$. Para isso, mostremos que $\alpha + \beta \subset 0^*$ e $0^* \subset \alpha + \beta$.

Seja $x \in \alpha + \beta$, com $x = a + b$, $a \in \alpha$ e $b \in \beta$ (lembre que $b \in \beta$ significa $-b \notin \alpha$ não é cota superior mínima de α). Como $a \in \alpha$ e $-b \notin \alpha$, temos que $a < -b$ (caso contrário, $-b \leq a$ implicaria $-b \in \alpha$). Daí, $x = a + b < 0$. Logo, concluímos que $x \in 0^*$.

Reciprocamente, seja $p \in 0^*$. Por definição, $p < 0$ ($-p > 0$). Aplicando o Lema 4.1, existem $r \in \alpha$ e $r' \notin \alpha$, com r' não sendo cota superior mínima de α, tais que $r' - r = -p$. Segue que $p = r + (-r')$, com $r \in \alpha$ e $-r' \in \beta$. Portanto, $p \in \alpha + \beta$. Isto nos informa que $0^* \subset \alpha + \beta$.

Por fim, $\alpha + \beta = 0^*$. □

Definição 4.7. Denotaremos β, encontrado no Teorema 4.7, por $-\alpha$ e o chamaremos simétrico de α. Além disso, $-\alpha$ é dado por

$$-\alpha = \{p \in \mathbb{Q} / -p \notin \alpha \text{ não é cota superior mínima de } \alpha\}.$$

Com a definição de simétrico em mãos podemos estabelecer quem é o simétrico de um corte racional em $\mathbb{R}$.

Proposição 4.9. *Seja $q \in \mathbb{Q}$. Então, $-q^* = (-q)^*$.*

Demonstração. Seja $q \in \mathbb{Q}$. Então, pela Proposição 4.8, chega-se a

$$q^* + (-q)^* = [q + (-q)]^* = 0^*.$$

Como o simétrico é único, então $-q^* = (-q)^*$. □

Através da existência e unicidade do elemento simétrico para cada elemento de $\mathbb{R}$, podemos definir a operação de subtração em $\mathbb{R}$.

Definição 4.8. Sejam $\alpha, \beta \in \mathbb{R}$. Definimos a subtração em $\mathbb{R}$ por

$$\alpha - \beta = \alpha + (-\beta).$$

Exemplo 4.9. É fácil checar que

$$1^* - 2^* = 1^* + (-2^*) = 1^* + (-2)^* = [1 + (-2)]^* = (-1)^*.$$

Proposição 4.10. *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Então, são válidas as seguintes afirmações:*

i) $-(-\alpha) = \alpha$*;*

ii) $-\alpha + \beta = \beta - \alpha$*;*

iii) $\alpha - (-\beta) = \alpha + \beta$*;*

iv) $-\alpha - \beta = -(\alpha + \beta)$*;*

v) $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$.

Demonstração. **i)** Note que

$$\alpha + (-\alpha) = -\alpha + \alpha = 0^*.$$

Portanto, $-(-\alpha) = \alpha$;

ii) Também podemos escrever

$$\beta - \alpha = \beta + (-\alpha) = -\alpha + \beta;$$

iii) Por **i**), segue que

$$\alpha - (-\beta) = \alpha + [-(-\beta)] = \alpha + \beta;$$

iv) Pela unicidade do simétrico, temos que

$$(-\alpha - \beta) + (\alpha + \beta) = (-\alpha + \alpha) + (-\beta + \beta) = 0^*$$

implica que $-\alpha - \beta = -(\alpha + \beta)$;

v) Por fim, por **iv**), chegamos a

$$\alpha - (\beta + \gamma) = \alpha + [-(\beta + \gamma)] = \alpha - \beta - \gamma.$$

□

Teorema 4.8. *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Então,*

$$\alpha \leq \beta \Leftrightarrow \alpha + \gamma \leq \beta + \gamma.$$

Demonstração. ($\Rightarrow$) Temos, pela Proposição 4.6, que

$$\alpha + \gamma \leq \beta + \gamma \Leftrightarrow \alpha + \gamma \subset \beta + \gamma.$$

Assim sendo, seja $t \in \alpha + \gamma$, ou seja, $t = r + s$ com $r \in \alpha$ e $s \in \gamma$. Como $\alpha \subset \beta$ ($\Leftrightarrow \alpha \leq \beta$, pela Proposição 4.6), então $r \in \beta$. Consequentemente, $t = r + s \in \beta + \gamma$, isto é, $\alpha + \gamma \subset \beta + \gamma$. Portanto $\alpha + \gamma \leq \beta + \gamma$.

($\Leftarrow$) Reciprocamente, suponha que $\alpha + \gamma \leq \beta + \gamma$. Pelo que foi feito acima, concluímos que

$$(\alpha + \gamma) + (-\gamma) \leq (\beta + \gamma) + (-\gamma),$$

ou equvalentemente, por associatividade, temos que

$$\alpha + [\gamma + (-\gamma)] \leq \beta + [\gamma + (-\gamma)].$$

Portanto, chegamos a

$$\alpha + 0^* \leq \beta + 0^*.$$

Por fim, podemos escrever $\alpha \leq \beta$. Deste modo, o teorema em questão segue.

□

Proposição 4.11. Seja $\alpha \in \mathbb{R}$. Então, $\alpha < 0^* \Leftrightarrow -\alpha > 0^*$.

Demonstração. ($\Rightarrow$) Como $\alpha < 0^*$, então, por definição, $\exists q \in 0^*$ tal que $q \notin \alpha$. Vamos admitir, sem perda de generalidade, que q não é cota superior mínima de α. Como $q \in 0^*$, então $q < 0$. Denote $-r = q$, o que nos fornece $r > 0$. Assim, vemos que $r \in -\alpha$ já que $-r = q \notin \alpha$ não é cota superior mínima de α, e que $r \notin 0^*$. O que nos garante que $-\alpha > 0^*$.

($\Leftarrow$) Suponha que $-\alpha > 0^*$. Então, existe $p \in -\alpha$ e $p \notin 0^*$. Isto nos diz que $-p \notin \alpha$ (pois $-p$ é cota superior de α), $-p$ não é cota superior mínima de α (ver definição de simétrico) e $p \geq 0$. Como $-p$ não é uma cota superior mínima de α, então existe q cota superior de α ($q \notin \alpha$) tal que $q < -p$. Seja $r = 2^{-1}[q + (-p)] \in \mathbb{Q}$, então $q < r < -p$. Como α é um corte, então $r \notin \alpha$ (caso contrário, $q \in \alpha$, um absurdo). Além disso, como $p \geq 0$, temos que $r < -p \leq 0$. Portanto, $r < 0$. Isto nos diz que $r \notin \alpha$ e $r \in 0^*$. Por fim, $r \in 0^* \backslash \alpha$. Consequentemente, $\alpha < 0^*$. □

A partir de agora, nossa meta é definir a multiplicação entre dois cortes. Permita-nos começar estabelecendo o que significa multiplicar dois cortes não negativos.

Definição 4.9. Sejam $\alpha, \beta \in \mathbb{R}$ tais que $\alpha \geq 0^*$, $\beta \geq 0^*$. Definimos a multiplicação $\alpha \cdot \beta$ (ou $\alpha\beta$) como sendo o conjunto

$$\alpha \cdot \beta = \mathbb{Q}^*_- \cup \{r \in \mathbb{Q} / r = pq, p \in \alpha, q \in \beta, p \geq 0, q \geq 0\}.$$

A proposição a seguir prova que a multiplicação entre dois cortes não negativos é novamente um corte não negativo.

Proposição 4.12. *Sejam $\alpha, \beta \in \mathbb{R}$ tais que $\alpha, \beta \geq 0^*$. Então, $\alpha\beta$ é um corte e $\alpha\beta \geq 0^*$.*

Demonstração. Mostraremos primeiramente que $\alpha\beta$ é um corte.

i) Como $p = -1 \in \alpha\beta$, logo $\alpha\beta \neq \emptyset$. Por outro lado, temos que $\exists p_0 \in \mathbb{Q}$ tal que $p_0 \notin \alpha$ ($\alpha \neq \mathbb{Q}$) e $\exists q_0 \in \mathbb{Q}$ tal que $q_0 \notin \beta$ ($\beta \neq \mathbb{Q}$). Mostremos que $p_0 q_0 \notin \alpha\beta$. Suponhamos que $p_0 q_0 \in \alpha\beta$, ou seja, $\exists p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$ tais que $p_0 q_0 = pq$. Não podemos ter $p_0 \leq p$ (pois, obteríamos $p_0 \in \alpha$), nem $q_0 \leq q$ (pois, teríamos $q_0 \in \beta$). Dessa forma, $p < p_0$ e $q < q_0$. Daí, $pq < p_0 q_0$. O que é uma contradição, visto que $p_0 q_0 = pq$. Portanto, $p_0 q_0 \notin \alpha\beta$ e assim $\alpha\beta \neq \mathbb{Q}$;

ii) Sejam $r \in \alpha\beta$ e $s < r$ ($s \in \mathbb{Q}$). Precisamos mostrar que $s \in \alpha\beta$. De fato, se $s < 0$, temos que $s \in \mathbb{Q}^*_-$, logo $s \in \alpha\beta$. Suponhamos que $s \geq 0$ e, portanto, $r > 0$. Pelo fato de $r \in \alpha\beta$, então existem $p \in \alpha$ e $q \in \beta$, tais que $r = pq$ com $p \geq 0$, $q \geq 0$. Como $r > 0$, segue que $p > 0$ e $q > 0$. Tomemos $t = \frac{s}{p}$ ($s \geq 0$ e $p > 0 \Rightarrow t \geq 0$). Se $q \leq t$, teríamos $pq \leq pt$, ou seja, $s \geq r$. O que é um absurdo, já que $s < r$ por hipótese. Logo, devemos ter $t < q$. Mas, como $q \in \beta$, então $t \in \beta$ (β é corte). Desse modo, como $s = pt$, com $p \in \alpha$, $t \in \beta$ com $p > 0$ e $t \geq 0$, então $s \in \alpha\beta$.

iii) Mostremos agora que $\alpha\beta$ não possui elemento máximo, isto é, dado $r \in \alpha\beta$, $\exists s \in \alpha\beta$ tal que $r < s$.

De fato, se $r < 0$ basta tomar $s = \frac{r}{3} < 0$ ($s \in \alpha\beta$) em ordem a obter $s > r$.

Suponhamos agora $r \geq 0$. Neste caso, $r = pq$, como $p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$. Sabemos que existem $t \in \alpha$ e $u \in \beta$ tais que $p < t$ e $q < u$ (já que α e β não possuem máximos). Logo, $r = pq < tu$. Tomando $s = tu$, temos $s \in \alpha\beta$ (pois $s = tu$ com $t \in \alpha, u \in \beta, t > 0$ e $u > 0$) e $s > r$. Portanto, $\alpha\beta$ não tem máximo.

Deste modo, $\alpha\beta$ é um corte.

Por fim, vamos provar que $\alpha\beta \geq 0^*$. Com efeito, se $\alpha, \beta > 0^*$, então $\exists p \in \alpha$ e $q \in \beta$ tais que $p, q \notin 0^*$. Assim, $p, q \geq 0$. Logo, $pq \geq 0$. Deste modo, podemos concluir que $pq \in \alpha\beta$. Daí, $pq \in \alpha\beta$ e $pq \notin 0^*$. Isto nos diz que $\alpha\beta > 0^*$. Se $\alpha = 0^*$ ou $\beta = 0^*$, então $\alpha\beta = \mathbb{Q}^*_- = 0^*$. Por fim, $\alpha\beta \geq 0^*$. □

Para definir a multiplicação de cortes com, pleo menos, um dos fatores sendo negativo, trabalharemos com a noção de módulo em $\mathbb{R}$. Mais precisamente, temos a seguinte definição.

Definição 4.10. Dado $\alpha \in \mathbb{R}$ definimos o módulo (ou o valor absoluto) de α, representado por $|\alpha|$, do seguinte modo:

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

Vejamos algumas propriedades básicas envolvendo o módulo de elementos de $\mathbb{R}$.

Proposição 4.13. *Seja $\alpha \in \mathbb{R}$. Então, as seguintes afirmações são válidas:*

1) $|\alpha| \geq 0^*$*;*

2) $|\alpha| = 0^* \Leftrightarrow \alpha = 0^*$*;*

3) $|-\alpha| = |\alpha|$.

Demonstração. **i)** Se $\alpha \geq 0^*$, então $|\alpha| = \alpha \geq 0^*$. Se $\alpha < 0^*$, então, pela Proposição 4.11, temos que $-\alpha > 0^*$. Logo, $|\alpha| = -\alpha > 0^*$;

ii) ($\Rightarrow$) Suponha que $|\alpha| = 0^*$. Assim, se $\alpha > 0^*$, temos que $\alpha = |\alpha| = 0^*$. Isto é uma contradição. Agora, se $\alpha < 0^*$, temos que $-\alpha = |\alpha| = 0^*$. Logo, $\alpha = 0^*$. Novamente uma contradição. Logo, pela tricotomia em $\mathbb{R}$, $\alpha = 0^*$.

($\Leftarrow$) Seja $\alpha = 0^*$, então, por definição de módulo, $|\alpha| = \alpha = 0^*$;

iii) Sabemos, através da Proposição 4.11, que se $\alpha \geq 0^*$, então $-\alpha \leq 0^*$. Logo,

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

Por outro lado, se $\alpha < 0^*$, então $-\alpha > 0^*$. Assim,

$$|\alpha| = -\alpha = |-\alpha|.$$

Isto completa a prova da proposição em questão. □

Estamos prontos para definir as multiplicações que restam entre dois cortes.

Definição 4.11. Se $\alpha, \beta \in \mathbb{R}$, definimos:

$$\alpha\beta = \begin{cases} -|\alpha||\beta|, & \text{se } \alpha \leq 0^*, \beta \geq 0^* \text{ ou } \alpha \geq 0^*, \beta \leq 0^*; \\ |\alpha||\beta|, & \text{se } \alpha \leq 0^*, \beta \leq 0^*. \end{cases}$$

A proposição abaixo, mostra como devemos proceder com as usuais regras de sinal envolvendo a multiplicação em $\mathbb{R}$.

Proposição 4.14. *Sejam $\alpha, \beta \in \mathbb{R}$. Então,*

$$(-\alpha)\beta = \alpha(-\beta) = -\alpha\beta, \text{ e } (-\alpha)(-\beta) = \alpha\beta.$$

Demonstração. Vamos separar a prova em quatro casos.

- Caso 1: $\alpha \geq 0^*$ e $\beta \geq 0^*$:

Neste caso, temos que $-\alpha \leq 0^*$ e $-\beta \leq 0^*$. Daí,

$$(-\alpha)\beta := -|-\alpha||\beta| = -|\alpha||\beta| = -\alpha\beta, \tag{4.1}$$

$$\alpha(-\beta) := -|\alpha||-\beta| = -|\alpha||\beta| = -\alpha\beta \tag{4.2}$$

e também

$$(-\alpha)(-\beta) := |-\alpha||-\beta| = |\alpha||\beta| = \alpha\beta. \tag{4.3}$$

- Caso 2: $\alpha \leq 0^*$ e $\beta \leq 0^*$:

Aqui $-\alpha \geq 0^*$ e $-\beta \geq 0^*$. Por (4.3), obtemos

$$(-\alpha)\beta := -|-\alpha||\beta| = -[(-\alpha)(-\beta)] = -\{[-(-\alpha)][-(-\beta)]\} = -\alpha\beta,$$
$$\alpha(-\beta) := -|\alpha||-\beta| = -[(-\alpha)(-\beta)] = -\{[-(-\alpha)][-(-\beta)]\} = -\alpha\beta$$

e também

$$(-\alpha)(-\beta) = [-(-\alpha)][-(-\beta)] = \alpha\beta.$$

- Caso 3: $\alpha \geq 0^*$ e $\beta \leq 0^*$:

Neste caso, $-\alpha \leq 0^*$ e $-\beta \geq 0^*$. Com isso, por (4.2) e (4.3), encontramos

$$\begin{aligned}(-\alpha)\beta &:= |-\alpha||\beta| = |\alpha||\beta| = \alpha(-\beta)\\ &= -\{-[\alpha(-\beta)]\} = -\{\alpha[-(-\beta)]\}\\ &= -\alpha\beta,\end{aligned}$$

$$\alpha(-\beta) = (-\alpha)[-(-\beta)] = (-\alpha)\beta = -\alpha\beta$$

e também

$$\begin{aligned}(-\alpha)(-\beta) &:= -|-\alpha|-\beta| = -|\alpha|-\beta|\\ &= -[\alpha(-\beta)] = -[-\alpha\beta]\\ &= \alpha\beta.\end{aligned}$$

• Caso 4: $\alpha \leq 0^*$ e $\beta \geq 0^*$:

Aqui $-\alpha \geq 0^*$ e $-\beta \leq 0^*$. Logo, por (4.1), encontramos

$$(-\alpha)\beta = -\{-[(-\alpha)\beta]\} = -\{[-(-\alpha)]\beta\} = -\alpha\beta,$$

$$\alpha(-\beta) := |\alpha|-\beta| = |\alpha||\beta| = (-\alpha)\beta = -\alpha\beta$$

e também

$$\begin{aligned}(-\alpha)(-\beta) &:= -|-\alpha|-\beta| = -[|-\alpha||\beta|]\\ &= -[(-\alpha)\beta] = -[-\alpha\beta]\\ &= \alpha\beta.\end{aligned}$$

□

O teorema abaixo, demonstra que não importa a ordem que realizamos a multiplicação entre dois elementos de $\mathbb{R}$.

Teorema 4.9 (Comutatividade)**.** *Sejam $\alpha, \beta \in \mathbb{R}$. Então, $\alpha\beta = \beta\alpha$.*

Demonstração. Vamos dividir a prova deste resultado em quatro casos.

Caso 1: Assuma $\alpha, \beta \geq 0^*$:

Seja $r \in \alpha\beta$. Se $r < 0$, então $r \in \beta\alpha$ (ver definição de multiplicação). Suponhamos $r \geq 0$. Então, $r = pq$, $p \in \alpha$, $q \in \beta$, $p \geq 0$ e $q \geq 0$. Portanto, $r = pq = qp$, $q \in \beta$, $p \in \alpha$, $q \geq 0$ e $p \geq 0$, isto

é, $r \in \beta\alpha$. Logo $\alpha\beta \subset \beta\alpha$. Analogamente $r \in \beta\alpha \Rightarrow r \in \alpha\beta$, ou seja, $\beta\alpha \subset \alpha\beta$. Isto nos garante que $\alpha\beta = \beta\alpha$.

Caso 2: Considere que $\alpha \leq 0^*$ e $\beta \geq 0^*$:

Logo,

$$\alpha\beta = -|\alpha||\beta| = -|\beta||\alpha| = \beta\alpha.$$

Caso 3: Suponha que $\alpha \leq 0^*$ e $\beta \leq 0^*$:

É fácil ver que

$$\alpha\beta = |\alpha||\beta| = |\beta||\alpha| = \beta\alpha.$$

Caso 4: Assuma $\alpha \geq 0^*$ e $\beta \leq 0^*$:

Dessa forma,

$$\alpha\beta = -|\alpha||\beta| = -|\beta||\alpha| = \beta\alpha.$$

□

A seguir, provaremos que a associatividade, com relação à multiplicação, é válida em $\mathbb{R}$.

Teorema 4.10 (Associatividade)**.** *Sejam* $\alpha, \beta, \gamma \in \mathbb{R}$. *Então,* $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

Demonstração. Dividiremos, novamente, a prova deste teorema em oito casos:

Caso 1: Assuma $\alpha, \beta, \gamma \geq 0^*$:

Esta propriedade tem demonstração análoga a anterior, se dando imediatamente pela associatividade dos racionais, ou seja,

$$\begin{aligned}
x \in (\alpha\beta)\gamma &\Rightarrow x \in \mathbb{Q}^*_- \text{ ou } x = pq, p \in \alpha\beta, q \in \gamma, p \geq 0, q \geq 0 \\
&\Rightarrow x \in \mathbb{Q}^*_- \text{ ou } x = (rs)q, r \in \alpha, s \in \beta, q \in \gamma, r, s, q \geq 0 \\
&\Rightarrow x \in \mathbb{Q}^*_- \text{ ou } x = r(sq), r \in \alpha, s \in \beta, q \in \gamma, r, s, q \geq 0 \\
&\Rightarrow x \in \mathbb{Q}^*_- \text{ ou } x = rt, r \in \alpha, t \in \beta\gamma, r, t \geq 0 \\
&\Rightarrow x \in \alpha(\beta\gamma).
\end{aligned}$$

Reciprocamente,

$$\begin{aligned} y \in \alpha(\beta\gamma) &\Rightarrow y \in \mathbb{Q}^*_- \text{ ou } y = pq, p \in \alpha, q \in \beta\gamma, p, q \geq 0 \\ &\Rightarrow y \in \mathbb{Q}^*_- \text{ ou } y = p(rs), p \in \alpha, r \in \beta, s \in \gamma, p, r, s \geq 0 \\ &\Rightarrow y \in \mathbb{Q}^*_- \text{ ou } y = (pr)s, p \in \alpha, r \in \beta, s \in \gamma, p, r, s \geq 0 \\ &\Rightarrow y \in \mathbb{Q}^*_- \text{ ou } y = ts, t \in \alpha\beta, s \in \gamma, t, s \geq 0 \\ &\Rightarrow y \in (\alpha\beta)\gamma. \end{aligned}$$

Logo, $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

Caso 2: Considere $\alpha \leq 0^*, \beta \leq 0^*$ e $\gamma \geq 0^*$:

Dessa forma, chegamos a

$$(\alpha\beta)\gamma = (|\alpha||\beta|)\gamma = |\alpha|(|\beta|\gamma) = (-\alpha)[(-\beta)\gamma] = (-\alpha)[-(\beta\gamma)] = \alpha(\beta\gamma).$$

Caso 3 : $\alpha \geq 0^*, \beta \leq 0^*$ e $\gamma \geq 0^*$:

É fácil checar que

$$\begin{aligned} (\alpha\beta)\gamma := [-|\alpha||\beta|]\gamma &= -(|\alpha||\beta|)\gamma \\ &= -|\alpha|(|\beta|\gamma) = -\alpha[(-\beta)\gamma] \\ &= -\alpha[-\beta\gamma] = -[-\alpha(\beta\gamma)] \\ &= \alpha(\beta\gamma). \end{aligned}$$

Caso 4: Assuma $\alpha \geq 0^*, \beta \leq 0^*$ e $\gamma \leq 0^*$:

Através do Caso 1, encontramos

$$\begin{aligned} (\alpha\beta)\gamma := [-|\alpha||\beta|]\gamma &= (|\alpha||\beta|)(-\gamma) \\ &= |\alpha|[|\beta|(-\gamma)] = \alpha[(-\beta)(-\gamma)] \\ &= \alpha(\beta\gamma). \end{aligned}$$

Caso 5: Considere $\alpha \leq 0^*, \beta \leq 0^*$ e $\gamma \leq 0^*$:

Veja que

$$\begin{aligned}(\alpha\beta)\gamma &:= (|\alpha||\beta|)\gamma = (|\alpha||\beta|)[-(-\gamma)] \\ &= -(|\alpha||\beta|)(-\gamma) = -|\alpha|[|\beta|(-\gamma)] \\ &= -(-\alpha)[(-\beta)(-\gamma)] = [-(-\alpha)][(-\beta)(-\gamma)] \\ &= \alpha(\beta\gamma).\end{aligned}$$

Caso 6: Suponha $\alpha, \beta \geq 0^*$ e $\gamma \leq 0^*$:

Neste caso, temos que

$$\begin{aligned}(\alpha\beta)\gamma &:= (\alpha\beta)[-(-\gamma)] = -(\alpha\beta)(-\gamma) \\ &= -\alpha[\beta(-\gamma)] = (-\alpha)(-\beta\gamma) \\ &= \alpha(\beta\gamma).\end{aligned}$$

Caso 7: Assuma $\alpha \leq 0^*, \beta \geq 0^*$ e $\gamma \leq 0^*$:

Note que

$$\begin{aligned}(\alpha\beta)\gamma &:= -(|\alpha||\beta|)\gamma = -(|\alpha||\beta|)[-(-\gamma)] \\ &= [|\alpha||\beta|](-\gamma) = |\alpha|[|\beta|(-\gamma)] \\ &= -\alpha[\beta(-\gamma)] = -\alpha[-\beta\gamma] \\ &= \alpha(\beta\gamma).\end{aligned}$$

Caso 8: Considere que $\alpha \leq 0^*$, $\beta \geq 0^*$ e $\gamma \geq 0^*$:

Assim sendo, chegamos a

$$\begin{aligned}(\alpha\beta)\gamma &:= -(|\alpha||\beta|)\gamma = -|\alpha|(|\beta|\gamma) \\ &= -(-\alpha)(\beta\gamma) = [-(-\alpha)](\beta\gamma) \\ &= \alpha(\beta\gamma).\end{aligned}$$

□

O resultado abaixo nos apresenta qual é o elemento neutro da multiplicação em $\mathbb{R}$.

Teorema 4.11 (Elemento Neutro)**.** *Seja $\alpha \in \mathbb{R}$. Então, $\alpha \cdot 1^* = \alpha$. Além disso, 1^* é o único elemento de $\mathbb{R}$ que satisfaz esta igualdade.*

Demonstração. Dividiremos a prova deste teorema em dois casos:

Caso 1: Assuma que $\alpha \geq 0^*$:

Seja $r \in \alpha \cdot 1^*$. Suponha primeiramente que $r < 0$. Se $\alpha = 0^*$, então $r \in 0^* = \alpha$. Portanto, $r \in \alpha$. Se $\alpha > 0^*$, então $\exists p \in \alpha$ tal que $p \notin 0^*$. Dessa forma, $r < 0 \leq p$. Logo, $r \in \alpha$ (pois $p \in \alpha$ e α é um corte).

Suponhamos agora que $r \geq 0$. Assim, $r = pq$ com $p \in \alpha$, $q \in 1^*$, $p \geq 0$ e $q \geq 0$. Como $q \in 1^*$, temos que, $q < 1$. Daí, $r = pq \leq p$. Como $p \in \alpha$, $r \leq p$ e α é corte, então $r \in \alpha$. Logo, $\alpha \cdot 1^* \subset \alpha$.

Por outro lado, considere que $r \in \alpha$. Se $r < 0$ então $r \in \alpha \cdot 1^*$, por definição de multiplicação. Suponhamos agora que $r \geq 0$. Tomemos $p \in \alpha$ tal que $0 \leq r < p$ (pois α não tem máximo). Se $q = \frac{r}{p}$ então $0 \leq q < 1$ e portanto $q \in 1^*$. Por outro lado, $r = pq$, $p \in \alpha$, $q \in 1^*$, $p > 0$, $q \geq 0$. Assim sendo, $r \in \alpha \cdot 1^*$. Portanto, $\alpha \subset \alpha \cdot 1^*$. Logo, $\alpha = \alpha \cdot 1^*$.

Caso 2: Considere que $\alpha < 0^*$:

Com isso, podemos concluir que $-\alpha > 0^*$ (ver Proposição 4.11). Dessa forma, concluímos, pelo caso anterior, que

$$\alpha = -(-\alpha) = -[(-\alpha) \cdot 1^*] = [-(-\alpha)] \cdot 1^* = \alpha \cdot 1^*.$$

Portanto, 1^* é o elemento neutro da multiplicação.

Agora, suponhamos que existe $\beta \in \mathbb{R}$ tal que

$$\alpha\beta = \alpha, \forall \alpha \in \mathbb{R}.$$

Assim,

$$1^* = 1^* \cdot \beta = \beta \cdot 1^* = \beta.$$

Isto mostra que 1^* é o único elemento neutro de $\mathbb{R}$. □

Permita-nos, agora, provarmos a distributividade em $\mathbb{R}$.

Teorema 4.12 (Distributividade)**.** *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Então, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.*

Demonstração. Dividiremos esta prova em seis casos:

Caso 1: Assuma que $\alpha, \beta, \gamma \geq 0^*$.

Sabemos que $\beta \geq 0^*$ e $\gamma \geq 0^*$, implicam que

$$\beta + \gamma \geq 0^* + \gamma = \gamma \geq 0^*.$$

Logo, $\beta + \gamma \geq 0^*$. Dessa forma,

$$\alpha(\beta + \gamma) = \mathbb{Q}^*_- \cup \{r \in \mathbb{Q} / r = pq, \text{ com } 0 \leq p \in \alpha \text{ e } 0 \leq q \in \beta + \gamma\}.$$

Como $0 \leq q \in \beta + \gamma$, então $0 \leq q = y + z$, com $y \in \beta$ e $z \in \gamma$. Logo, se $r \in \alpha(\beta + \gamma)$, então $r \in \mathbb{Q}^*_-$ ou $r = p(y + z)$, onde $0 \leq p \in \alpha$ e $0 \leq y + z$ com $y \in \beta$ e $z \in \gamma$. Com isso, $r = py + pz$, com $0 \leq p \in \alpha$, $y \in \beta, z \in \gamma$ e $0 \leq y + z$. Por outro lado, temos que

$$\alpha\beta = \mathbb{Q}^*_- \cup \{r^{'} \in \mathbb{Q} / r^{'} = p^{'}y^{'}, \text{ com } 0 \leq p^{'} \in \alpha \text{ e } 0 \leq y^{'} \in \beta\} \ ,$$

$$\alpha\gamma = \mathbb{Q}^*_- \cup \{r^{''} \in \mathbb{Q} / r^{''} = p^{''}z^{''}, \text{ com } 0 \leq p^{''} \in \alpha \text{ e } 0 \leq z^{''} \in \gamma\}$$

e também

$$\alpha\beta + \alpha\gamma = \{s + t \in \mathbb{Q} / s \in \alpha\beta \text{ e } t \in \alpha\gamma\}.$$

Assim, os elementos de $\alpha\beta + \alpha\gamma$ são de uma das formas seguintes:

a) $a + b$, com $a, b \in \mathbb{Q}^*_-$;

b) $a + p^{''}z^{''}$, com $a \in \mathbb{Q}^*_-$, $0 \leq p^{''} \in \alpha$ e $0 \leq z^{''} \in \gamma$;

c) $p^{'}y^{'} + b$, com $b \in \mathbb{Q}^*_-$, $0 \leq p^{'} \in \alpha$ e $0 \leq y^{'} \in \beta$;

d) $p^{'}y^{'} + p^{''}z^{''}$, com $0 \leq p^{'} \in \alpha$, $0 \leq y^{'} \in \beta$, $0 \leq p^{''} \in \alpha$ e $0 \leq z^{''} \in \gamma$.

Vamos primeiramente provar que os elementos de $\alpha(\beta + \gamma)$ são escritos por uma das expressões acima. De fato, se o elemento de $\alpha(\beta + \gamma)$ é racional negativo, então este é dado por **a**); portanto, este também está em $\alpha\beta + \alpha\gamma$. Agora considere um elemento de $\alpha(\beta + \gamma)$ da forma $py + pz$, com $0 \leq p \in \alpha$, $y \in \beta$, $z \in \gamma$ e $0 \leq y + z$. Se $y, z \geq 0$, então $py + pz$ está representado em **d**) e; consequentemente, pertence a $\alpha\beta + \alpha\gamma$. Se $y < 0$ e $z \geq 0$, então $py + pz$ é da forma dada em **b**) (se $p > 0$) ou **d**) (se $p = 0$); em ambos os casos, $py + pz \in \alpha\beta + \alpha\gamma$. Se $y \geq 0$ e $z < 0$, então $py + pz$ é da forma estabelecida em **c**) (se $p > 0$) ou **d**) (se $p = 0$); em qualquer caso $py + pz \in \alpha\beta + \alpha\gamma$. Concluímos que $\alpha(\beta + \gamma) \subset \alpha\beta + \alpha\gamma$.

Reciprocamente, tomemos agora um elemento de $\alpha\beta + \alpha\gamma$ da forma **a**). É óbvio que este pertence a $\alpha(\beta+\gamma)$, por definição de multiplicação. Se o elemento de $\alpha\beta+\alpha\gamma$ é da forma **b**), isto é, $a + p^{''}z^{''}$, com $0 \leq p^{''} \in \alpha$ e $0 \leq z^{''} \in \gamma$. Note que, se $p^{''} = 0$, então $a + p^{''}z^{''} = a < 0$. Logo, $a + p^{''}z^{''} \in \alpha(\beta+\gamma)$. Assuma que $p^{''} > 0$. Se $a + p^{''}z^{''} < 0$, então $a + p^{''}z^{''} \in \alpha(\beta+\gamma)$. Considere, então que $a + p^{''}z^{''} \geq 0$. Logo,

$$\frac{1}{p^{''}}(a + p^{''}z^{''}) \geq \frac{1}{p^{''}} \cdot 0 = 0.$$

Daí, $\frac{a}{p^{''}} + z^{''} \geq 0$. Seja $y = \frac{a}{p^{''}}$. Então, $y < 0$ ($y \in 0^* \subset \beta$); logo, $y \in \beta$. Além disso, $y + z^{''} \geq 0$. Portanto,

$$a + p^{''}z^{''} = p^{''}(\frac{a}{p^{''}}) + p^{''}z^{''} = p^{''}y + p^{''}z^{''},\ 0 \leq p^{''} \in \alpha,\ y \in \beta,\ 0 \leq z^{''} \in \gamma,\ y + z'' \geq 0.$$

Isto nos diz que $a + p^{''}z^{''} \in \alpha(\beta+\gamma)$. Se o elemento de $\alpha\beta+\alpha\gamma$ é da forma **c**), faz-se de maneira análoga ao item **b**. Se o elemento de $\alpha\beta+\alpha\gamma$ é da forma **d**), ou seja, $p^{'}y^{'} + p^{''}z^{''}$, com $0 \leq p^{'} \in \alpha$, $0 \leq y^{'} \in \beta$, $0 \leq p^{''} \in \alpha$ e $0 \leq z^{''} \in \gamma$. Suponhamos $p^{''} \geq p^{'}$, então

$$p^{'}y^{'}+p^{''}z^{''} = p^{'}y^{'}-p^{''}y^{'}+p^{''}y^{'}+p^{''}z^{''} = (p^{'}-p^{''})y^{'}+p^{''}y^{'}+p^{''}z^{''} \leq 0+p^{''}y^{'}+p^{''}z^{''} = p^{''}y^{'}+p^{''}z^{''} \in \alpha(\beta+\gamma).$$

Daí, $p^{'}y^{'} + p^{''}z^{''} \in \alpha(\beta+\gamma)$ (corte). Suporemos agora, que $p^{''} < p^{'}$, temos

$$p^{'}y^{'} + p^{''}z^{''} = p^{'}y^{'} + p^{'}z^{''} - p^{'}z^{''} + p^{''}z^{''} = p^{'}y^{'} + p^{'}z^{''} + z^{''}(-p^{'} + p^{''}) \leq p^{'}y^{'} + p^{'}z^{''} \in \alpha(\beta+\gamma).$$

Como $\alpha(\beta+\gamma)$ é um corte, então $p^{'}y^{'} + p^{''}z^{''} \in \alpha(\beta+\gamma)$. Portanto, $\alpha\beta+\alpha\gamma \subset \alpha(\beta+\gamma)$. Logo, $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$.

Caso 2: Assuma $\alpha \leq 0^*$ e $\beta, \gamma \geq 0^*$:

Aqui, temos que

$$\begin{aligned}\alpha(\beta+\gamma) &= -(-\alpha)(\beta+\gamma) = -[(-\alpha)\beta + (-\alpha)\gamma] \\ &= [-(-\alpha)\beta] - (-\alpha)\gamma = -(-\alpha\beta) + \{-[-(\alpha\gamma)]\} \\ &= \alpha\beta + \alpha\gamma.\end{aligned}$$

Caso 3: Considere que $\alpha, \beta \leq 0^*$ e $\gamma \geq 0^*$:

Note que, se $\beta + \gamma \leq 0^*$, então

$$\begin{aligned}\alpha(\beta+\gamma) + (-\alpha)\gamma &= (-\alpha)(-\beta-\gamma) + (-\alpha)\gamma = (-\alpha)[-\beta-\gamma+\gamma] \\ &= (-\alpha)(-\beta) = \alpha\beta.\end{aligned}$$

Assim, somando o simétrico de $(-\alpha)\gamma$ em ambos os lados da igualdade resultante, encontramos

$$\alpha(\beta+\gamma) = \alpha\beta + [-(-\alpha)\gamma] = \alpha\beta + \alpha\gamma.$$

Agora, se $\beta+\gamma \geq 0^*$, então

$$\begin{aligned} \alpha\beta + (-\alpha)(\beta+\gamma) &= (-\alpha)(-\beta) + (-\alpha)[\beta+\gamma] \\ &= (-\alpha)[-\beta+\beta+\gamma] \\ &= (-\alpha)\gamma. \end{aligned}$$

Dessa forma, $\alpha\beta + [-(-\alpha)\gamma] = -(-\alpha)(\beta+\gamma)$, o que nos diz que $\alpha\beta+\alpha\gamma = \alpha(\beta+\gamma)$.

Caso 4: Assuma $\alpha, \beta, \gamma \leq 0^*$:

Veja que

$$\beta+\gamma \leq 0^* + \gamma = \gamma \leq 0^*.$$

Logo, pela Proposição 4.11, chegamos a

$$\begin{aligned} \alpha(\beta+\gamma) &= (-\alpha)[-(\beta+\gamma)] = (-\alpha)(-\beta-\gamma) \\ &= (-\alpha)[(-\beta)+(-\gamma)] = (-\alpha)(-\beta)+(-\alpha)(-\gamma) \\ &= \alpha\beta+\alpha\gamma, \end{aligned}$$

desde que $-\alpha, -\beta, -\gamma \geq 0^*$.

Caso 5: Suponha que $\alpha \leq 0^*$ e $\beta, \gamma \geq 0^*$:

Note que, $\beta+\gamma \geq 0^*$. Consequentemente,

$$\begin{aligned} \alpha(\beta+\gamma) &= -|\alpha||\beta+\gamma| = -[(-\alpha)(\beta+\gamma)] \\ &= -[(-\alpha)\beta+(-\alpha)\gamma] = -[-\alpha\beta-\alpha\gamma] \\ &= \alpha\beta+\alpha\gamma. \end{aligned}$$

Caso 6: Assuma $\alpha \geq 0^*$ e $\beta, \gamma \leq 0^*$:

Sabemos que

$$\beta+\gamma \leq 0^* + \gamma = \gamma \leq 0^*.$$

Assim,

$$\begin{aligned}\alpha(\beta+\gamma) &= -|\alpha||\beta+\gamma| = -\alpha[-(\beta+\gamma)] \\ &= -\alpha(-\beta-\gamma) = -[\alpha(-\beta)+\alpha(-\gamma)] \\ &= -(-\alpha\beta)-(-\alpha\gamma) = \alpha\beta+\alpha\gamma.\end{aligned}$$

□

A seguir, provaremos que quando multiplicamos qualquer elemento de $\mathbb{R}$ por 0^* encontramos novamente o elemento neutro da adição 0^*.

Teorema 4.13. *Seja $\alpha \in \mathbb{R}$. Então, $\alpha \cdot 0^* = 0^*$.*

Demonstração. Note que, pela distributividade, que

$$\alpha \cdot 0^* = \alpha \cdot (0^* + 0^*) = \alpha \cdot 0^* + \alpha \cdot 0^*.$$

Daí, somando $-\alpha \cdot 0^*$, em ambos os lados da igualdade, obtemos

$$\begin{aligned}0^* &= \alpha \cdot 0^* + (-\alpha \cdot 0^*) = (\alpha \cdot 0^* + \alpha \cdot 0^*) + (-\alpha \cdot 0^*) \\ &= \alpha \cdot 0^* + [\alpha \cdot 0^* + (-\alpha \cdot 0^*)] = \alpha \cdot 0^* + 0^* = \alpha \cdot 0^*.\end{aligned}$$

Portanto, $\alpha \cdot 0^* = 0^*$. □

Agora, vejamos como provar a compatibilidade entre a relação de ordem $\leq$ e a operação de multiplicação em $\mathbb{R}$.

Teorema 4.14. *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Então, vale os seguintes itens:*

i) $\alpha \leq \beta, \gamma \geq 0^* \Rightarrow \alpha\gamma \leq \beta\gamma$;

ii) $\alpha \leq \beta, \gamma \leq 0^* \Rightarrow \alpha\gamma \geq \beta\gamma$.

Demonstração. **i)** Como $\alpha \leq \beta$, então, pelo Teorema 4.8, temos que

$$0^* = \alpha + (-\alpha) \leq \beta + (-\alpha).$$

Logo, $\beta + (-\alpha) \geq 0^*$. Além disso, como $\gamma \geq 0^*$, então $[\beta + (-\alpha)]\gamma \geq 0^*$, pela Proposição 4.12. Daí, por distributividade, concluímos que $\beta\gamma + (-\alpha)\gamma \geq 0^*$ e, novamente, pelo Teorema 4.8, podemos escrever $\beta\gamma \geq \alpha\gamma$, isto é, $\alpha\gamma \leq \beta\gamma$;

ii) Como $\alpha \leq \beta$, logo, pelo Teorema 4.8, obtemos

$$0^* = \alpha + (-\alpha) \leq \beta + (-\alpha).$$

Com isso, inferimos $\beta + (-\alpha) \geq 0^*$. Como $-\gamma \geq 0^*$ (ver Proposição 4.11), encontramos $[\beta + (-\alpha)](-\gamma) \geq 0^*$, pela Proposição 4.12. Daí, por distributividade, chegamos a $\beta(-\gamma) + (-\alpha)(-\gamma) \geq 0^*$ e, novamente, pelo Teorema 4.8, encontramos $\beta\gamma \leq \alpha\gamma$, ou seja, $\alpha\gamma \geq \beta\gamma$.

□

Em ordem a definir o inverso multiplicativo para cada elemento não nulo de $\mathbb{R}$, mostremos o seguinte resultado.

Teorema 4.15. *Seja $\alpha \in \mathbb{R}$, com $\alpha > 0^*$. O conjunto $\beta = \mathbb{Q}_- \cup \{p \in \mathbb{Q}/p^{-1} \notin \alpha\}$ é um corte. Além disso, $\beta > 0^*$.*

Demonstração. **i)** Note que $0 \in \beta$, portanto $\beta \neq \emptyset$. Como $\alpha > 0^*$, então $\exists q \in \alpha$ tal que $q \notin 0^*$. Assim, $q \in \alpha$ e $q \geq 0$. Como α é um corte, então $\exists p \in \alpha$ tal que $0 \leq q < p$. Dessa forma, encontramos $p \in \alpha$ que satisfaz $p > 0$. Vamos provar agora que $p^{-1} \notin \beta$. De fato, se $p^{-1} \in \beta$, então teríamos que $p = (p^{-1})^{-1} \notin \alpha$, o que é contradição ($p \in \alpha$). Logo, $p^{-1} \notin \beta$, ou seja, temos pelo menos, um elemento em $\mathbb{Q}$, tal que, este elemento não está em β, isto é, $\beta \neq \mathbb{Q}$.

ii) Seja $p \in \beta$ e $q \in \mathbb{Q}$ com $q < p$. Devemos mostrar que $q \in \beta$. Se $q \leq 0$, então $q \in \beta$, pela definição de β. Suponhamos então $q > 0$. Assim, temos $0 < q < p$. Daí, como $p, q \in \mathbb{Q}_+^*$ e $q < p$, pelas propriedades dos racionais, $p^{-1} < q^{-1}$. Como $p^{-1} \notin \alpha$ ($p \in \beta$ e $p > 0$), segue que $q^{-1} \notin \alpha$ (α é um corte). Assim, $q \in \beta$.

iii) Seja $p \in \beta$. Mostraremos que existe $q \in \beta$ tal que $p < q$. Suponha que $p \leq 0$. Afirmamos que $\exists q_0 \notin \alpha$ tal que $q_0 > 0$. De fato, sabemos que $\exists p_0 \in \mathbb{Q}$ tal que $p_0 \notin \alpha$ ($\alpha \neq \mathbb{Q}$). Assim, se $p_0 > 0$, basta tomar $q_0 = p_0$ nada há a fazer. Considere que $p_0 \leq 0$. Como vimos acima $\exists p' \in \alpha$ tal que $0 < p'$. Como α é um corte, $p_0 \in \alpha$, o que é um absurdo. Assim, $q_0^{-1} \in \beta$ e $p \leq 0 < q_0^{-1}$.

Vamos supor agora que $p > 0$. Como $p \in \beta$ e $p > 0$, então $p^{-1} \notin \alpha$. Sem perda de generalidade, suponhamos $q_0 < p^{-1}$. Tomemos $s = \frac{q_0 + p^{-1}}{2}$. Assim temos que $q_0 < s < p^{-1}$. Tomando $q = s^{-1}$, chegamos a $q > p > 0$. Portanto, $q > 0$. Além disso, $q^{-1} = s \notin \alpha$ (pois $s > q_0$ e $q_0 \notin \alpha$). Logo, $q \in \beta$. Portanto, β não possui elemento máximo.

Isto prova que β é um corte. Por fim, observe que $0^* = \mathbb{Q}_-^* \subset \beta$, $0 \in \beta$ e $0 \notin 0^*$. Assim, $\beta > 0^*$. □

Definição 4.12. Seja α um corte tal que $\alpha \neq 0^*$. Se $\alpha > 0^*$, então o corte β do Teorema 4.15 é denotado por α^{-1} e chamado de inverso de α. Se $\alpha < 0^*$, então definimos o inverso de α como sendo $\alpha^{-1} = -|\alpha|^{-1}$.

Vamos provar que $\alpha^-1 \in \mathbb{R}$ é, de fato, o inverso multiplicativo de $\alpha \in \mathbb{R}$, se $\alpha \neq 0^*$.

Teorema 4.16. *Seja $\alpha \in \mathbb{R}$, com $\alpha \neq 0^*$. Então, $\alpha\alpha^{-1} = 1^*$. Além disso, o inverso de α é único.*

Demonstração. Consideremos dois casos, $\alpha > 0^*$ e $\alpha < 0^*$ (tricotomia).

• Caso $\alpha > 0^*$:

Vamos, primeiramente, provar que $\alpha\alpha^{-1} \subset 1^*$. Assim sendo, seja $r \in \alpha\alpha^{-1}$. Se $r \leq 0$, então $r \in 1^*$. Suponhamos $r > 0$. Como $r \in \alpha\alpha^{-1}$, então existem $s \in \alpha$, $p \in \alpha^{-1}$ tais que $r = sp$, com $s > 0$ e $p > 0$ ($r > 0$). Como $p \in \alpha^{-1}$ e $p > 0$, $\exists q \in \alpha^{-1}$, tal que $p < q$ (α^{-1} é corte). Logo, $q^{-1} \notin \alpha$ ($q > 0$) e $q^{-1} < p^{-1}$. Como $s \in \alpha$ e $q^{-1} \notin \alpha$, temos $s < q^{-1}$. Daí, temos $sq < 1$. Assim, $r = sp < sq < 1$, ou seja, $r \in 1^*$. Dessa forma, $\alpha\alpha^{-1} \subset 1^*$.

Reciprocamente, seja $r \in 1^*$. Se $r < 0$, então $r \in \alpha\alpha^{-1}$, pela definição de multiplicação. Se $r = 0$, temos $r = p \cdot 0$, onde $p \in \alpha$, $0 \in \alpha^{-1}$ e $p > 0$ (confira a existência deste p na prova do Teorema 4.15). Logo, $r \in \alpha\alpha^{-1}$. Suponhamos $0 < r < 1$. Seja $s \in \alpha$ com $s > 0$ (s existe ver prova do Teorema 4.15). Seja n o menor natural (Princípio da Boa Ordem) que satisfaz $s(r^{-1})^n \notin \alpha$ (este n existe, pois $r^{-1} > 1$ e se $s(r^{-1})^n \in \alpha$, $\forall n \in \mathbb{N}$, teríamos $\alpha = \mathbb{Q}$. De fato, seja $x \in \mathbb{Q}$, seja $n_0 \in \mathbb{N}$ tal que $n_0(r^{-1} - 1) > (xs^{-1} - 1)$ ($\mathbb{Q}$ é Arquimediano). Daí, utilizando a desigualdade de Bernoulli, obteríamos

$$s(r^{-1})^{n_0} = s[1 + (r^{-1} - 1)]^{n_0} \geq s[1 + n_0(r^{-1} - 1)] > s(1 + xs^{-1} - 1) = x.$$

Logo, chegaríamos que $x \in \alpha$ (α é corte), o que é uma contradição). Tomemos $p_1 = s(r^{-1})^{n-1} \in \alpha$ e $t = s(r^{-1})^n \notin \alpha$. Seja $p_2 \in \alpha$ tal que $p_1 < p_2$ (α não tem máximo). Tomemos $q_1 = t^{-1}p_2^{-1}p_1$, ou seja, $q_1^{-1} = tp_2p_1^{-1}$. Assim, devemos ter,

$$p_1 < p_2 \Rightarrow p_1p_1^{-1} < p_2p_1^{-1} \Rightarrow 1 < p_2p_1^{-1} \Rightarrow t < tp_2p_1^{-1} \Rightarrow t < q_1^{-1}.$$

Como $t \notin \alpha$, então $q_1^{-1} \notin \alpha$ e q_1^{-1} não é cota superior mínima de α (pois t é uma cota superior

mínima de α menor que q_1^{-1}, salientando que este elemento é qualquer). Temos ainda,

$$\begin{aligned} q_1 = t^{-1}p_2^{-1}p_1 &\Rightarrow p_2q_1 = t^{-1}p_1 \\ &\Rightarrow p_2q_1 = [s(r^{-1})^n]^{-1}s(r^{-1})^{n-1} \\ &\Rightarrow p_2q_1 = s^{-1}(r^{-1})^{-n}s(r^{-1})^{n-1} \\ &\Rightarrow p_2q_1 = (r^{-1})^{-1} = r. \end{aligned}$$

Como $p_2 \in \alpha$ e $q_1 \in \alpha^{-1}$ (pois $q_1^{-1} \notin \alpha$), então $r \in \alpha\alpha^{-1}$. Deste modo, $1^* \subset \alpha\alpha^{-1}$. Por fim, concluímos que $\alpha\alpha^{-1} = 1^*$.

- Caso $\alpha < 0^*$:

Por definição, temos que $\alpha^{-1} = -|\alpha|^{-1}$. Como $|\alpha|^{-1} > 0^*$, então $-|\alpha|^{-1} < 0^*$ (ver Proposição 4.11), ou seja, $\alpha^{-1} < 0^*$. Daí, pela definição de produto,

$$\alpha\alpha^{-1} = |\alpha||\alpha^{-1}| = |\alpha|| - |\alpha|^{-1}| = |\alpha|||\alpha|^{-1}| = |\alpha||\alpha|^{-1} = 1^*.$$

Resta provarmos a unicidade. Suponhamos a existência de $\gamma \in \mathbb{R}$ tal que $\alpha\gamma = 1^*$. Dessa forma,

$$\gamma = \gamma \cdot 1^* = \gamma(\alpha\alpha^{-1}) = (\gamma\alpha)\alpha^{-1} = (\alpha\gamma)\alpha^{-1} = 1^*(\alpha^{-1}) = \alpha^{-1}.$$

Isto nos diz que $\gamma = \alpha^{-1}$. □

Com a definição de inverso multiplicativo em $\mathbb{R}$, podemos estabelecer as recíprocas das afirmações dadas no Teorema 4.14.

Teorema 4.17. *Sejam $\alpha, \beta, \gamma \in \mathbb{R}$. Então, vale os seguintes itens:*

i) *Se $\gamma > 0^*$, então $\alpha\gamma \leq \beta\gamma \Rightarrow \alpha \leq \beta$;*

ii) *Se $\gamma < 0^*$, então $\alpha\gamma \geq \beta\gamma \Rightarrow \alpha \leq \beta$.*

Demonstração. **i)** Vimos no Teorema 4.15, que $\gamma^{-1} > 0^*$. Portanto, pelo Teorema 4.14, chegamos a $(\alpha\gamma)\gamma^{-1} \leq (\beta\gamma)\gamma^{-1}$. Por usar a associatividade, encontramos $\alpha(\gamma\gamma^{-1}) \leq \beta(\gamma\gamma^{-1})$. Aplicando o Teorema 4.16, concluímos que $\alpha \leq \beta$;

ii) Usando a prova do Teorema 4.15, inferimos que $\gamma^{-1} < 0^*$. Portanto, pelo Teorema 4.14, obtemos $(\alpha\gamma)\gamma^{-1} \leq (\beta\gamma)\gamma^{-1}$. Por associatividade, resulta $\alpha(\gamma\gamma^{-1}) \leq \beta(\gamma\gamma^{-1})$. Aplicando o Teorema 4.16, chegamos a $\alpha \leq \beta$.

Isto conclui a prova do teorema em questão. □

Abaixo, esclarecemos por que $\mathbb{R}$ não possui divisor de zero.

Proposição 4.15. Sejam $\alpha, \beta \in \mathbb{R}$. Então, $\alpha\beta = 0^*$ se, e somente se, $\alpha = 0^*$ ou $\beta = 0^*$.

Demonstração. ($\Rightarrow$) Considere que $\alpha\beta = 0^*$ e suponhamos que $\beta \neq 0^*$. Daí, $\exists \beta^{-1} \in \mathbb{R}$ tal que $\beta\beta^{-1} = 1^*$. Assim,

$$\alpha = \alpha \cdot 1^* = \alpha(\beta\beta^{-1}) = (\alpha\beta)\beta^{-1} = 0^* \cdot \beta^{-1} = 0^*.$$

($\Leftarrow$) Se $\alpha = 0^*$ ou $\beta = 0^*$, então já foi provado que $\alpha\beta = 0^*$. □

O resultado abaixo mostra que é o corte racional de um produto de números racionais.

Proposição 4.16. *Sejam $p, q \in \mathbb{Q}$. Então, $p^*q^* = (pq)^*$.*

Demonstração. Caso $p, q > 0$:

Vamos provar, primeiramente, que $p^*q^* \subset (pq)^*$. Assim, seja $r \in p^*q^*$. Então $r < 0$ ou $r = st$, com $p > s \geq 0$ e $q > t \geq 0$ ($p^* > 0^*$ e $q^* > 0^*$); de modo que, $r < 0$ ou $r = st < pq$. Logo, $r \in (pq)^*$. Reciprocamente, seja $r \in (pq)^*$, então podemos afirmar que ou $r < 0$ ou $0 \leq r < pq$. Se $r < 0$, claramente $r \in p^*q^*$, pela definição de multiplicação. Se $0 \leq r < pq$, então existem $p_1, q_1 \in \mathbb{Q}$ tais que $0 < p_1 < p$, $0 < q_1 < q$ e $r < p_1q_1 < pq$ (basta escolher $q_1, p_1 > 0$ tais que $\frac{r}{p_1} < q_1 < q$ e $\frac{r}{q_1} < p_1 < p$). Salientemos que $p_1 \in p^*$ e $q_1 \in q^*$. Assim, $p_1q_1 \in p^*q^*$. Logo, $r \in p^*q^*$ (p^*q^* é um corte).

Caso $p > 0$ e $q < 0$:

Neste caso, temos que

$$p^*q^* = -|p^*||q^*| = -p^*(-q^*) = -p^*(-q)^* = -[p(-q)]^* = -[-pq]^* = (pq)^*.$$

Caso $p < 0$ e $q > 0$:

Aqui, é possível escrever

$$p^*q^* = -|p^*||q^*| = -(-p^*)q^* = -(-p)^*q^* = -[(-p)q]^* = -[-pq]^* = (pq)^*.$$

Caso $p < 0$ e $q < 0$:

Analogamente, chegamos a

$$p^*q^* = |p^*||q^*| = (-p^*)(-q^*) = (-p)^*(-q)^* = [(-p)(-q)]^* = (pq)^*.$$

Caso $p = 0$ ou $q = 0$:

Neste caso, $(pq)^* = 0^* = p^*q^*$. □

Para exemplificar a definição de inverso multiplicativo provaremos o seguinte corolário, o qual busca pelo inverso de um corte racional.

Corolário 4.18. *Sejam $p \in \mathbb{Q}^*$. Então, $(p^*)^{-1} = (p^{-1})^*$.*

Demonstração. Por aplicar a Proposição 4.16, chegamos a

$$p^*(p^{-1})^* = (pp^{-1})^* = 1^*.$$

Pela unicidade do elemento inverso, concluímos que $(p^*)^{-1} = (p^{-1})^*$. □

O nosso interesse agora é provar que existe um corte racional entre dois cortes quaisquer dados. Primeiramente, trabalharemos com a seguinte Proposição.

Proposição 4.17. *Seja $\alpha \in \mathbb{R}$. Então, $r \in \alpha \Leftrightarrow r^* < \alpha$.*

Demonstração. ($\Rightarrow$) Suponha que $r \in \alpha$. Como $r \notin r^*$, então $r^* < \alpha$.

($\Leftarrow$) Reciprocamente, se $r^* < \alpha$ temos que existe $s \in \alpha \backslash r^*$ ($s \in \alpha$ e $s \notin r^*$). Então, $s \geq r$ e $s \in \alpha$. Logo, $r \in \alpha$ (α é um corte). □

Teorema 4.19. *Sejam $\alpha, \beta \in \mathbb{R}$ tais que $\alpha < \beta$. Então, existe um corte racional $r^* \in \mathbb{R}$ tal que $\alpha < r^* < \beta$.*

Demonstração. Dividiremos esta prova em dois casos.

Caso 1 : Considere que α é um corte racional, digamos $\alpha = s^*$.

Como $\alpha < \beta$, existe $r \in \beta \backslash \alpha$ (r racional). Assim, $r \in \beta$ e $r \notin \alpha = s^*$. Logo, $r \geq s$. Afirmamos que $r > s$; caso contrário, $\beta \backslash \alpha = \{s\}$, isto é, $\beta = \alpha \cup \{s\}$ contrariando a condição **iii**) da definição

de corte (s seria um máximo de β). De $r \in \beta$ e $r \notin r^*$(definião de corte racional), obtemos $r^* < \beta$. Por outro lado, como $s < r$, então $\alpha = s^* < r^*$. Portanto, $\alpha < r^* < \beta$.

Caso 2 : α não é um corte racional.

Como $\alpha < \beta$, existe $r \in \beta \backslash \alpha$ (r racional). De $r \in \beta \backslash \alpha$, temos que $r \in \beta$ e $r \notin \alpha$. Como $r \in \beta$ e $r \notin r^*$, obtemos $r^* < \beta$. Mas, r é cota superior de α (pois $r \notin \alpha$) e α não é corte racional, então r não é cota superior mínima de α. Logo, $\exists s$ cota superior de α ($s \notin \alpha$) tal que $s < r$, ou seja, existe $s \in r^* \backslash \alpha$. Deste modo, $\alpha < r^*$. Por fim, $\alpha < r^* < \beta$. □

Temos, então, $\mathbb{R}$ munido de duas operações e de uma relação de ordem obedecendo às mesmas leis aritméticas dos racionais. Assim, resgatando a linguagem algébrica da Seção 3.6, $\mathbb{R}$ é, como $\mathbb{Q}$, um corpo ordenado.

Para finalizar esta subseção, gostaríamos de ressaltar que, a partir do que foi provado acima, é possível definir a operação de divisão em $\mathbb{R}$.

Definição 4.13. Sejam $\alpha, \beta \in \mathbb{R}$, com $\beta \neq 0^*$. Definimos a divisão de α por β em $\mathbb{R}$, e denotamos $\frac{\alpha}{\beta}$, por

$$\frac{\alpha}{\beta} := \alpha\beta^{-1}.$$

Note que esta operação associa dois elementos de $\mathbb{R}$ a um outro elemento de $\mathbb{R}$.

Proposição 4.18. *Sejam $p, q \in \mathbb{Q}$. Então, $\left(\frac{p}{q}\right)^* = \frac{p^*}{q^*}$.*

Demonstração. Esta proposição segue diretamente de alguns resultados, já provados, para cortes racionais. De fato,

$$\frac{p^*}{q^*} = p^* \cdot (q^*)^{-1} = p^* \cdot (q^{-1})^* = (p \cdot q^{-1})^* = \left(\frac{p}{q}\right)^*.$$

□

4.1.4 Caracterização Usual dos Números Reais

Iniciaremos esta subseção mostrando uma maneira de identificar um número racional q com o respectivo corte racional q^* em $\mathbb{R}$. Deste modo, teremos uma cópia de $\mathbb{Q}$ em $\mathbb{R}$.

Proposição 4.19. *A aplicação $f_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}$, dada por $f_{\mathbb{Q}}(r) = r^*$, para todo $r \in \mathbb{Q}$, satisfaz as seguintes afirmações:*

i) $f_{\mathbb{Q}}$ *é injetora;*

ii) $f_{\mathbb{Q}}(r) + f_{\mathbb{Q}}(s) = f_{\mathbb{Q}}(r+s)$*;*

iii) $f_{\mathbb{Q}}(r) f_{\mathbb{Q}}(s) = f_{\mathbb{Q}}(rs)$*;*

iv) $f_{\mathbb{Q}}(r) < f_{\mathbb{Q}}(s) \Leftrightarrow r < s$.

Demonstração. A Proposição 4.5 nos garante que $f_{\mathbb{Q}}$ é injetora e satisfaz **iv**). Os itens **ii**) e **iii**) foram provados nas Proposições 4.8 e 4.16, respectivamente. □

Mais uma vez, obtivemos uma cópia algébrica de um conjunto em outro, desta vez, $f_{\mathbb{Q}}(\mathbb{Q})$ é a cópia de $\mathbb{Q}$ em $\mathbb{R}$, sendo $f_{\mathbb{Q}}(\mathbb{Q})$ precisamente o conjunto dos cortes racionais. Vimos também que há em $\mathbb{R}$ cortes não racionais. Assim, $\mathbb{R} \backslash f_{\mathbb{Q}}(\mathbb{Q}) \neq \emptyset$.

Definição 4.14. O conjunto $\mathbb{R}$ dos cortes será, a partir de agora, denominado de conjunto dos números reais. Os cortes racionais serão identificados, via injeção $f_{\mathbb{Q}}$, com os números racionais. Todo corte que não for racional será denominado número irracional.

A identificação de $f_{\mathbb{Q}}(\mathbb{Q})$ com $\mathbb{Q}$ nos permite escrever $\mathbb{Q} \subset \mathbb{R}$. O conjunto $\mathbb{R} \backslash \mathbb{Q}$ representa o conjunto dos números irracionais.

Os resultados seguintes mostram que, apesar da semelhança entre as propriedades aritméticas e de ordem entre $\mathbb{Q}$ e $\mathbb{R}$, há uma importante propriedade de $\mathbb{R}$ que $\mathbb{Q}$ não possui, a da completude.

Teorema 4.20 (Dedekind)**.** *Sejam* $A, B \subset \mathbb{R}$ *tais que:*

i) $\mathbb{R} = A \cup B$*;*

ii) $A \cap B = \emptyset$*;*

iii) $A \neq \emptyset$ *e* $B \neq \emptyset$*;*

iv) $\alpha \in A, \beta \in B \Rightarrow \alpha < \beta$.

Nessas condições, existe um único $\gamma \in \mathbb{R}$ *tal que* $\alpha \leq \gamma \leq \beta$*, para todo* $\alpha \in A$ *e para todo* $\beta \in B$.

Demonstração. Existência: Seja $\gamma = \{r \in \mathbb{Q} / r \in \alpha$, para algum $\alpha \in A\}$. Mostremos que γ é um corte.

i) $\gamma \neq \emptyset$ resulta imediatamente de $A \neq \emptyset$ e de que qualquer elemento de A é um corte. Para mostrar que $\gamma \neq \mathbb{Q}$, tomemos $\beta \in B$ ($B \neq \emptyset$). Seja $s \notin \beta$ um racional (β é um corte). Como $\alpha \subset \beta$, $\forall \alpha \in A$ ($\alpha < \beta$), então $s \notin \alpha$, $\forall \alpha \in A$. De onde obtemos $s \notin \gamma$. Daí, $\gamma \neq \mathbb{Q}$.

ii) Sejam $r \in \gamma$ e $s < r$. Logo, $r \in \alpha$ para algum $\alpha \in A$ e, como $s < r$, então $s \in \alpha$ de onde segue que $s \in \gamma$.

iii) Se $r \in \gamma$, então $r \in \alpha$ para algum $\alpha \in A$. Como α é um corte, existe $s \in \alpha$ tal que $s > r$. Logo, $s \in \gamma$.

Assim, $\gamma \in \mathbb{R}$ e temos que $\alpha \leq \gamma$, $\forall \alpha \in A$, pois pela definição de γ, sabemos que $\alpha \subset \gamma$, $\forall \alpha \in A$. Mostremos agora que $\gamma \leq \beta$, $\forall \beta \in B$. Suponhamos que exista $\beta \in B$ com $\beta < \gamma$. Neste caso, existe um racional $r \in \gamma \backslash \beta$. Por pertencer a γ, r é um elemento de algum $\alpha \in A$ e, não sendo elemento de β, obtemos $\beta < \alpha$. Isto contradiz **iv**). Por fim, $\alpha \leq \gamma \leq \beta, \forall \alpha \in A$ e $\beta \in B$.

Unicidade: suponhamos que existam dois números reais distintos γ_1 e γ_2 satisfazendo o enunciado acima. Sem perda de generalidade assuma que $\gamma_1 < \gamma_2$. Consideremos γ_3 tal que $\gamma_1 < \gamma_3 < \gamma_2$, o que é possível pelo Teorema 4.19. De $\gamma_3 < \gamma_2$ resulta $\gamma_3 \in A$, pois $\beta \geq \gamma_2$ ($> \gamma_3$), para todo $\beta \in B$ e $\mathbb{R} = A \cup B$. Analogamente, de $\gamma_1 < \gamma_3$, resulta $\gamma_3 \in B$. Dessa forma, $\gamma_3 \in A \cap B$. Mas, $A \cap B = \emptyset$. Contradição! □

Corolário 4.21. *Nas condições do Teorema* 4.20, *ou existe* $\max A$, *ou* $\min B$.

Demonstração. Seja $\gamma \in \mathbb{R}$ encontrado no Teorema 4.20. Então, γ está ou em A ou em B, pelas hipóteses **i**) e **ii**) deste mesmo resultado. Portanto, se $\gamma \in A$, então $\gamma = \max A$ e, se $\gamma \in B$, tem-se $\gamma = \min B$. □

De maneira informal temos que $\mathbb{R}$ não há lacunas, ou é "completo". O mesmo não podemos dizer sobre $\mathbb{Q}$. Conforme veremos na proposição abaixo.

Proposição 4.20. *Considere os seguintes subconjuntos de* $\mathbb{Q}$*:*

$$A = \mathbb{Q}_-^* \cup \{x \in \mathbb{Q}_+ / x^2 < 2\} \text{ e } B = \{x \in \mathbb{Q}_+ / x^2 > 2\}.$$

A e B satisfazem as hipóteses do teorema anterior, com $\mathbb{Q}$ no lugar de $\mathbb{R}$, mas não existe $r \in \mathbb{Q}$ satisfazendo $a \leq r \leq b$, $\forall a \in A$ e $\forall b \in B$.

Demonstração. Suponha, por absurdo, que existe $r \in \mathbb{Q}$: $a \leq r \leq b$, $\forall a \in A$ e $\forall b \in B$. Então, $r \notin A$ [r é uma cota superior do corte A (A é um corte de acordo com o teorema 4.1)]. Daí, $r \in B$, já que $\mathbb{Q} = A \cup B$. Logo, $r > 0$ e $r^2 > 2$. Seja $0 < \varepsilon < \frac{r^2-2}{2r}$. Assim,

$$\begin{aligned}(r-\varepsilon)^2 &= r^2 - 2r\varepsilon + \varepsilon^2 > r^2 - 2r\varepsilon \\ &> r^2 - 2r\frac{(r^2-2)}{2r} = r^2 - r^2 + 2 \\ &= 2.\end{aligned}$$

Dessa forma, $r - \varepsilon \in B$, o que é um absurdo ($r - \varepsilon < r$). □

Notemos, informalmente, que em $\mathbb{R}$ não há lacunas, mas, em $\mathbb{Q}$ há. Por esta razão, dizemos que $\mathbb{R}$ é completo.

Para finalizar esta subseção, permita-nos listar a usual notação para intervalos de números reais, que são os subconjuntos de $\mathbb{R}$ dos seguintes tipos, onde a e b são reais com $a < b$:

1. $(a, b) = \{x \in \mathbb{R} / a < x < b\}$;
2. $[a, b) = \{x \in \mathbb{R} / a \leq x < b\}$;
3. $(a, b] = \{x \in \mathbb{R} / a < x \leq b\}$;
4. $[a, b] = \{x \in \mathbb{R} / a \leq x \leq b\}$;
5. $(a, +\infty) = \{x \in \mathbb{R} / x > a\}$;
6. $[a, +\infty) = \{x \in \mathbb{R} / x \geq a\}$;
7. $(-\infty, a) = \{x \in \mathbb{R} / x < a\}$;
8. $(-\infty, a] = \{x \in \mathbb{R} / x \leq a\}$;
9. $(-\infty, +\infty) = \mathbb{R}$.

4.1.5 Completude de $\mathbb{R}$

Nesta subseção, definiremos o significado de ínfimo e supremo de conjuntos limitados em $\mathbb{R}$.

Definição 4.15. Seja $A \subset \mathbb{R}$. Estabelecemos as seguintes definições:

i) Dizemos que A é limitado superiormente se existe $k \in \mathbb{R}$ tal que $k \geq x$, $\forall x \in A$. Um tal k diz-se cota superior de A;

ii) Dizemos que A é limitado inferiormente se existe $y \in \mathbb{R}$ tal que $y \leq x$, $\forall x \in A$. Um tal y diz-se cota inferior de A;

iii) A diz-se limitado se for limitado superior e inferiormente;

iv) Suponhamos que A seja limitado superiormente e que s é uma cota superior mínima de A (no sentido de que qualquer cota superior de A seja maior ou igual a s). Neste caso, s diz-se supremo de A e é denotado por $\sup A$.

v) De modo análogo, define-se ínfimo de A (para conjuntos A limitados inferiormente), denotado por $\inf A$, como sendo uma cota inferior máxima para o conjunto A.

A seguir apresentaremos exemplos sobre as definições dadas acima.

Proposição 4.21. *As seguintes afirmações são válida:*

i) *Seja* $A = \{\frac{1}{n}/n \in \mathbb{N}^*\}$. *Assim,* A *é limitado,* $\sup A = 1$ *e* $\inf A = 0$*;*

ii) $B = \{x \in \mathbb{R}/x \geq 0\}$. *Então,* B *é limitado inferiormente e* $\inf B = 0$.

Demonstração. De fato,

i) Sabemos que $0 \leq \frac{1}{n}$, $\forall n \in \mathbb{N}^*$, ou seja, 0 é cota inferior de A. Seja $y > 0$, vamos provar que y não é cota inferior de A. Usando o fato de $\mathbb{Q}$ ser Arquimediano, temos que $\exists n \in \mathbb{N}^*$ tal que $\frac{1}{y} < n$, isto é, $y > \frac{1}{n}$ e $\frac{1}{n} \in A$. Portanto, $\inf A = 0$.

Por outro lado, sabemos também que $n \geq 1, \forall n \in \mathbb{N}^*$. Logo, $\frac{1}{n} \leq 1, \forall n \in \mathbb{N}^*$. Assim, $\sup A = 1$ (pois $1 \in A$);

ii) Note que qualquer $r \in \mathbb{R}$, tal que $r \leq 0$ é uma cota inferior de B. Precisamos mostrar que 0 é a maior cota inferior de B. De fato, se $r > 0$, então r não pode ser cota inferior de B, pois $\frac{1}{2} \in B$ e $\frac{1}{2} < r$. Portanto, $\inf B = 0$.

□

O resultado a seguir garante a unicidade do supremo, caso exista, para conjuntos limitados superiormente em $\mathbb{R}$.

Proposição 4.22. Um subconjunto não vazio de $\mathbb{R}$ admite, no máximo, um supremo.

Demonstração. Seja $A \subset \mathbb{R}$ não vazio. Suponhamos que existam $a_1 = \sup A$ e $a_2 = \sup A$. Daí, $a_1, a_2 \leq x$, para todo x cota superior de A. Assim, usando o fato de a_1 e a_2 serem cotas superiores de A, obtemos

$$a_1 \leq a_2 \text{ e } a_2 \leq a_1.$$

Portanto, $a_1 = a_2$ (tricotomia). Isto nos diz que se o supremo de um conjunto não vazio existe, então este é único. □

Agora, vamos provar a existência do supremo para qualquer subconjunto de $\mathbb{R}$ não vazio e limitado superiormente (esta propriedade não é válida em $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$).

Teorema 4.22. *Seja $X \subset \mathbb{R}$ um conjunto não vazio e limitado superiormente. Então,* $\sup X \in \mathbb{R}$ *existe.*

Demonstração. Definamos

$$A = \{\alpha \in \mathbb{R} / \alpha < x, \text{ para algum } x \in X\},$$

isto é, A é o conjunto constituído pelos números reais que não são cotas superiores de X. Seja $B = \mathbb{R} \backslash A$, isto é, B é o conjunto constituído pelas cotas superiores de X. Vamos verificar que A e B satisfazem as condições do Teorema 4.20.

As condições **i**) e **ii**) são claramente válidas. Quanto a **iii**), temos que, sendo $X \neq \emptyset$, existe $x \in X$ e, portanto, qualquer $\alpha < x$ é elemento de A. Logo, $A \neq \emptyset$. Além disso, como X é limitado superiormente, $B \neq \emptyset$. Para verificar **iv**), sejam $\alpha \in A$ e $\beta \in B$. Assim, existe $x \in X$ tal que $\alpha < x$. Como $\beta \geq x$ (β é cota superior de X), obtemos $\beta > \alpha$.

Pelo Corolário 4.21, ou A possui máximo, ou B possui mínimo. Vamos mostrar que a primeira alternativa não pode ocorrer, de onde decorrerá que B possui mínimo, que é a tese do teorema. Tomemos, então, α arbitrário em A. Assim, existe $x \in X$ tal que $\alpha < x$. Consideremos $\alpha^{'}$ tal que $\alpha < \alpha^{'} < x$. Logo, $\alpha^{'} \in A$ e $\alpha < \alpha^{'}$. Portanto, A não possui máximo. Como queríamos verificar. □

O teorema a seguir garante que $\mathbb{R}$, assim como $\mathbb{Q}$, é um corpo Arquimediano.

Teorema 4.23. *O conjunto $\mathbb{N}$ dos naturais é ilimitado em $\mathbb{R}$.*

Demonstração. Suponhamos que $\mathbb{N}$ é limitado superiormente em $\mathbb{R}$ e seja $\alpha = \sup \mathbb{N}$ ($\mathbb{N} \neq \emptyset$). Assim, $\alpha \geq n$, $\forall n \in \mathbb{N}$. Como $n+1 \in \mathbb{N}, \forall n \in \mathbb{N}$, então $n+1 \leq \alpha$, para todo $n \in \mathbb{N}$. Logo, obtemos $\alpha - 1 \geq n$, para todo $n \in \mathbb{N}$, isto é, $\alpha - 1$ é cota superior para $\mathbb{N}$ e $\alpha - 1 < \alpha = \sup \mathbb{N}$. Isto é uma contradição. Por fim, $\mathbb{N}$ não é limitado em $\mathbb{R}$. □

Provaremos agora a existência de números não racionais em $\mathbb{R}$ (note que a definição dada para potência no capítulo sobre $\mathbb{Q}$ pode ser aplicada a $\mathbb{R}$ (ver Definição 3.11), juntamente com as propriedades dadas nas Proposições 3.13 e 3.14).

Proposição 4.23. *Existe um único número real positivo cujo quadrado é 2, isto é, a equação $x^2 = 2$ tem uma única solução real positiva. Tal solução é denotada por $\sqrt{2}$.*

Demonstração. Seja $X = \{x \in \mathbb{R}_+^* / x^2 < 2\}$. É claro que $X \neq \emptyset$, pois $1 \in X$. X é limitado superiormente, por exemplo, pelo número 3. De fato, $0 < x < 3$ equivale a $x^2 < 3^2$, que é verdadeira para $x \in X$, pois, para esses números, $x^2 < 2$. Pelo Teorema 4.22, X possui supremo, digamos $s = \sup X$. Mostremos que $s^2 = 2$, por exclusão dos casos $s^2 < 2$ e $s^2 > 2$, de onde seguirá a afirmação.

Suponhamos $s^2 < 2$. Então, podemos escolher $h \in \mathbb{R}$ tal que $0 < h < \min\{1, \frac{2-s^2}{2s+1}\}$. Dessa forma, obtemos

$$\begin{aligned}(s+h)^2 &= s^2 + 2sh + h^2 < s^2 + 2sh + h \\ &= s^2 + h(2s+1) < s^2 + \frac{2-s^2}{2s+1} \cdot (2s+1) = 2,\end{aligned}$$

ou seja, $(s+h)^2 < 2$; logo, $s+h \in X$, contradizendo o fato de que s é cota superior de X ($s < s+h$).

Suponhamos agora $s^2 > 2$. Então, podemos escolher $h \in \mathbb{R}$ tal que $0 < h < \frac{s^2-2}{2s}$ para obter

$$(s-h)^2 = s^2 - 2sh + h^2 > s^2 - 2s\frac{s^2-2}{2s} > 2,$$

isto é, $(s-h)^2 > 2$, logo $s - h > x$, $\forall x \in X$, contradizendo o fato de s ser a menor cota superior de X ($s - h < s$).

Por fim, $s^2 = 2$. Como queríamos demonstrar. □

4.1.6 Representação Decimal dos Números Reais

Em ordem a representar cada número real de forma decimal, precisamos estabelecer o conceito de soma infinita em $\mathbb{R}$. Mais precisamente, temos a definição abaixo.

Definição 4.16. Seja $x_n \in \mathbb{R}$, para todo $n \in \mathbb{N}^*$. A soma infinita

$$x_1 + x_2 + ... + x_n + ...$$

é chamada série de números reais. Esta é denotada por $\sum_{n=1}^{\infty} x_n$. Dizemos que $\sum_{n=1}^{\infty} x_n = x \in \mathbb{R}$ quando dado ε real positivo existe $n_0 \in \mathbb{N}^*$ tal que $\forall n \geq n_0$, com $n \in \mathbb{N}^*$, tem-se

$$|s_n - x| < \varepsilon,$$

onde $s_n = x_1 + x_2 + ... + x_n, \forall n \in \mathbb{N}^*$.

Vejamos, a seguir, um exemplo de série envolvendo números reais.

Exemplo 4.10. Considere que $a, r \in \mathbb{R}_+^*$. A série de números reais $\sum_{n=1}^{\infty} ar^{n-1}$ é chamada de série geométrica de razão r.

Afirmamos que $\sum_{n=1}^{\infty} ar^{n-1} = \frac{a}{1-r}$, sempre que $r < 1$.

De fato, é fácil ver que, para $n \in \mathbb{N}^*$, vale

$$s_n = a + ar + ar^2 + ... + ar^n.$$

Multiplicando s_n, descrita acima, por $r \in \mathbb{R}_+^*$, obtemos

$$rs_n = ar + ar^2 + ... + ar^{n+1}.$$

Logo, $s_n - rs_n = a - ar^{n+1}$. Assim, $s_n = \frac{a(1-r^{n+1})}{1-r}$ $(1 - r > 0)$. Dado ε real positivo, existe, pela propriedade Arquimediana, $n_0 \in \mathbb{N}$ tal que

$$n_0 > \frac{r}{1-r}\left[\frac{a}{(1-r)\varepsilon} - 1 - \frac{1-r}{r}\right].$$

Daí. para todo $n \geq n_0$, com $n \in \mathbb{N}^*$, tem-se

$$\left|s_n - \frac{a}{1-r}\right| = \left|\frac{a(1-r^{n+1})}{1-r} - \frac{a}{1-r}\right| = \frac{a}{1-r}r^{n+1} < \varepsilon.$$

Com efeito,

$$\frac{a}{1-r}r^{n+1} < \varepsilon \Leftrightarrow r^{n+1} < \frac{(1-r)\varepsilon}{a} \Leftrightarrow \left(\frac{1}{r}\right)^{n+1} > \frac{a}{(1-r)\varepsilon}.$$

Mas, pela desigualdade de Bernoulli, chegamos a

$$\begin{aligned}\left(\frac{1}{r}\right)^{n+1} &= \left[1+\left(\frac{1}{r}-1\right)\right]^{n+1} \geq 1+(n+1)\left(\frac{1-r}{r}\right)\\ &\geq 1+(n_0+1)\left(\frac{1-r}{r}\right) = 1+n_0\left(\frac{1-r}{r}\right)+\frac{1-r}{r}\\ &> 1+\frac{r}{1-r}\left[\frac{a}{(1-r)\varepsilon}-1-\frac{1-r}{r}\right]\frac{1-r}{r}+\frac{1-r}{r}\\ &= 1+\frac{a}{(1-r)\varepsilon}-1-\frac{1-r}{r}+\frac{1-r}{r} = \frac{a}{(1-r)\varepsilon}.\end{aligned}$$

Portanto, $\sum\limits_{n=1}^{\infty} ar^{n-1} = \frac{a}{1-r}$.

Veja que, por exemplo, temos

$$\sum_{n=1}^{\infty}\frac{9}{10^n} = \sum_{n=1}^{\infty}\frac{9}{10}\left(\frac{1}{10}\right)^{n-1} = \frac{\frac{9}{10}}{1-\frac{1}{10}} = 1.$$

Portanto, se considerarmos a notação usual de números decimais, conhecida do ensino elementar, que será melhor justificada a seguir, temos que $0,999... = 1$ (o qual pode ser escrito também na forma $1,000...$) Analogamente, obtemos $1,4999... = 1,5$; já que,

$$\begin{aligned}1,4+\sum_{n=1}^{\infty}\frac{9}{10^{n+1}} &= 1,4+\sum_{n=1}^{\infty}\frac{9}{100}\left(\frac{1}{10}\right)^{n-1} = 1,4+\frac{\frac{9}{100}}{1-\frac{1}{10}}\\ &= 1,4+\frac{\frac{9}{100}}{\frac{9}{10}} = 1,4+\frac{90}{900}\\ &= 1,4+0,1 = 1,5.\end{aligned}$$

Vamos, agora, estudar a representação decimal dos números reais. Para isso, comecemos com o seguinte lema.

Lema 4.2. *Seja $\alpha \in \mathbb{R}_+$. Então, existe um máximo $m_0 \in \mathbb{N}$ tal que $m_0 \leq \alpha$. Além disso, $0 \leq \alpha - m_0 < 1$.*

Demonstração. Consideremos o conjunto $A = \{n \in \mathbb{N}/n \leq \alpha\}$. Mostremos que A possui um elemento máximo. De fato, para $B = \{p \in \mathbb{N}/p > \alpha\}$ temos que $B \subset \mathbb{N}$ e ainda $B \neq \emptyset$, pois, como vimos $\mathbb{N}$ é ilimitado em $\mathbb{R}$. Com isso, pelo Princípio da Boa Ordem, B possui um elemento mínimo, digamos, $p_0 = \min B$. Dessa forma, $\alpha < p_0 \leq p, \forall p \in B$ $(p_0 \in B)$. Desse modo, $p_0 - 1 \notin B$, ou seja, $p_0 - 1 \leq \alpha$; logo, $p_0 - 1 \in A$.

Afirmamos que $p_0 - 1$ é o máximo de A, isto é, $p_0 - 1 \geq n$ para todo $n \in A$. Com efeito, suponhamos $p_0 - 1 < n_0$ para algum $n_0 \in A$. Daí, $p_0 - 1 < n_0 \leq \alpha$, ou ainda, $p_0 \leq n_0 \leq \alpha$, o que

é uma contradição, pois $p_0 > \alpha$. Denotando $m_0 = p_0 - 1$, obtemos $m_0 \leq \alpha < m_0 + 1$ ($m_0 \in A$ e $m_0 + 1 \notin A$), donde $0 \leq \alpha - m_0 < 1$. □

No teorema a seguir, estudaremos a representação decimal dos números reais não negativos menores do que 1.

Teorema 4.24. *As seguintes afirmações são verdadeiras:*

i) *A cada número real α, tal que $0 \leq \alpha < 1$, corresponde uma única sequência de dígitos, denotada por $(n_k)_{k\in\mathbb{N}^*}$, i.e., uma aplicação $n : \mathbb{N}^* \to \mathbb{R}$, satisfazendo:*

a) $0 \leq n_k \leq 9, \forall k \in \mathbb{N}^*$;

b) $(n_k)_{k\in\mathbb{N}^*}$ *não possui infinitos dígitos consecutivos iguais a* 9;

c) *definindo, $S_k = \frac{n_1}{10} + ... + \frac{n_k}{10^k}, \forall k \in \mathbb{N}^*$, concluímos que $\alpha = \sup S$, onde $S = \{S_k \in \mathbb{R}/k \in \mathbb{N}^*\}$.*

ii) *Reciprocamente, a cada sequência de dígitos $(n_k)_{k\in\mathbb{N}^*}$, satisfazendo **a**) e **b**) acima, e definindo S_k como em **c**), corresponde um único número real α tal que $\alpha = \sup S \in [0, 1)$, onde $S = \{S_k \in \mathbb{R}/k \in \mathbb{N}^*\}$.*

Demonstração. **i)** Seja n_1 o maior natural tal que $0 \leq 10\alpha - n_1 < 1$ (ver Lema 4.2). Logo, $\frac{n_1}{10} = \alpha$ e $0 \leq n_1 \leq 9$ ($0 \leq \alpha < 1$).

Se $\frac{n_1}{10} = \alpha$, associamos a α a sequência $(n_1, 0, 0, 0...)$ (neste caso $S_k = \alpha, \forall k \in \mathbb{N}^*$; logo, $\alpha = \sup S$).

Se $\frac{n_1}{10} < \alpha$, temos que $\exists n_2$ o maior número natural tal que

$$\frac{n_1}{10} + \frac{n_2}{10^2} \leq \alpha.$$

Tal n_2 existe e satisfaz $0 \leq n_2 \leq 9$, já que

$$n_2 \leq 10^2(\alpha - \frac{n_1}{10}) \Leftrightarrow n_2 \leq 10(10\alpha - n_1) < 10,$$

ver Lema 4.2.

Se $\frac{n_1}{10} + \frac{n_2}{10^2} = \alpha$, associamos a α a sequência $(n_1, n_2, 0, 0, 0...)$ (neste caso, $S_1 < S_k = \alpha, \forall k \geq 2$; assim, $\alpha = \sup S$).

Se $\frac{n_1}{10} + \frac{n_2}{10^2} < \alpha$, tomamos n_3 como o maior natural satisfazendo

$$\frac{n_1}{10} + \frac{n_2}{10^2} + \frac{n_3}{10^3} \leq \alpha.$$

(Aqui $0 \leq (10^3\alpha - 10^2 n_1 - 10n_2) - n_3 < 1$). Logo, $n_3 \leq 10[10^2\alpha - (10n_1 + n_2)] < 10$. Consequentemente, $0 \leq n_3 \leq 9$. Neste caso, α corresponde a $(n_1, n_2, n_3, 0, ...)$ (note que, $S_1 < S_2 < S_k = \alpha, \forall k \geq 3$; assim $\alpha = \sup S$).

Seguindo este processo, assuma que foram encontrados $n_1, n_2, ..., n_{k-1}$ naturais entre 0 e 9 tais que

$$\frac{n_1}{10} + \frac{n_2}{10^2} + ... + \frac{n_{k-1}}{10^{k-1}} < \alpha \text{ e } 0 \leq 10^{k-1}\alpha - 10^{k-2}n_1 - ... - 10n_{k-2} - n_{k-1} < 1.$$

Logo, existe n_k o maior inteiro tal que

$$\frac{n_1}{10} + \frac{n_2}{10^2} + ... + \frac{n_k}{10^k} \leq \alpha.$$

(Aqui $0 \leq 10^k\alpha - 10^{k-1}n_1 - ... - 10n_{k-1} - n_k < 1$), com n_k satisfazendo, necessariamente, $0 \leq n_k \leq 9$ (pois, $n_k \leq 10(10^{k-1}\alpha - 10^{k-2}n_1 - ... - n_{k-1}) < 9$).

A α, associamos a sequência $(n_k)_{k\in\mathbb{N}^*}$ determinada na construção acima. O fato de que esta sequência não possui infinitos noves consecutivos vem do fato de estarmos aplicando as ideias expostas no Exemplo 4.10.

Consideremos agora S e S_k como na primeira parte do teorema e verifiquemos que, de fato, $\alpha = \sup S$. α é cota superior de S, por construção ($\alpha \geq S_k, \forall k \in \mathbb{N}^*$). Seja β um real positivo menor do que α. Mostremos que β não pode ser cota superior de S. Como $\mathbb{R}$ é Arquimediano, existe $k_0 \in \mathbb{N}$ tal que $\frac{1}{10^{k_0}} < \alpha - \beta$ (isto segue, como já foi feito antes, da desigualdade de Bernoulli). Logo, $\alpha - S_{k_0} < \frac{1}{10^{k_0}} < \alpha - \beta$ (pois, $10^{k_0}\alpha - 10^{k_0}S_{k_0} = 10^{k_0} - 10^{k_0-1}_{n_1} - ... - 10n_{k_0-1} - n_{k_0} < 1$), de onde segue que $\beta < S_{k_0}$, para algum $k_0 \in \mathbb{N}^*$. Como queríamos. Portanto $\alpha = \sup S$.

ii) Reciprocamente, dada uma sequência $(n_k)_{k\in\mathbb{N}^*}$, com $0 \leq n_k \leq 9$, para todo k, como foi estabelecido acima. É fácil ver que

$$S_k = \tfrac{n_1}{10} + ... + \tfrac{n_k}{10^k} \leq \tfrac{9}{10} + ... + \tfrac{9}{10^k} < \lambda < \sum_{n=1}^{\infty} \tfrac{9}{10^n} = 1,$$

onde λ é encontrado pelo fato de não termos infinitos noves na sequência $(n_k)_{k\in\mathbb{N}^*}$. S é limitado superiormente por 1. Assim, $\alpha = \sup S$ ($S \neq \emptyset$) é o número real associado à sequência $(n_k)_{k\in\mathbb{N}^*}$. Note que $0 \leq \alpha < 1$ (pois, $0 \leq \lambda < 1$).

Isto conclui a prova do teorema em questão. □

Estamos prontos para estabelecer a representação de qualquer número real da maneira conhecida do ensino elementar.

Definição 4.17. Estabelecemos, em $\mathbb{R}$, as seguintes definições:

i) Dado um número real α, com $0 \leq \alpha < 1$, seja $(n_k)_{k\in\mathbb{N}^*}$ a sequência de dígitos correspondente a α, sem infinitos noves consecutivos, construída na primeira parte do teorema acima. A representação decimal de α se define como sendo a expressão $0, n_1n_2n_3n_4....$ Se $n_k \neq 0$ e $n_l = 0$, para todo $l > k$, convenciona-se representar $0, n_1n_2n_3n_4...$ por $0, n_1n_2n_3n_4...n_k$, que será dita representação decimal finita de α;

ii) Se $\alpha \geq 1$, sabemos que existe $n_0 \in \mathbb{N}$ o maior natural tal que $0 \leq \alpha - n_0 < 1$ ($n_0 \leq \alpha$) (ver Lema 4.2). Seja $0, n_1n_2n_3n_4...n_k...$ a representação decimal de $\alpha - n_0$ definida em **i)**. Definimos a expressão decimal de α como sendo a expressão $n_0, n_1n_2n_3n_4...n_k...$;

iii) Se $\alpha < 0$, definimos sua representação decimal como sendo $-x$, onde x é a representação decimal de $-\alpha$.

Nossas representações decimais não consideram, então, expressões com infinitos noves consecutivos, como $0,999....$ Vimos no Exemplo 4.10 que é possível, no entanto, atribuir a elas um significado similar ao das expressões sem infinitos noves consecutivos. Mais precisamente, vimos que a representação decimal de 1 é, pela definição acima, $1,00000...$, que convencionamos representar pelo próprio símbolo 1. Dessa forma, escrevemos $0,999... = 1$ (para mais detalhes ver Exemplo 4.10).

Deste modo, estamos apontando para o fato de que representações decimais finitas ou periódicas (aquelas que contêm uma repetição sucessiva de um bloco de dígitos) correspondem os números racionais. De fato, seja $0 \leq \alpha < 1$, onde $\alpha = 0, \alpha_1\alpha_2...\alpha_n$ um número real com representação decimal finita. Multiplicando por 10^n ambos os membros da igualdade, obtemos

$$10^n\alpha = \alpha_1\alpha_2...\alpha_n \Rightarrow \alpha = \frac{\alpha_1\alpha_2...\alpha_n}{10^n} \in \mathbb{Q}.$$

Do mesmo modo, seja $\alpha = 0, \alpha_1\alpha_2...\alpha_n\alpha_1\alpha_2...\alpha_n...$ um número real com representação decimal periódica ($n \geq 1$). Multiplicando por 10^n ambos lados desta igualdade, encontramos

$$10^n\alpha = \alpha_1\alpha_2...\alpha_n, \alpha_1\alpha_2...\alpha_n...$$

Subtraindo os lados destas igualdades na ordem dada, obtemos

$$10^n\alpha - \alpha = \alpha_1\alpha_2...\alpha_n \Rightarrow \alpha = \frac{\alpha_1\alpha_2...\alpha_n}{10^n - 1} \in \mathbb{Q}.$$

De qualquer forma, $\alpha \in \mathbb{Q}$. Agora suponha que $\alpha \geq 1$ é dado com uma representação decimal finita ou periódica. Daí, existe $n_0 \in \mathbb{N}$ tal que $0 \leq \alpha - n_0 < 1$. Vimos acima que $\alpha - n_0 \in \mathbb{Q}$. Logo,

$\alpha \in \mathbb{Q}$. Por fim, se $\alpha < 0$ tem representação decimal finita ou periódica, então $-\alpha \in \mathbb{Q}$. Logo, $\alpha \in \mathbb{Q}$.

4.1.7 Não Enumerabilidade de $\mathbb{R}$

A representação decimal dos números reais permite demonstrar que $\mathbb{R}$ não é enumerável (diferentemente de $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$). Como faremos a seguir. Comecemos discutindo a não enumerabilidade de $I = (0, 1)$.

Lema 4.3. *O intervalo $I = (0, 1)$ não é enumerável.*

Demonstração. Mostremos que, qualquer que seja a enumeração estabelecida para elementos de I, sempre existirá um elemento de I não considerado na dada enumeração. De fato, seja $I^{'}$ um conjunto enumerável constituído de elementos de I que, portanto, pode ser escrito na forma $I^{'} = \{x_0, x_1, x_2, ...\}$, onde, para cada $n \in \mathbb{N}$, x_n representa a imagem de n por uma certa bijeção de $\mathbb{N}$ em $I^{'}$. Vamos representar cada elemento de $I^{'}$ pela sua representação decimal, dada acima, da seguinte forma:

$$\begin{aligned} x_0 &= 0, x_{00}x_{01}x_{02}... \\ x_1 &= 0, x_{10}x_{11}x_{12}... \\ x_2 &= 0, x_{20}x_{21}x_{22}... \\ &\vdots \\ x_k &= 0, x_{k0}x_{k1}x_{k2}... \\ &\vdots \end{aligned}$$

Vamos construir agora um número real $x \in I$, diferente de todos os elementos de $I^{'}$ através da seguinte representação decimal: $0, a_0a_1a_2a_3...$ onde, $1 \leq a_n \leq 8$ e $a_n \neq x_{nn}, \forall n \in \mathbb{N}$. Pela correspondência bijetora estabelecida acima entre números reais e representações decimais sem infinitos noves, a representação decimal $0, a_0a_1a_2a_3...$ corresponde a um único número real de I que é diferente de todos os elementos de $I^{'}$. Como queríamos demonstrar. □

Teorema 4.25. *O conjunto dos números reais é não enumerável.*

Demonstração. Como $I = (0, 1)$ é não enumerável, então pela Proposição 1.19, $\mathbb{R}$ não pode ser enumerável. □

4.2 Construção por Sequências de Cauchy

Nesta seção, realizaremos uma construção alternativa do conjunto dos números reais. Esta se dará por meio de uma relação de equivalência envolvendo sequências de Cauchy em $\mathbb{Q}$.

4.2.1 Classes de Equivalência

Nesta subseção, definiremos classes de equivalência para as sequências de Cauchy que trabalhamos no nosso estudo dos números racionais. Gostaríamos de lembrar que a definição, juntamente com todas as propriedades, de módulo, utilizadas a seguir, foi estabelecida na construção de $\mathbb{Q}$.

Definição 4.18. Sejam (x_n) e (y_n) duas sequências de Cauchy de números racionais. Dizemos que (x_n) e (y_n) são equivalentes, e denotamos por $(x_n) \sim (y_n)$, se $\lim_{n\to\infty} |x_n - y_n| = 0$.

A relação da Definição 4.18 é de equivalência como mostra a seguinte proposição.

Proposição 4.24. *Se (x_n), (y_n) e (z_n) são sequências de Cauchy de números racionais e $\sim$ como na Definição* 4.18. *Então, são válidas as seguintes propriedades:*

i) [*Reflexividade*]*:* $(x_n) \sim (x_n)$*;*

ii) [*Simetria*]*:* $(x_n) \sim (y_n) \Leftrightarrow (y_n) \sim (x_n)$*;*

iii) [*Transitividade*]*:* $(x_n) \sim (y_n)$ *e* $(y_n) \sim (z_n) \Rightarrow (x_n) \sim (z_n)$.

Demonstração. **i)** É fácil ver que $(x_n) \sim (x_n)$, pois $|x_n - x_n| = 0 \to 0$.

ii) Note que $(x_n) \sim (y_n) \Leftrightarrow |x_n - y_n| \to 0 \Leftrightarrow |y_n - x_n| \to 0 \Leftrightarrow (y_n) \sim (x_n)$.

iii) $(x_n) \sim (y_n)$ e $(y_n) \sim (z_n) \Rightarrow |x_n - y_n| \to 0$ e $|y_n - z_n| \to 0$. Mas,

$$|x_n - z_n| = |x_n - y_n + y_n - z_n| \leq |x_n - y_n| + |y_n - z_n|, \forall n \in \mathbb{N}^*.$$

Como $|x_n - y_n| \to 0$ e $|y_n - z_n| \to 0$, pelo Teorema 3.20, então $|x_n - z_n| \to 0$. Donde, $(x_n) \sim (z_n)$.

□

Através da relação de equivalência, dada acima, podemos definir o que significa classe de equivalência de sequências de Cauchy.

Definição 4.19. Seja (x_n) uma sequência de Cauchy de números racionais. Designaremos por $[x_n]$ o conjunto de todas as sequências equivalentes a (x_n), isto é,

$$[x_n] = \{(y_n) \subseteq \mathbb{Q}/(y_n) \sim (x_n)\}.$$

Denotaremos por $\mathbb{R}$ o conjunto $\{[x_n]/(x_n) \subseteq \mathbb{Q}$ é de Cauchy$\}$.

Vejamos uma maneira canônica de verificar quando duas classes de equivalência são iguais em $\mathbb{R}$.

Proposição 4.25. *Sejam* $[x_n]$ *e* $[y_n] \in \mathbb{R}$. *Então,* $[x_n] = [y_n] \Leftrightarrow (x_n) \sim (y_n)$.

Demonstração. ($\Rightarrow$) Com efeito, se $[x_n] = [y_n]$, então

$$(x_n) \in [x_n] = [y_n],$$

através da propriedade reflexiva de $\sim$. Consequentemente, $(x_n) \in [y_n]$. Isto nos diz que, $(x_n) \sim (y_n)$.

($\Leftarrow$) Reciprocamente, suponhamos que $(x_n) \sim (y_n)$. Seja $(z_n) \in [x_n]$, então $(z_n) \sim (x_n)$. Por transitividade, concluímos que $(z_n) \sim (y_n)$. Portanto, $(z_n) \in [y_n]$. Isto nos informa que $[x_n] \subseteq [y_n]$. Agora considere que $(w_n) \in [y_n]$. Assim sendo, $(w_n) \sim (y_n)$. Como $(x_n) \sim (y_n)$, então $(y_n) \sim (x_n)$ (por simetria). Dessa forma, $(w_n) \sim (x_n)$. Logo, $(w_n) \in [x_n]$. Portanto, $[y_n] \subseteq [x_n]$ (por transitividade). Por fim, $[x_n] = [y_n]$. □

Adotaremos, a seguir, uma maneira mais simples de denotar classes de sequências de Cauchy convergentes em $\mathbb{Q}$.

Seja (x_n) uma sequência de Cauchy convergente em $\mathbb{Q}$, digamos $\lim_{n\to\infty} x_n = a \in \mathbb{Q}$. Neste caso, obtemos $[a] = [x_n]$; desde que

$$\lim_{n\to\infty} |x_n - a| = 0.$$

4.2.2 Relação de Ordem em $\mathbb{R}$

Nesta subseção, trataremos de definir o que significa um elemento de $\mathbb{R}$ ser menor do que ou igual a outro. Comecemos com a definição de quando um elemento de $\mathbb{R}$ é maior do que $[0]$.

Definição 4.20. Seja $[x_n] \in \mathbb{R}$. Dizemos que $[x_n]$ é maior do que $[0]$, e denotamos $[x_n] > [0]$, se existem $d \in \mathbb{Q}_+^*$ e $n_0 \in \mathbb{N}^*$ tais que, para todo $n \in \mathbb{N}^*$, tem-se que $n \geq n_0 \Rightarrow x_n > d$.

A seguir estabelecemos a definição do que significa um elemento de $\mathbb{R}$ ser menor do que $[0]$.

Definição 4.21. Seja $[x_n] \in \mathbb{R}$. Dizemos que $[x_n]$ é menor do que $[0]$, e denotamos $[x_n] < [0]$, se existem $d \in \mathbb{Q}_+^*$ e $n_0 \in \mathbb{N}^*$ tais que, para todo $n \in \mathbb{N}$, tem-se que $n \geq n_0 \Rightarrow x_n < -d$.

Agora, estamos prontos para definir quando um elemento de $\mathbb{R}$ é menor do que outro.

Definição 4.22. Sejam $[x_n], [y_n] \in \mathbb{R}$. Dizemos que $[x_n]$ é maior do que $[y_n]$, e indicamos por $[x_n] > [y_n]$, se $[x_n - y_n] > [0]$. Também definimos que $[x_n]$ é menor do que $[y_n]$, e indicamos por $[x_n] < [y_n]$, se $[y_n - x_n] > [0]$.

A relação $<$ está bem definida, ou seja, as classes de equivalência que estão sendo comparadas independem dos seus representantes.

Proposição 4.26. *Sejam $[x_n]$, $[y_n]$, $[z_n]$ e $[w_n] \in \mathbb{R}$. Se $[x_n] = [z_n]$ e $[y_n] = [w_n]$, então*

$$[x_n] < [y_n] \Rightarrow [z_n] < [w_n].$$

Demonstração. Como $[y_n] > [x_n]$, então $[y_n - x_n] > [0]$. Daí, existem $d \in \mathbb{Q}_+^*$ e $n_1 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow y_n - x_n > d.$$

Por outro lado, $(x_n) \sim (z_n)$ e $(y_n) \sim (w_n)$ (pois, $[x_n] = [z_n]$ e $[y_n] = [w_n]$) nos diz que

$$\lim_{n\to\infty} |x_n - z_n| = 0 \text{ e } \lim_{n\to\infty} |y_n - w_n| = 0.$$

Assim sendo, existem n_2 e n_3 em $\mathbb{N}^*$ tais que

$$n \geq n_2 \Rightarrow |x_n - z_n| < \frac{d}{4} \text{ e } n \geq n_3 \Rightarrow |w_n - y_n| < \frac{d}{4}.$$

Seja $n_0 = \max\{n_1, n_2, n_3\} \in \mathbb{N}^*$. Deste modo, chegamos a

$$n \geq n_0 \Rightarrow -\frac{d}{2} < x_n - z_n + w_n - y_n \text{ e } x_n - y_n < -d.$$

Dessa forma, inferimoes que

$$n \geq n_0 \Rightarrow -\frac{d}{2} < w_n - z_n - d.$$

Logo, adicionando d à desigualdade acima, chegamos a

$$n \geq n_0 \Rightarrow \frac{d}{2} < w_n - z_n.$$

Donde, $[z_n] < [w_n]$, uma vez que $\frac{d}{2} \in \mathbb{Q}_+^*$. □

Proposição 4.27 (Tricotomia)**.** *Sejam* $[x_n], [y_n] \in \mathbb{R}$*. Então, apenas uma das três possibilidades pode ocorrer:* $[x_n] < [y_n]$*, ou* $[x_n] = [y_n]$*, ou* $[x_n] > [y_n]$*.*

Demonstração. Vamos mostrar inicialmente que pelo menos uma das três opções ocorre. De fato, dados $[x_n]$ e $[y_n] \in \mathbb{R}$ ou $[x_n] = [y_n]$, ou $[x_n] \neq [y_n]$. Caso valha a igualdade, então nada há a verificar. Caso contrário, temos que $[x_n]$ e $[y_n]$ não são equivalentes, via relação de equivalência $\sim$. Daí $\lim\limits_{n\to\infty} |x_n - y_n| \neq 0$. Logo, $\exists \varepsilon \in \mathbb{Q}_+^*$ tal que para todo $n \in \mathbb{N}^*$, podemos encontrar $m_n \in \mathbb{N}$, com $m_n \geq n$, que satisfaz

$$|x_{m_n} - y_{m_n}| \geq \varepsilon.$$

Como (x_n) e (y_n) são sequências de Cauchy de números racionais, então $\exists n_0 \in \mathbb{N}^*$ tal que

$$|x_n - x_m| < \frac{\varepsilon}{4} \text{ e } |y_n - y_m| < \frac{\varepsilon}{4}, \forall n, m \geq n_0.$$

Sendo $m_{n_0} \geq n_0$, chegamos a

$$|x_n - x_{m_{n_0}}| < \frac{\varepsilon}{4} \text{ e } |y_n - y_{m_{n_0}}| < \frac{\varepsilon}{4}, \forall n \geq n_0.$$

Por outro lado, $x_{m_{n_0}} - y_{m_{n_0}} \geq \varepsilon$ ou $x_{m_{n_0}} - y_{m_{n_0}} \leq -\varepsilon$.

i) Considere que $x_{m_{n_0}} - y_{m_{n_0}} \geq \varepsilon$. Como, $x_n - x_{m_{n_0}} > -\frac{\varepsilon}{4}, \forall n \geq n_0$, então

$$x_n > x_{m_{n_0}} - \frac{\varepsilon}{4}, \forall n \geq n_0.$$

Analogamente, temos que

$$-y_n > -y_{m_{n_0}} - \frac{\varepsilon}{4}, \forall n \geq n_0.$$

Dessa forma, concluímos que

$$x_n - y_n > x_{m_{n_0}} - \frac{\varepsilon}{4} - y_{m_{n_0}} - \frac{\varepsilon}{4} = (x_{m_{n_0}} - y_{m_{n_0}}) - \frac{\varepsilon}{2} \geq \varepsilon - \frac{\varepsilon}{2} = \frac{\varepsilon}{2}, \forall n \geq n_0.$$

Donde concluímos que $x_n - y_n > \frac{\varepsilon}{2}, \forall n \geq n_0$. Isto nos diz que $[x_n] > [y_n]$.

ii) Considere que $x_{m_{n_0}} - y_{m_{n_0}} \leq -\varepsilon$. Como $x_n - x_{m_{n_0}} < \frac{\varepsilon}{4}, \forall n \geq n_0$, então

$$x_n < x_{m_{n_0}} + \frac{\varepsilon}{4}, \forall n \geq n_0.$$

Dessa mesma forma, encontramos

$$-y_n < -y_{m_{n_0}} + \frac{\varepsilon}{4}, \forall n \geq n_0.$$

Daí,

$$x_n - y_n < x_{m_{n_0}} + \frac{\varepsilon}{4} - y_{m_{n_0}} + \frac{\varepsilon}{4} = (x_{m_{n_0}} - y_{m_{n_0}}) + \frac{\varepsilon}{2} \leq -\varepsilon + \frac{\varepsilon}{2} = -\frac{\varepsilon}{2}, \forall n \geq n_0.$$

Donde concluímos que $x_n - y_n < -\frac{\varepsilon}{2}, \forall n \geq n_0$. Isto significa que $[x_n] < [y_n]$.

Assim, se $[x_n] \neq [y_n]$, deve ocorrer $[x_n] < [y_n]$ ou $[x_n] > [y_n]$.

Provaremos agora que $[x_n] \neq [y_n]$, $[x_n] < [y_n]$ e $[x_n] > [y_n]$ não podem ocorrer simultaneamente.

Suponhamos que $[x_n] = [y_n]$ e $[x_n] > [y_n]$ ocorram simultaneamente. De $[y_n] < [x_n]$, existem $d \in \mathbb{Q}_+^*$ e $n_1 \in \mathbb{N}^*$ tais que para todo $n \in \mathbb{N}^*$ com $n \geq n_1$ tem-se $x_n - y_n > d$. Por outro lado, temos também que $[x_n] = [y_n]$ então $\lim_{n\to\infty} |x_n - y_n| = 0$. Dessa forma, $\exists n_2 \in \mathbb{N}^*$ tal que para todo $n \in \mathbb{N}$ com $n \geq n_2$ tem-se $|x_n - y_n| < d$. O que nos leva a concluir que $x_n - y_n < d$. Tomando $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$, podemos inferir, para todo $n \geq n_0$, que $x_n - y_n > d$ e $x_n - y_n < d$. Pela Tricotomia em $\mathbb{Q}$ as desigualdades não podem ser satisfeitas.

Suponhamos agora que $[x_n] = [y_n]$ e $[x_n] < [y_n]$ sejam válidas. De $[y_n] > [x_n]$, existem $d_1 \in \mathbb{Q}_+^*$ e $n_3 \in \mathbb{N}^*$ tais que para todo $n \in \mathbb{N}$, com $n \geq n_3$, $y_n - x_n > d_1$. Por outro lado, temos também que $[x_n] = [y_n]$ então $\lim_{n\to\infty} |x_n - y_n| = 0$. Dessa forma, $\exists n_4 \in \mathbb{N}^*$ para todo $n \in \mathbb{N}$, com $n \geq n_4$, tem-se $|y_n - x_n| < d_1$. Assim sendo, $y_n - x_n < d_1$. Assumindo $n_5 = \max\{n_3, n_4\} \in \mathbb{N}^*$, podemos concluir, para todo $n \geq n_5$, que

$$y_n - x_n > d_1 \text{ e } y_n - x_n < d_1.$$

Pela Tricotomia em $\mathbb{Q}$ as desigualdades acima não podem ser satisfeitas.

Suponhamos agora que $[x_n] < [y_n]$ e $[x_n] > [y_n]$ sejam válidas. Por $[x_n] < [y_n]$, sabemos que existem $d_2 \in \mathbb{Q}_+^*$ e $n_6 \in \mathbb{N}^*$ tais que $n \geq n_6 \Rightarrow y_n - x_n > d_2$. Por outro lado, por $[x_n] > [y_n]$, existem $d_3 \in \mathbb{Q}_+^*$ e $n_7 \in \mathbb{N}$ tais que $n \geq n_7 \Rightarrow x_n - y_n > d_3$. Tomando $n_8 = \max\{n_6, n_7\} \in \mathbb{N}^*$, obtemos

$$n \geq n_8 \Rightarrow y_n - x_n + x_n - y_n > d_2 + d_3 \Rightarrow 0 > d_2 + d_3.$$

Isso é uma contradição, já que d_2 e $d_3 \in \mathbb{Q}_+^*$.

Por fim, a prova do teorema em questão está completa. □

Permita-nos provar que $\leq$ é uma relação de ordem em $\mathbb{R}$. Comecemos com a antissimetria.

Proposição 4.28 (Antissimetria)**.** *Sejam* $[x_n]$ *e* $[y_n] \in \mathbb{R}$. *Se* $[x_n] \leq [y_n]$ *e* $[y_n] \leq [x_n]$, *então* $[x_n] = [y_n]$.

Demonstração. Suponha que $[x_n] \neq [y_n]$, então, por hipótese, temos que $[x_n] < [y_n]$ e $[x_n] > [y_n]$. Mas, isto é uma contradição de acordo com a tricotomia em $\mathbb{R}$. Logo, $[x_n] = [y_n]$. □

O resultado abaixo mostra que $\leq$ é uma relação reflexiva.

Proposição 4.29 (Reflexividade)**.** *Seja* $[x_n] \in \mathbb{R}$*, então* $[x_n] \leq [x_n]$*.*

Demonstração. Note que

$$[x_n] \leq [x_n] \Leftrightarrow [x_n - x_n] \geq [0] \Leftrightarrow [0] \geq [0].$$

Como queríamos demonstrar. □

Com a finalidade de provar que $\leq$ é uma relação de ordem, resta-nos estabelecer a transitividade desta relação.

Proposição 4.30 (Transitividade)**.** *Sejam* $[x_n]$*,* $[y_n]$ *e* $[z_n] \in \mathbb{R}$*. Se* $[x_n] \leq [y_n]$ *e* $[y_n] \leq [z_n]$*, então* $[x_n] \leq [z_n]$*.*

Demonstração. Primeiramente, note que se $[x_n] = [y_n]$ e $[y_n] = [z_n]$, então $[x_n] = [z_n]$ (por igualdade de conjuntos).

Agora considere que $[x_n] = [y_n]$ e $[y_n] < [z_n]$. Vamos provar que $[x_n] < [z_n]$. Por definição, temos que existem $d \in \mathbb{Q}_+^*$ e $n_0 \in \mathbb{N}^*$ tais que

$$n \geq n_0 \Rightarrow z_n - y_n > d.$$

Além disso, existe $n_1 \in \mathbb{N}^*$ tal que $n \geq n_0 \Rightarrow |y_n - x_n| < \frac{d}{2} \Rightarrow y_n - x_n > -\frac{d}{2}$ (pois $\lim_{n\to\infty} |x_n - y_n| = 0$). Logo, somando estas duas últimas desigualdades, chegamos a

$$n \geq n_0 \Rightarrow z_n - x_n > \frac{d}{2}.$$

Isto nos diz que $[x_n] < [z_n]$. O caso $[x_n] < [y_n]$ e $[y_n] = [z_n]$ é análogo.

Agora, assuma que $[x_n] < [y_n]$ e $[y_n] < [z_n]$.

Como $[x_n] < [y_n]$, então existem $d_1 \in \mathbb{Q}_+^*$ e $n_1 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow y_n - x_n > d_1.$$

Por outro lado, como $[y_n] < [z_n]$, então existem $d_2 \in \mathbb{Q}_+^*$ e $n_2 \in \mathbb{N}^*$ tais que

$$n \geq n_2 \Rightarrow z_n - y_n > d_2.$$

Tomando $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$, tem-se que

$$n \geq n_0 \Rightarrow y_n - x_n + z_n - y_n > d_1 + d_2 \Rightarrow z_n - x_n > d_1 + d_2.$$

Como $d_1 + d_2 \in \mathbb{Q}_+^*$, então $[x_n] < [z_n]$. Isto completa a prova da proposição em questão. □

É importante destacar que na prova da Proposição 4.30, garantimos que no enunciado deste resultado podemos substituir $\leq$ por $<$.

A partir de agora, podemos afirmar que $\leq$ é uma relação de ordem. Mais ainda é verdade, $\leq$ é uma relação de ordem total.

Proposição 4.31. *Sejam* $[x_n]$ *e* $[y_n] \in \mathbb{R}$. *Então,* $[x_n] \leq [y_n]$ *ou* $[y_n] \leq [x_n]$.

Demonstração. Segue diretamente da Tricotomia em $\mathbb{R}$. □

Desta forma, verificamos que a relação $\leq$ é de ordem total.

Para concluir esta subseção, provaremos que se uma sequência de números racionais não converge para zero, então esta é equivalente a uma outra sequência que possui todos os seus termos não nulos.

Proposição 4.32. *Se* (x_n) *é um sequência de Cauchy de números racionais tal que* $\lim_{n\to\infty} x_n \neq 0$, *então existe uma sequência de Cauchy em* $\mathbb{Q}$ *tal que* $[x_n] = [y_n]$ *e* $y_n \neq 0, \forall n \in \mathbb{N}^*$.

Demonstração. Note que

$$[x_n] = [0] \Leftrightarrow \lim_{n\to\infty} |x_n - 0| = 0 \Leftrightarrow \lim_{n\to\infty} x_n = 0.$$

Como $\lim_{n\to\infty} x_n \neq 0$, temos que $[x_n] > [0]$ ou $[x_n] < [0]$ (tricotomia).

Caso $[x_n] > 0$, temos que existem $d_1 \in \mathbb{Q}_+^*$ e $n_1 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow x_n > d_1.$$

Isto significa que todos os termos $x_{n_1}, x_{n_1+1}, x_{n_1+2}, ...$ são maiores do que d_1. Assim as sequências (x_n) e $(y_n) = (d_1, ..., d_1, x_{n_1}, x_{n_1+1}, x_{n_1+2}, ...)$ são equivalentes (note que todos os termos desta sequência são positivos), visto que para todo $n \geq n_1$ todos os termos $x_n - y_n$ são iguais a zero garantindo então $\lim_{n\to\infty} |x_n - y_n| = 0$. Donde $(x_n) \sim (y_n)$. Consequentemente, $[x_n] = [y_n]$.

Por outro lado, se $[x_n] < [0]$, então existem $d_2 \in \mathbb{Q}_+^*$ e $n_2 \in \mathbb{N}^*$ tais que

$$n \geq n_2 \Rightarrow x_n < -d_2.$$

Assim, todos os termos $x_{n_2}, x_{n_2+1}, x_{n_2+2}, ...$ são menores que $-d_2$. Assim as sequências (x_n) e $(y_n) = (-d_2, ..., -d_2, x_{n_2}, x_{n_2+1}, x_{n_2+2}, ...)$ são equivalentes (note que todos os termos desta sequência são

negativos), visto que para todo $n \geq n_2$ todos os termos $x_n - y_n$ são iguais a zero garantindo então $\lim_{n\to\infty} |x_n - y_n| = 0$. Logo, $(x_n) \sim (y_n)$. Por conseguinte, $[x_n] = [y_n]$.

Nos dois casos (y_n) é constituída de termos todos diferentes de zero. Como queríamos demonstrar. □

Obs 4.1. Note que provamos acima que se $[x_n] > 0$ (respectivamente, < 0), então $[x_n] = [y_n]$, onde $y_n > 0$ (respectivamente, < 0), para todo $n \in \mathbb{N}^*$.

4.2.3 Operações Elementares em $\mathbb{R}$

Nesta subseção, estabeleceremos, precisamente, como definir a adição e a multiplicação entre dois elementos de $\mathbb{R}$. Sendo assim, permita-nos começarmos pela adição.

Definição 4.23. Sejam $[x_n]$ e $[y_n] \in \mathbb{R}$. A adição de $[x_n]$ com $[y_n]$, indicada por $[x_n] + [y_n]$, é definida por $[x_n] + [y_n] := [x_n + y_n]$.

Mostremos a seguir que a operação de adição está bem definida, ou seja, não depende da escolha dos elementos que representam cada parcela desta operação.

Proposição 4.33. *Sejam* $[x_n]$, $[y_n]$, $[z_n]$, $[w_n] \in \mathbb{R}$. *Se* $[x_n] = [z_n]$ *e* $[y_n] = [w_n]$, *então* $[x_n]+[y_n] = [z_n] + [w_n]$.

Demonstração. Por hipótese, $(x_n) \sim (z_n)$ e $(y_n) \sim (w_n)$ (pois, $[x_n] = [z_n]$ e $[y_n] = [w_n]$), isto significa que $\lim_{n\to\infty} |x_n - z_n| = 0$ e $\lim_{n\to\infty} |y_n - w_n| = 0$. Então, dado $\varepsilon \in \mathbb{Q}_+^*$ existem $n_1, n_2 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow |x_n - z_n| < \frac{\varepsilon}{2} \text{ e } n \geq n_2 \Rightarrow |y_n - w_n| < \frac{\varepsilon}{2}.$$

Logo, chegamos a

$$n \geq n_1 \Rightarrow -\frac{\varepsilon}{2} < x_n - z_n < \frac{\varepsilon}{2} \text{ e } n \geq n_2 \Rightarrow -\frac{\varepsilon}{2} < y_n - w_n < \frac{\varepsilon}{2}.$$

Seja $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$. Então,

$$n \geq n_0 \Rightarrow -\varepsilon < (x_n + y_n) - (z_n + w_n) < \varepsilon.$$

Logo, $\lim_{n\to\infty} |(x_n + y_n) - (z_n + w_n)| = 0$. Portanto, $(x_n + y_n) \sim (z_n + w_n)$. Consequentemente, $[x_n + y_n] = [z_n + w_n]$. Isto significa que $[x_n] + [y_n] = [z_n] + [w_n]$. □

Abaixo, mostraremos que é sempre possível somar qualquer elemento de $\mathbb{R}$ a dois membros de uma igualdade em $\mathbb{R}$.

Proposição 4.34. *Sejam* $[x_n]$, $[y_n]$ *e* $[z_n] \in \mathbb{R}$. *Então,* $[x_n] = [y_n] \Rightarrow [x_n] + [z_n] = [y_n] + [z_n]$.

Demonstração. Como $[x_n] = [y_n]$, então $\lim_{n\to\infty} |x_n - y_n| = 0$. Então, dado $\varepsilon \in \mathbb{Q}_+^*$, existe $n_0 \in \mathbb{N}^*$ tal que

$$n \geq n_0 \Rightarrow |x_n - y_n| < \varepsilon.$$

Logo,

$$n \geq n_0 \Rightarrow |(x_n + z_n) - (y_n + z_n)| = |x_n - y_n| < \varepsilon.$$

Isto nos diz que $\lim_{n\to\infty} |(x_n + z_n) - (y_n + z_n)| = 0$. Assim, $(x_n + z_n) \sim (y_n + z_n)$. Dessa forma, inferimos que $[x_n] + [z_n] = [y_n] + [z_n]$. □

A partir de agora, vamos provar as propriedades aritméticas elementares da adição em $\mathbb{R}$ tais como: associatividade, comutatividade, elementos neutro e simétrico, compatibilidade entre $\leq$ e $\cdot$.

Comecemos com a associatividade.

Teorema 4.26 (Associatividade)**.** *Sejam* $[x_n]$, $[y_n]$ *e* $[z_n] \in \mathbb{R}$. *Então,*

$$[x_n] + ([y_n] + [z_n]) = ([x_n] + [y_n]) + [z_n].$$

Demonstração. Como a adição entre números racionais satisfaz a propriedade associativa e (x_n), (y_n) e (z_n) são sequências de números racionais, então

$$\begin{aligned}[x_n] + ([y_n] + [z_n]) &= [x_n] + [y_n + z_n] = [x_n + (y_n + z_n)] \\ &= [(x_n + y_n) + z_n] = [x_n + y_n] + [z_n] \\ &= ([x_n] + [y_n]) + [z_n].\end{aligned}$$

Isto prova o teorema em questão. □

Teorema 4.27 (Comutatividade)**.** *Sejam* $[x_n]$, $[y_n] \in \mathbb{R}$. *Então,* $[x_n] + [y_n] = [y_n] + [x_n]$.

Demonstração. É fácil checar que

$$[x_n] + [y_n] = [x_n + y_n] = [y_n + x_n] = [y_n] + [x_n].$$

Isto completa a prova o teorema em questão. □

Afirmamos que o único elemento neutro da adição em $\mathbb{R}$ é $[0]$.

Teorema 4.28 (Elemento Neutro)**.** *Seja $[x_n] \in \mathbb{R}$. Então, $[x_n] + [0] = [x_n]$. Além disso, $[0]$ é o único elemento que satisfaz esta igualdade.*

Demonstração. Para mostrar a existência de elemento neutro basta tomar $[0]$ como a classe de equivalência da sequência em que todos os seus termos são iguais a $0 \in \mathbb{Q}$. Tal sequência é de fato de Cauchy pois converge para $0 \in \mathbb{Q}$. Além disso,

$$[x_n] + [0] = [x_n + 0] = [x_n].$$

Suponhamos que $[y_n] \in \mathbb{R}$ é tal que $[x_n] + [y_n] = [x_n]$, para todo $[x_n] \in \mathbb{R}$. Então, pela comutatividade, chegamos a

$$[0] = [0] + [y_n] = [y_n] + [0] = [y_n].$$

Portanto, $[0] = [y_n]$. □

Chequemos a existência única de um simétrico para cada elemento de $\mathbb{R}$ dado.

Teorema 4.29 (Simétrico)**.** *Seja $[x_n] \in \mathbb{R}$. Então, $[x_n] + [-x_n] = [0]$. Além disso, $[-x_n]$ é o único elemento que satisfaz esta igualdade.*

Demonstração. Seja $[x_n] \in \mathbb{R}$, defina $[y_n] = [-x_n]$, daí temos que $[y_n] \in \mathbb{R}$. De fato, $(-x_n)$ é uma sequência de Cauchy de números racionais, pois como x_n é um número racional para todo $n \in \mathbb{N}^*$ então $-x_n$ também o é. Além disso, então dado $\varepsilon \in \mathbb{Q}_+^*$ existe $n_0 \in \mathbb{N}^*$ tal que

$$m, n \geq n_0 \Rightarrow |x_n - x_m| < \varepsilon.$$

Por outro lado, dados $m, n \in \mathbb{N}, m, n \geq n_0$,

$$|-x_n - (-x_m)| = |-x_n + x_m| = |x_n - x_m| < \varepsilon.$$

Assim, $(-x_n)$ é uma sequência de Cauchy de números racionais. Portanto, $[y_n] \in \mathbb{R}$. Além disso, temos que

$$[x_n] + [-x_n] = [x_n + (-x_n)] = [0].$$

Agora, suponhamos que existe $[z_n] \in \mathbb{R}$ tal que $[x_n] + [z_n] = [0]$.. Portanto, por associatividade e comutatividade, obtemos

$$\begin{aligned}
[z_n] &= [z_n] + [0] = [z_n] + ([x_n] + [-x_n]) \\
&= ([z_n] + [x_n]) + [-x_n] = ([x_n] + [z_n]) + [-x_n] \\
&= [0] + [-x_n] = [-x_n].
\end{aligned}$$

□

Neste ponto, poderíamos definir a subtração entre dois elementos de $\mathbb{R}$ da seguinte forma:

$$[x_n] - [y_n] := [x_n] + [-y_n], \forall [x_n], [y_n] \in \mathbb{R}.$$

Quanto a compatibilidade entre a relação $\leq$ e a operação $+$, temos o seguinte resultado.

Teorema 4.30. *Sejam* $[x_n]$, $[y_n]$ *e* $[z_n] \in \mathbb{R}$. *Então,*

$$[x_n] \leq [y_n] \Leftrightarrow [x_n] + [z_n] \leq [y_n] + [z_n].$$

Demonstração. ($\Rightarrow$) Suponha que $[x_n] < [y_n]$, então existem $d \in \mathbb{Q}_+^*$ e $n_1 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow x_n - y_n > -d \Rightarrow x_n > y_n - d.$$

Observemos que para cada $n \in \mathbb{N}^*$, x_n, y_n e z_n são números racionais e vale a compatibilidade da adição em relação a ordem. Logo, para todo $n \geq n_1$, obtemos

$$x_n > y_n - d \Rightarrow x_n + z_n > y_n + z_n - d \Rightarrow (x_n + z_n) - (y_n + z_n) > -d.$$

Portanto, $[x_n] < [y_n] \Rightarrow [x_n] + [z_n] < [y_n] + [z_n]$.

Por outro lado, se $[x_n] = [y_n]$, então $[x_n] + [z_n] = [y_n] + [z_n]$ (ver Proposição 4.34).

($\Leftarrow$) Agora suponha que $[x_n] + [z_n] \leq [y_n] + [z_n]$. Consequentemente, adicionando o elemento $[-z_n] \in \mathbb{R}$ a esta desigualdade (pelo que foi feito acima), chegamos a

$$([x_n] + [z_n]) + [-z_n] \leq ([y_n] + [z_n]) + [-z_n].$$

Pela associatividade, encontramos

$$[x_n] + ([z_n] + [-z_n]) \leq [y_n] + ([z_n] + [-z_n]).$$

Desta forma, encontramos

$$[x_n] + [0] \leq [y_n] + [0].$$

Por fim, $[x_n] \leq [y_n]$. □

Observe que na prova do Teorema 4.30, garantimos que

$$[x_n] < [y_n] \Rightarrow [x_n] + [z_n] < [y_n] + [z_n],$$

para todo $[x_n], [y_n], [z_n] \in \mathbb{R}$.

A seguir provaremos a lei do cancelamento para a adição em $\mathbb{R}$.

Teorema 4.31 (Lei do Cancelamento)**.** *Sejam* $[x_n]$, $[y_n]$ *e* $[z_n] \in \mathbb{R}$. *Então,*

$$[x_n] + [z_n] = [y_n] + [z_n] \Rightarrow [x_n] = [y_n].$$

Demonstração. Suponha que $[x_n] + [z_n] = [y_n] + [z_n]$. Consequentemente, adicionando o elemento $[-z_n] \in \mathbb{R}$ a esta igualdade (pela Proposição 4.34), chegamos a

$$([x_n] + [z_n]) + [-z_n] = ([y_n] + [z_n]) + [-z_n].$$

Pela associatividade, encontramos

$$[x_n] + ([z_n] + [-z_n]) = [y_n] + ([z_n] + [-z_n]).$$

Desta forma, encontramos

$$[x_n] + [0] = [y_n] + [0].$$

Por fim, $[x_n] = [y_n]$. □

Agora, definiremos a operação de multiplicação no conjunto $\mathbb{R}$. Além disso, provaremos propriedadades aritméticas elementares análogas as obtidas para a adição.

Definição 4.24. Sejam $[x_n]$ e $[y_n] \in \mathbb{R}$. A multiplicação de $[x_n]$ por $[y_n]$, indicada por $[x_n] \cdot [y_n]$, é é dada por $[x_n] \cdot [y_n] = [x_n y_n]$.

Veremos agora que a operação de multiplicação estabelecida acima está bem definida.

Proposição 4.35. *Sejam* $[x_n]$, $[y_n]$, $[z_n]$ *e* $[w_n] \in \mathbb{R}$. *Se* $[x_n] = [z_n]$ *e* $[y_n] = [w_n]$, *então* $[x_n y_n] = [z_n w_n]$.

Demonstração. Notemos primeiramente que

$$\begin{aligned} |x_n y_n - z_n w_n| &= |x_n y_n - x_n w_n + x_n w_n - z_n w_n| \\ &= |x_n(y_n - w_n) + w_n(x_n - z_n)| \\ &\leq |x_n||y_n - w_n| + |w_n||x_n - z_n|, \forall n \in \mathbb{N}^*. \end{aligned}$$

Como (x_n), (w_n) são limitadas, já que ambas são sequências de Cauchy de números racionais, temos que existem $c, d \in \mathbb{Q}_+^*$ tais que $|x_n| \leq c$ e $|w_n| \leq d$ para todo $n \in \mathbb{N}^*$. Tomando $k = \max\{c, d\} \in \mathbb{Q}_+^*$, então $|x_n| \leq k$ e $|w_n| \leq k$, para todo $n \in \mathbb{N}^*$. E, daí,

$$|x_n y_n - z_n w_n| \leq |x_n||y_n - w_n| + |w_n||x_n - z_n| \leq k|y_n - w_n| + k|x_n - z_n|, \forall n \in \mathbb{N}^*.$$

Por outro lado, como $[x_n] = [z_n]$ e $[y_n] = [w_n]$, temos que $(x_n) \sim (z_n)$ e $(y_n) \sim (w_n)$. Isto significa que $\lim\limits_{n\to\infty} |x_n - z_n| = 0$ e $\lim\limits_{n\to\infty} |y_n - w_n| = 0$. Então, dado $\varepsilon \in \mathbb{Q}_+^*$, existem $n_1, n_2 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow |x_n - z_n| < \frac{\varepsilon}{2k} \text{ e } n \geq n_2 \Rightarrow |y_n - w_n| < \frac{\varepsilon}{2k}.$$

Seja $n_0 = \max\{n_1, n_2\}$, então para todo $n \geq n_0$, tem-se

$$|x_n y_n - z_n w_n| \leq k|y_n - w_n| + k|x_n - z_n| \leq k\frac{\varepsilon}{2k} + k\frac{\varepsilon}{2k} = \varepsilon.$$

Daí, $\lim\limits_{n\to\infty} |x_n y_n - z_n w_n| = 0$. Portanto, $(x_n y_n) \sim (z_n w_n)$. Por fim, $[x_n y_n] = [z_n w_n]$. □

Vejamos a justificativa para podermos multiplicar os dois membros de uma igualdade por qualquer elemento de $\mathbb{R}$.

Proposição 4.36. *Sejam* $[x_n]$, $[y_n]$, $[z_n] \in \mathbb{R}$. *Então,* $[x_n] = [z_n] \Rightarrow [x_n] \cdot [y_n] = [z_n] \cdot [y_n]$.

Demonstração. Como (y_n) é uma sequência de Cauchy de números racionais, então (y_n) é limitada. Assim, $\exists c \in \mathbb{Q}_+^*$ tal que

$$|y_n| \leq c, \forall n \in \mathbb{N}^*.$$

Por outro lado, como $[x_n] = [z_n]$, então $(x_n) \sim (z_n)$. Isto nos diz que $\lim\limits_{n\to\infty} |x_n - z_n| = 0$. Assim sendo, dado $\varepsilon \in \mathbb{Q}_+^*$, $\exists n_0 \in \mathbb{N}^*$ tal que

$$n \geq n_0 \Rightarrow |x_n - z_n| < \tfrac{\varepsilon}{c}.$$

Logo, para todo $n \geq n_0$, conclui-se

$$|x_n y_n - z_n y_n| = |(x_n - z_n)y_n| = |x_n - z_n||y_n| < \frac{\varepsilon}{c} \cdot c = \varepsilon.$$

Portanto,

$$\lim_{n\to\infty} |x_n y_n - z_n y_n| = 0.$$

Isto equivale a dizer que $(x_n y_n) \sim (z_n y_n)$. Por fim, $[x_n] \cdot [y_n] = [z_n] \cdot [y_n]$. □

A partir de agora, vamos provar as propriedades aritméticas elementares para a multiplicação em $\mathbb{R}$ tais como: associatividade, comutatividade, elementos neutro e inverso, compatibilidade entre $\leq$ e $+$.

Comecemos com a associatividade.

Teorema 4.32 (Associatividade)**.** *Sejam* $[x_n]$, $[y_n]$ *e* $[z_n] \in \mathbb{R}$. *Então,*

$$[x_n] \cdot ([y_n] \cdot [z_n]) = ([x_n] \cdot [y_n]) \cdot [z_n].$$

Demonstração. Sabemos que $\mathbb{Q}$ possui a propriedade associativa com relação a multiplicação e como (x_n), (y_n) e (z_n) são sequências de números racionais, então

$$\begin{aligned}[x_n] \cdot ([y_n] \cdot [z_n]) &= [x_n] \cdot [y_n z_n] = [x_n (y_n z_n)] \\ &= [(x_n y_n) z_n] = [x_n y_n] \cdot [z_n] \\ &= ([x_n] \cdot [y_n]) \cdot [z_n].\end{aligned}$$

Como queríamos demonstrar. □

Vamos demonstrar que a multiplicação satisfaz a propriedade comutativa.

Teorema 4.33 (Comutatividade)**.** *Sejam* $[x_n]$, $[y_n] \in \mathbb{R}$. *Então,*

$$[x_n] \cdot [y_n] = [y_n] \cdot [x_n].$$

Demonstração. É fácil checar que

$$[x_n] \cdot [y_n] = [x_n y_n] = [y_n x_n] = [y_n] \cdot [x_n].$$

Isto completa a prova do teorema em questão. □

O único elemento neutro da multiplicação em $\mathbb{R}$ é dado por $[1]$.

Teorema 4.34 (Elemento Neutro)**.** *Seja* $[x_n] \in \mathbb{R}$. *Então,* $[x_n] \cdot [1] = [x_n]$. *Além disso,* $[1]$ *é o único elemento de* $\mathbb{R}$ *que satisfaz esta igualdade.*

Demonstração. Como já discutimos, nocaso do elemento neutro da adição, $[1] \in \mathbb{R}$, de fato. além disso, é fácil ver que

$$[x_n] \cdot [1] = [x_1 \cdot 1] = [x_n].$$

Agora, considere que existe $[y_n] \in \mathbb{R}$ tal que $[x_n] \cdot [y_n] = [x_n]$, para todo $[x_n] \in \mathbb{R}$. Deste modo, podemos escrever

$$[1] = [1] \cdot [y_n] = [1 \cdot y_n] = [y_n].$$

Isto completa a prova do teorema em questão. □

Teorema 4.35 (Inverso)**.** *Seja* $[x_n] \in \mathbb{R}$ *tal que* $[x_n] \neq [0]$*. Então, existe* $[y_n] \in R$ *tal que* $[x_n] \cdot [y_n] = [1]$*. Além disso,* $[y_n]$ *é o único elemento de* $\mathbb{R}$ *que satisfaz esta igualdade.*

Demonstração. Como $[x_n] \in \mathbb{R}$, com $[x_n] \neq [0]$. Então, pela Proposição 4.32, temos a garantia que a sequência (x_n) representativa de $[x_n]$ pode ser tomada de modo que todos os seus termos sejam diferentes de zero. Assim, a sequência $(y_n) = \left(\dfrac{1}{x_n}\right)$ é também uma sequência de Cauchy em $\mathbb{Q}$. Logo, $[y_n] = [\frac{1}{x_n}] \in \mathbb{R}$. Dessa forma, inferimos que

$$[x_n] \cdot \left[\frac{1}{x_n}\right] = \left[x_n \cdot \frac{1}{x_n}\right] = [1].$$

Agora, suponha que existe $[z_n] \in \mathbb{R}$ tal que $[x_n] \cdot [z_n] = [1]$. Consequentemente,

$$\begin{aligned}[y_n] &= [y_n] \cdot [1] = [y_n] \cdot ([x_n] \cdot [z_n]) \\ &= ([y_n] \cdot [x_n]) \cdot [z_n] = ([x_n] \cdot [y_n]) \cdot [z_n] \\ &= [1] \cdot [z_n] = [z_n].\end{aligned}$$

Isto finaliza a prova do teorema em questão. □

Definição 4.25. Designaremos por $[x_n^{-1}]$ o elemento $[y_n]$ encontrado na prova do Teorema 4.35.

É importante ressaltar aqui que se $[x_n] > [0]$, então pela Observação 4.1, podemos assumir que $x_n > 0$, para todo $n \in \mathbb{N}^*$. Como (x_n) é uma sequência de Cauchy em $\mathbb{Q}$, temos que existe $k \in \mathbb{Q}_+^*$ tal que $x_n = |x_n| \leq k$, para todo $n \in \mathbb{N}^*$. Logo, $x_n^{-1} \geq k^{-1}$, para todo $n \in \mathbb{N}^*$. Escolha $d \in \mathbb{Q}$ tal que $0 < d < k^{-1}$. Portanto, $x_n^{-1} > d$, para todo $n \in \mathbb{N}^*$. Isto nos informa que $[x_n^{-1}] > [0]$. Analogamente conseguimos provar que $[x_n] < [0] \Rightarrow [x_n^{-1}] < [0]$.

Neste ponto, poderíamos definir a divisão entre dois elementos de $\mathbb{R}$ da seguinte maneira:

$$[x_n] : [y_n] := [x_n] \cdot [y_n^{-1}],\ \forall [x_n], [y_n] \in \mathbb{R},$$

onde $[y_n] \neq [0]$.

Permita-nos provar a distributividade em $\mathbb{R}$.

Teorema 4.36 (Distributividade)**.** *Sejam* $[x_n], [y_n], [z_n] \in \mathbb{R}$*. Então,*

$$[x_n] \cdot ([y_n] + [z_n]) = [x_n] \cdot [y_n] + [x_n] \cdot [z_n].$$

Demonstração. Este resultado segue das seguintes igualdades:

$$\begin{aligned}[x_n] \cdot ([y_n] + [z_n]) &= [x_n] \cdot [y_n + z_n] = [x_n(y_n + z_n)] \\ &= [x_n y_n + x_n z_n] = [x_n y_n] + [x_n z_n] \\ &= [x_n] \cdot [y_n] + [x_n] \cdot [z_n].\end{aligned}$$

□

Agora, provaremos a compatibilidade existente entre a relação de ordem $\leq$ e a operação de multiplicação em $\mathbb{R}$.

Teorema 4.37. *Sejam* $[x_n]$*,* $[y_n]$ *e* $[z_n] \in \mathbb{R}$*. Então, são válidas as seguintes propriedades:*

i) $[x_n] \leq [y_n]$ *e* $[z_n] > [0] \Leftrightarrow [x_n] \cdot [z_n] \leq [y_n] \cdot [z_n]$*;*

ii) $[x_n] \leq [y_n]$ *e* $[z_n] < [0] \Leftrightarrow [x_n] \cdot [z_n] \geq [y_n] \cdot [z_n]$.

Demonstração. **i)** ($\Rightarrow$) Se $[x_n] = [y_n]$, então, pela Proposição 4.36, concluímos que $[x_n] \cdot [z_n] = [y_n] \cdot [z_n]$.

Considere, então, que $[x_n] < [y_n]$. Daí, existem $d_1 \in \mathbb{Q}_+^*$ e $n_1 \in \mathbb{N}^*$ tais que

$$n \geq n_1 \Rightarrow x_n - y_n < -d_1.$$

Analogamente, como $[z_n] > [0]$, concluímos que existem $d_2 \in \mathbb{Q}_+^*$ e $n_2 \in \mathbb{N}^*$ tais que

$$n \geq n_2 \Rightarrow z_n > d_2.$$

Seja $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$, então para todo $n \in \mathbb{N}^*, n \geq n_0$, temos que

$$x_n z_n - y_n z_n < -d_1 z_n. \tag{4.4}$$

e também

$$z_n d_1 > d_2 d_1. \tag{4.5}$$

Das equações (4.4) e (4.5), inferimos que, para todo $n \in \mathbb{N}^*$, com $n \geq n_0$, chega-se a

$$x_n z_n - y_n z_n < -d_1 z_n < -d_2 \cdot d_1 \Rightarrow x_n z_n - y_n z_n < -d_2 d_1.$$

Como $d_2 d_1 \in \mathbb{Q}_+^*$, então

$$[x_n] \cdot [z_n] < [y_n] \cdot [z_n].$$

($\Leftarrow$) Reciprocamente, assuma que $[x_n] \cdot [z_n] \leq [y_n] \cdot [z_n]$. Como $[z_n] > [0]$, então $[z_n^{-1}] > [0]$. Por usar a ida, chegamos a

$$([x_n] \cdot [z_n]) \cdot [z_n^{-1}] \leq ([y_n] \cdot [z_n]) \cdot [z_n^{-1}].$$

Por associatividade, e a aplicação do elemento neutro, encontramos $[x_n] \leq [y_n]$.

ii) ($\Rightarrow$) Vimos acima que podemos considerar que $[x_n] < [y_n]$. Então, existem $d_3 \in \mathbb{Q}_+^*$ e $n_3 \in \mathbb{N}^*$ tais que

$$n \geq n_3 \Rightarrow x_n - y_n < -d_3.$$

Também temos de $[z_n] < [0]$ que existem $d_4 \in \mathbb{Q}_+^*$ e $n_4 \in \mathbb{N}^*$ tais que

$$n \geq n_4 \Rightarrow z_n < -d_4.$$

Seja $n_5 = \max\{n_3, n_4\} \in \mathbb{N}^*$, então, para todo $n \in \mathbb{N}^*, n \geq n_5$, tem-se que

$$x_n z_n - y_n z_n > -d_3 z_n. \tag{4.6}$$

e também

$$-z_n d_3 > d_3 d_4. \tag{4.7}$$

Das equações (4.6) e (4.7) temos que, para todo $n \in \mathbb{N}^*$, com $n \geq n_5$, chega-se a

$$x_n z_n - y_n z_n > -d_3 z_n > d_3 d_4 \Rightarrow x_n z_n - y_n z_n > d_3 d_4.$$

Como $d_3 d_4 \in \mathbb{Q}_+^*$, então $[x_n] \cdot [z_n] > [y_n] \cdot [z_n]$.

($\Leftarrow$) A recíproca segue os mesmos passos da recíproca do item **i**).

□

Abaixo expomos a lei do cancelamento para a multiplicação em $\mathbb{R}$.

Proposição 4.37. *Sejam* $[x_n]$, $[y_n]$, $[z_n] \in \mathbb{R}$ *com* $[y_n] \neq 0$. *Então,*

$$[x_n] \cdot [y_n] = [z_n] \cdot [y_n] \Rightarrow [x_n] = [z_n].$$

Demonstração. Como $[y_n] \neq 0$, pela Proposição 4.32, temos a garantia que a sequência representativa (y_n) de $[y_n]$ pode ser tomada de modo que todos os seus termos sejam diferentes de zero. Como (y_n) é uma sequência de Cauchy de números racionais temos que $\left(\frac{1}{y_n}\right)$ também o é. Dessa forma, concluímos que $\left(\frac{1}{y_n}\right)$ é limitada. Assim, existe $c \in \mathbb{Q}_+^*$ tal que $|\frac{1}{y_n}| \leq c, \forall n \in \mathbb{N}^*$. Também sabemos que $[x_n] \cdot [y_n] = [z_n] \cdot [y_n]$, ou seja, $\lim\limits_{n\to\infty} |x_n y_n - z_n y_n| = 0$. Daí, dado $\varepsilon \in \mathbb{Q}_+^*$ existe $n_0 \in \mathbb{N}$ tal que

$$n \geq n_0 \Rightarrow |x_n y_n - z_n y_n| < \frac{\varepsilon}{c},$$

Então, para todo $n \geq n_0$, temos que

$$|x_n - z_n| = \left|x_n\Big(y_n\frac{1}{y_n}\Big) - z_n\Big(y_n\frac{1}{y_n}\Big)\right| = |x_n y_n - z_n y_n|\left|\frac{1}{y_n}\right| < \frac{\varepsilon}{c} \cdot c = \varepsilon.$$

Portanto, $\lim\limits_{n\to\infty} |x_n - z_n| = 0$, isto é, $(x_n) \sim (z_n)$. O que nos diz que $[x_n] = [z_n]$.

□

Agora vamos provar que, como em todos os outros conjuntos estudados até agora, multiplicar qualquer elemento de $\mathbb{R}$ por $[0]$ resulta em $[0]$.

Proposição 4.38. *Seja* $[x_n] \in \mathbb{R}$, *então* $[x_n] \cdot [0] = [0]$.

Demonstração. Note que

$$[x_n] \cdot [0] = [x_n \cdot 0] = [0].$$

Como queríamos demonstrar. □

Agora, estamos aptos a provar que $\mathbb{R}$ não possui divisores de zero.

Proposição 4.39. *Sejam* $[x_n], [y_n] \in \mathbb{R}$. *Se* $[x_n] \cdot [y_n] = [0]$, *então* $[x_n] = [0]$ *ou* $[y_n] = [0]$.

Demonstração. Suponhamos que $[y_n] \neq [0]$. Então,

$$[x_n] \cdot [y_n] = [0] = [0] \cdot [y_n].$$

Pela lei do cancelamento, concluímos que $[x_n] = [0]$. □

4.2.4 Caracterização Usual dos Números Reais

O nosso objetivo, nesta subseção, é mostrar que $\mathbb{R}$ pode ser visto como uma ampliação de $\mathbb{Q}$ em ordem a podermos definir o conjunto dos números naturais, como este é conhecido no ensino elementar.

Definição 4.26. Consideremos como $\mathbb{Q}^{'}$ o conjunto de todos os elementos $[x_n]$ de $\mathbb{R}$ de modo que a sequência (x_n), representativa de $[x_n]$, seja convergente para um número racional, isto é,

$$\mathbb{Q}^{'} = \{[r] \in \mathbb{R}/r \in \mathbb{Q}\}.$$

Vejamos agora como mostrar que $\mathbb{Q}^{'}$ é, na verdade, uma cópia de $\mathbb{Q}$ em $\mathbb{R}$.

Teorema 4.38. *Seja $f_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}^{'}$ uma aplicação definida por $f_{\mathbb{Q}}(r) = [r]$, para todo $r \in \mathbb{Q}$. Então, as seguintes afirmações são verdadeiras:*

i) *$f_{\mathbb{Q}}$ é bijetora;*

i) $f_{\mathbb{Q}}(r+s) = f_{\mathbb{Q}}(r) + f_{\mathbb{Q}}(s), \forall r, s \in \mathbb{Q}$;

iii) $f_{\mathbb{Q}}(rs) = f(r) \cdot f_{\mathbb{Q}}(s), \forall r, s \in \mathbb{Q}$;

iv) $r < s \Leftrightarrow f_{\mathbb{Q}}(r) < f_{\mathbb{Q}}(s)$, $r, s \in \mathbb{Q}$.

Demonstração. **i)** Para provar que $f_{\mathbb{Q}}$ é bijetora, precisamos estabelecer os dois itens abaixo:

a) $f_{\mathbb{Q}}$ é injetora:

Sejam $r, s \in \mathbb{Q}$. Então,

$$f_{\mathbb{Q}}(r) = f_{\mathbb{Q}}(s) \Leftrightarrow [r] = [s] \Leftrightarrow (r) \sim (s) \Leftrightarrow \lim_{n\to\infty} |r-s| = 0 \Leftrightarrow |r-s| = 0 \Leftrightarrow r = s.$$

b) $f_{\mathbb{Q}}$ é sobrejetora:

De fato, dado $[r] \in \mathbb{Q}'$, segue que $f_{\mathbb{Q}}(r) = [r]$, com $r \in \mathbb{Q}$.

ii) É fácil checar que

$$f_{\mathbb{Q}}(r+s) = [r+s] =: [r] + [s] = f_{\mathbb{Q}}(r) + f_{\mathbb{Q}}(s) \forall r, s \in \mathbb{Q}.$$

iii) Também é simples ver que:

$$f_{\mathbb{Q}}(rs) = [rs] =: [r] \cdot [s] = f_{\mathbb{Q}}(r) \cdot f_{\mathbb{Q}}(s), \forall r, s \in \mathbb{Q}.$$

iv) Primeiramente note que $x \in \mathbb{Q}_+^*$, então $[x] > [0]$ (isto segue do fato que $x > \frac{x}{2} \in \mathbb{Q}_+^*$). Portanto, $f_{\mathbb{Q}}(x) > f_{\mathbb{Q}}(0)$, $\forall x \in \mathbb{Q}_+^*$. Assim, dados $r, s \in \mathbb{Q}$, tem-se

$$r < s \Leftrightarrow s - r > 0 \Leftrightarrow [s - r] > [0] \Leftrightarrow [s] - [r] > [0] \Leftrightarrow [r] < [s] \Leftrightarrow f_{\mathbb{Q}}(r) < f_{\mathbb{Q}}(s).$$

□

A partir de agora consideraremos, através da aplicação $f_{\mathbb{Q}}$, dada acima, que $[r] = r$, para todo $r \in \mathbb{Q}$. Isto nos informa que $\mathbb{Q}$, observado como $\mathbb{Q}'$, satisfaz $\mathbb{Q} \subset \mathbb{R}$.

Abaixo, estabelecemos a notação usual do conjunto dos números reais.

Definição 4.27. O conjunto $\mathbb{R}$ constituído pelas classes de equivalência das sequências de Cauchy de números racionais, definido anteriormente, será denominado, a partir de agora, conjunto dos números reais.

Consequentemente, através da identificação $f_{\mathbb{Q}}$, concluímos que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

4.2.5 $\mathbb{R}$ Corpo Arquimediano

Nesta seção, mostraremos que o corpo ordenado $\mathbb{R}$ é Arquimediano e que sempre existe um número racional entre dois números reais quaisquer.

Comecemos com a prova do seguinte teorema.

Teorema 4.39 (Propriedade Arquimediana)**.** *Seja $x \in \mathbb{R}$. Então, existe $n \in \mathbb{N}$ tal que $x < n$.*

Demonstração. Seja $x = [x_n] \in \mathbb{R}$. Então (x_n) é uma sequência de Cauchy de números racionais. Consequentemente, (x_n) é limitada. Daí existe $k \in \mathbb{Q}_+^*$ tal que $|x_n| \leq k$, para todo $n \in \mathbb{N}^*$. Com isso,

$$x_n \leq k < k + 1 = k + 2 - 1, \forall n \in \mathbb{N}^*, \text{ pois } k \in \mathbb{Q}_+^*.$$

Portanto, obtemos

$$1 < k + 2 - x_n, \forall n \in \mathbb{N}^*.$$

Como $1 \in \mathbb{Q}_+^*$, então $[k + 2] > [x_n]$. Dessa forma, $k + 2 > x$, já que $k + 2 \in \mathbb{Q}_+^*$ (através da função $f_{\mathbb{Q}}$ definida acima). Além disso, $k + 2 = \frac{m}{n}$, com $m, n \in \mathbb{N}^*$. Note também que $\frac{m}{n} \leq m < m + 1$ (desde que $m, n \geq 1$). Por fim,

$$x < k + 2 = \frac{m}{n} < m + 1 \in \mathbb{N}.$$

□

Vejamos abaixo uma outra maneira de enunciar a Propriedade Arquimediana.

Teorema 4.40 (Propriedade Arquimediana)**.** *Sejam $x, y \in \mathbb{R}$ tais que $x > 0$. Então, existe um número natural n tal que $y < nx$.*

Demonstração. Como $x > 0$, então $\exists x^{-1} \in \mathbb{R}$ tal que $x^{-1} > 0$ e $x^{-1} \cdot x = 1$. Assim, usando o fato que $yx^{-1} \in \mathbb{R}$ e o Teorema 4.39, tem-se que $\exists n \in \mathbb{N}$ tal que $yx^{-1} < n$. Daí, multiplicando esta última desigualdade por $x > 0$, chegamos a

$$(yx^{-1})x < nx \Rightarrow y(x^{-1}x) < nx \Rightarrow y < nx.$$

□

Agora, estamos pronto para provar que o conjunto $\mathbb{Q}$ é denso[1] em $\mathbb{R}$. Mais precisamente, temos o seguinte resultado.

Proposição 4.40. *Sejam $x, y \in \mathbb{R}$ tais que $x < y$. Então, existe $r \in \mathbb{Q}$ tal que $x < r < y$.*

Demonstração. Como $x < y$, então, por definição, existem $d \in \mathbb{Q}_+^*$ e $n_0 \in \mathbb{N}^*$ tais que,

$$y_n - x_n > d, \forall n \geq n_0,$$

onde $x = [x_n]$ e $y = [y_n]$. Portanto, podemos escrever

$$\frac{y_n - x_n}{2} > \frac{d}{2}, \forall n \geq n_0.$$

Logo, inferimos que

$$\frac{y_n - x_n}{2} - \frac{d}{4} > \frac{d}{4}, \forall n \geq n_0.$$

Isto significa, através da identificação $f_{\mathbb{Q}}$, que

$$\left[\frac{y_n - x_n}{2}\right] > \left[\frac{d}{4}\right] = \frac{d}{4} \Rightarrow \frac{y - x}{2} > \frac{d}{4} =: h,$$

onde $h \in \mathbb{Q}_+^*$. E, como $\mathbb{R}$ é Arquimediano (ver Teorema 4.40), então existe $n \in \mathbb{N}$ tal que $y < nh$. De $x < y$, obtemos $x < nh$.

[1] A afirmação dada na Proposição 4.40 é a definição para que $\mathbb{Q}$ seja denso em $\mathbb{R}$.

Seja $X = \{m \in \mathbb{N}/x < mh\} \subseteq \mathbb{N}$. Acima, vimos que $n \in X$, logo $X \neq \emptyset$. Pelo Princípio da Boa Ordem em $\mathbb{N}$, existe um mínimo $p \in X$. Seja $r = ph$. Logo, $(p-1)h \leq x$ (pois $p = \min X$). Consequentemente,

$$r = ph + h - h = (p-1)h + h \leq x + h < x + (\frac{y-x}{2}) < x + y - x = y.$$

Assim, $r < y$. Como $p \in X$, então $x < ph = r$. Isto conclui a prova da proposição em questão. □

4.2.6 Completude de $\mathbb{R}$

Completaremos a construção do conjunto dos números reais mostrando que toda sequência de Cauchy de números racionais converge para um número real. Para este fim, precisamos, primeiramente, definir o que significa sequência de números reais.

Definição 4.28. Uma sequência de números reais é uma aplicação $x : \mathbb{N}^* \to \mathbb{R}$, que associa um número $n \in \mathbb{N}^*$ a um outro, chamado termo geral, $x(n) = x_n \in \mathbb{R}$. A sequência x é denotada por $x = (x_n)_{n\in\mathbb{N}^*} = (x_1, x_2, ...)$.

Quando não houver nenhuma possibilidade de confusão denotaremos $(x_n)_{n\in\mathbb{N}^*}$ por (x_n).

Vejamos, a seguir, como definir sequências de números reais convergentes.

Definição 4.29. Dizemos que uma sequência de números reais (x_n) converge para $a \in \mathbb{R}$, e indicamos por $x_n \to a$, ou ainda, $\lim_{n\to\infty} x_n = a$, se dado $\varepsilon \in \mathbb{R}^*_+$ (onde $\mathbb{R}^*_+ = \{x \in \mathbb{R}/x > 0\}$) existe $n_0 \in \mathbb{N}^*$ tal que, $\forall n \geq n_0$ $(n \in \mathbb{N}^*)$, tem-se $|x_n - a| < \varepsilon$.

Vejamos um exemplo simples de sequência de números reais convergente.

Exemplo 4.11. Considere uma sequência constante (x_n), isto é, $x_n = c$, $\forall n \in \mathbb{N}$, onde $c \in \mathbb{R}$. Logo, dado $\varepsilon \in \mathbb{R}^*_+$, temos que

$$|x_n - c| = |c - c| = 0 < \varepsilon, \forall n \in \mathbb{N}^*.$$

Neste caso, $n_0 = 1 \in \mathbb{N}^*$. Dessa forma, toda sequência $(c)_{n\in\mathbb{N}^*}$ constante é convergente e converge para c.

Abaixo provaremos que podemos aplicar o limite em uma desigualdade, que envolve termos gerais de duas sequências, desde que estas sejam convergentes.

Teorema 4.41. *Sejam (x_n), (y_n) sequências de números reais. Se $x_n \leq y_n, \forall n \in \mathbb{N}^*$ e se $\lim_{n\to\infty} x_n = a$ e $\lim_{n\to\infty} y_n = b$, com $a, b \in \mathbb{R}$, então $a \leq b$.*

Demonstração. Suponhamos $a > b$. Como $x_n \to a$ e $y_n \to b$, podemos tomar $\varepsilon = \frac{a-b}{2} \in \mathbb{R}_+^*$ para obter $n_1 \in \mathbb{N}$ tal que para todo $n \geq n_1$, tem-se $|x_n - a| < \varepsilon$, isto é, $a - \varepsilon < x_n$, ou seja, $\frac{a+b}{2} < x_n$.

Analogamente, obtém-se $n_2 \in \mathbb{N}$ tal que para todo $n \geq n_2$, chega-se a $|y_n - b| < \varepsilon$, isto é, $y_n < b + \varepsilon$, ou seja, $y_n < \frac{a+b}{2}$. Tomando $n_0 = \max\{n_1, n_2\} \in \mathbb{N}^*$, temos

$$y_n < \frac{a+b}{2} < x_n, \forall n \geq n_0^*.$$

Isto contraria a hipótese $x_n \leq y_n, \forall n \in \mathbb{N}^*$. Por fim, $a \leq b$. □

Corolário 4.42. Seja c um número real e (x_n) uma sequência de números reais. Se $x_n \leq b$, para todo $n \in \mathbb{N}^*$, e se $\lim_{n\to\infty} x_n = a$, $a \in \mathbb{R}$, então $a \leq b$.

Demonstração. Basta usarmos o Teorema 4.41 e tomarmos $y_n = b, \forall n \in \mathbb{N}^*$. □

Obs 4.2. Se $x_n \leq 0$, $\forall n \in \mathbb{N}^*$, então $\lim_{n\to\infty} x_n$, caso exista, é menor do que ou igual a 0 (basta usar o Teorema 4.41 com $y_n = 0, \forall n \in \mathbb{N}^*$).

Obs 4.3. Se $y_n \geq 0$, $\forall n \in \mathbb{N}^*$, então $\lim_{n\to\infty} y_n$, caso exista, é maior do que ou igual a 0 (basta usar o Teorema 4.41 com $x_n = 0, \forall n \in \mathbb{N}^*$).

Obs 4.4. Observe que se $x_n > 0$, $\forall n \in \mathbb{N}^*$ não significa que $\lim_{n\to\infty} x_n > 0$ (mesmo que este elemento exista). Considere, por exemplo o limite $\lim_{n\to\infty} \frac{1}{n} = 0$.

Vejamos, agora, como definir sequências de Cauchy em $\mathbb{R}$.

Definição 4.30. Uma sequência (x_n) de elementos em $\mathbb{R}$ é chamada sequência de Cauchy de números reais, se dado $\varepsilon \in \mathbb{R}_+^*$, existe $n_0 \in \mathbb{N}^*$ tal que, para todo $m, n \in \mathbb{N}$, com $m, n \geq n_0$, tem-se $|x_n - x_m| < \varepsilon$.

A seguir, mostraremos como comparar convergências em $\mathbb{Q}$ e $\mathbb{R}$.

Proposição 4.41. *Seja $a \in \mathbb{Q}$. Uma sequência de Cauchy de números racionais (x_n) converge para a em $\mathbb{Q}$ se, e somente se, converge para a em $\mathbb{R}$.*

Demonstração. ($\Rightarrow$) Seja (x_n) uma sequência de Cauchy de números racionais que converge para a em $\mathbb{Q}$. Seja $\varepsilon > 0$ um número real. Pela Proposição 4.40 existe um número racional $r > 0$ tal que $r < \varepsilon$. Como (x_n) converge para a em $\mathbb{Q}$, existe $n_0 \in \mathbb{N}^*$ tal que para todo $n \geq n_0$, tem-se $|x_n - a| < r$. Aplicando a desigualdade $r < \varepsilon$ chegamos a $|x_n - a| < \varepsilon$. Portanto, (x_n) converge para a em $\mathbb{R}$.

($\Leftarrow$) Suponhamos agora que (x_n) converge para a em $\mathbb{R}$. Seja $\varepsilon > 0$ um número racional. Mas, $\varepsilon \in \mathbb{R}$; logo, existe $n_0 \in \mathbb{N}^*$ tal que, para todo $n \geq n_0$, tem-se $|x_n - a| < \varepsilon$. Isto conclui a prova da proposição em questão. □

Agora, relacionemos as definições de sequências de Cauchy em $\mathbb{Q}$ e $\mathbb{R}$.

Proposição 4.42. *Seja (x_n) uma sequência de números racionais. Então, (x_n) é uma sequência de Cauchy em $\mathbb{Q}$ se, e somente se, (x_n) é uma sequência de Cauchy em $\mathbb{R}$.*

Demonstração. ($\Rightarrow$) Seja (x_n) uma sequência de Cauchy de números racionais em $\mathbb{Q}$. Seja $\varepsilon > 0$ um número real. Pela Proposição 4.40 existe um número racional $r > 0$ tal que $r < \varepsilon$. Como (x_n) é uma sequência de Cauchy em $\mathbb{Q}$ existe $n_0 \in \mathbb{N}^*$ tal que para todo $m, n \geq n_0$ tem-se $|x_n - x_m| < r$. Como $r < \varepsilon$, então $|x_n - x_m| < \varepsilon$. Portanto, (x_n) é uma sequência de Cauchy em $\mathbb{R}$.

($\Leftarrow$) Suponhamos agora que (x_n) seja uma sequência de Cauchy de números racionais em $\mathbb{R}$. Seja $\varepsilon > 0$ um número racional. Daí, $\varepsilon \in \mathbb{R}$, logo, existe $n_0 \in \mathbb{N}^*$ tal que, para todo $m, n \geq n_0$, tem-se $|x_n - x_m| < \varepsilon$. Portanto, (x_n) é uma sequência de Cauchy em $\mathbb{Q}$. □

Proposição 4.43. *Seja (x_n) uma sequência de Cauchy de números racionais. Considere que $x = [x_n] \in \mathbb{R}$. Então, $x_n \to x$.*

Demonstração. Seja $\varepsilon > 0$ um número real. Consideremos ainda $r > 0$ um número racional tal que $r < \varepsilon$, cuja existência é garantida pela Proposição 4.40. Como (x_n) é uma sequência de Cauchy em $\mathbb{Q}$, então existe $n_0 \in \mathbb{N}^*$ tal que, para todo $m, n \geq n_0$, tem-se

$$|x_n - x_m| < \frac{r}{2} \Rightarrow -\frac{r}{2} < x_m - x_n < \frac{r}{2} \Leftrightarrow -\frac{r}{2} + x_n < x_m < \frac{r}{2} + x_n.$$

Agora fixe $m \in \mathbb{N}^*$ tal que $m \geq n_0$. Logo,

$$x_m > x_n - \frac{r}{2} = x_n + \frac{r}{2} - r, \forall n \geq n_0.$$

Daí, $x_m - (x_n - r) > \frac{r}{2}, \forall n \geq n_0$ (onde $\frac{r}{2} \in \mathbb{Q}_+^*$). Consequentemente,

$$x_m = [x_m] > [x_n - r] := [x_n] + [-r] = x - r,$$

desde que $m \geq n_0$ está fixo. Analogamente, obtemos

$$x_m - (x_n + r) < -\frac{r}{2}, \forall n \geq n_0,$$

onde $\frac{r}{2} \in \mathbb{Q}_+^*$. Dessa forma, chegamos a

$$x_m = [x_m] < [x_n + r] := [x_n] + [r] = x + r,$$

com $m \geq n_0$ está fixo. Portanto,

$$x - r < x_m < x + r, \forall m \geq n_0.$$

Por fim, $|x_m - x| < r < \varepsilon, \forall m \geq n_0$. Isto nos diz que $\lim_{n\to\infty} x_m = x$. Isto prova o teorema em questão. □

A seguir provaremos que, ao contrário de $\mathbb{Q}$, toda sequência de Cauchy é convergente em $\mathbb{R}$. Isto qualifica $\mathbb{R}$ como um conjunto completo.

Teorema 4.43. *Toda sequência de Cauchy de números reais converge para um número real.*

Demonstração. Seja $(x_i)_{i\in\mathbb{N}^*}$ uma sequência de Cauchy de números reais. Temos $x_i = [x_n^i]$, onde $(x_n^i)_{n\in\mathbb{N}^*}$ é uma sequência de Cauchy de números racionais. Vimos na Proposição 4.43 que

$$\lim_{n\to\infty} x_n^i = x_i, \text{ para cada } i \in \mathbb{N}^*.$$

Por conseguinte, $\exists n_i \in \mathbb{N}^*$ tal que

$$|x_{n_i}^i - x_i| < \frac{1}{i}, \text{ para cada } i \in \mathbb{N}^*.$$

Agora, seja $y_i = x_{n_i}^i - x_i, \forall i \in \mathbb{N}^*$. Daí,

$$|y_i| < \frac{1}{i}, \forall i \in \mathbb{N}^*.$$

Passando ao limite, quando $i \to \infty$, temos que $\lim_{i\to\infty} y_i = 0$. Dessa forma, dado $\varepsilon \in \mathbb{R}_+^*$, $\exists i_0 \in \mathbb{N}^*$ tal que

$$\forall i \geq i_0 \Rightarrow |y_i| < \frac{\varepsilon}{3}.$$

Como $(x_i)_{i\in\mathbb{N}^*}$ é uma sequência de Cauchy em $\mathbb{R}$, então $\exists i_1 \in \mathbb{N}^*$ tal que

$$i, j \geq i_1 \Rightarrow |x_i - x_j| < \frac{\varepsilon}{3}.$$

Seja $i_2 = \max\{i_0, i_1\} \in \mathbb{N}^*$. Logo, para todo $i, j \geq i_2$, tem-se que

$$\begin{aligned} |x^i_{n_i} - x^j_{n_j}| &= |x^i_{n_i} - x_i + x_i - x_j + x_j - x^j_{n_j}| \\ &\leq |x^i_{n_i} - x_i| + |x_i - x_j| + |x_j - x^j_{n_j}| \\ &= |y_i| + |x_i - x_j| + |y_j| \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon. \end{aligned}$$

Isto significa que $(x^i_{n_i})_{i \in \mathbb{N}^*}$ é uma sequência de Cauchy de números racionais (pois é uma sequência de Cauchy em $\mathbb{R}$).

Seja $x = [x^i_{n_i}] \in \mathbb{R}$. Pela Proposição 4.43, temos que $\lim\limits_{i \to \infty} x^i_{n_i} = x$. Portanto, $\exists n_0 \in \mathbb{N}^*$ tal que, para todo $i \geq n_0$, tem-se

$$|x^i_{n_i} - x| < \frac{2\varepsilon}{3}.$$

Por fim, chegamos a

$$\begin{aligned} |x_i - x| &= |x_i - x^i_{n_i} + x^i_{n_i} - x| \\ &\leq |x_i - x^i_{n_i}| + |x^i_{n_i} - x| \\ &= |y_i| + |x^i_{n_i} - x| \\ &< \frac{\varepsilon}{3} + \frac{2\varepsilon}{3} = \varepsilon, \end{aligned}$$

para todo $i \geq m_0 = \max\{i_0, n_0\}$. Isto significa que $\lim\limits_{i \to \infty} x_i = x$. A prova do teorema em questão segue. □

4.2.7 Supremo em $\mathbb{R}$

Nesta subseção, nossa meta é provar a existência do supremo para qualquer conjunto não vazio e limitado superiormente de $\mathbb{R}$. É importante destacar que a definição de conjuntos limitados, tanto inferior quanto superiormente, e supremo foram estabelecidas na Definição 4.15.

Comecemos listando algumas definições necessárias para alcançarmos nosso objetivo.

Definição 4.31. Dizemos que uma sequência (x_n) de números reais é não decrescente (respectivamente crescente) se $x_n \leq x_{n+1}, \forall n \in \mathbb{N}^*$ (respectivamente $x_n < x_{n+1}, \forall n \in \mathbb{N}^*$).

Definição 4.32. Uma sequência (x_n) de números reais é não crescente (respectivamente decrescente) se $x_{n+1} \leq x_n, \forall n \in \mathbb{N}^*$ (respectivamente $x_{n+1} < x_n, \forall n \in \mathbb{N}^*$).

Definição 4.33. Uma sequência é dita monótona se esta é crescente, decrescente, não crescente ou não decrescente.

Definição 4.34. Uma sequência (x_n) de números reais, diz-se limitada se existe $c \in \mathbb{R}_+^*$, tal que $|x_n| \leq c$, $\forall n \in \mathbb{N}^*$.

O primeiro resultado desta subseção relaciona sequências monótonas e limitadas com sequências de Cauchy em $\mathbb{R}$.

Proposição 4.44. *Se (x_n) é uma sequência monótona e limitada de números reais, então (x_n) é uma sequência de Cauchy em $\mathbb{R}$.*

Demonstração. Consideremos que (x_n) seja monótona não decrescente. Como (x_n) é limitada, então existe $a \in \mathbb{R}_+^*$ tal que $x_n \leq a$, para todo $n \in \mathbb{N}^*$. Assim,

$$x_1 \leq x_2 \leq ... \leq x_n \leq ... \leq a.$$

Suponhamos, por absurdo, que (x_n) não seja uma sequência de Cauchy. Isto significa que existe $\varepsilon \in \mathbb{R}_+^*$ tal que para qualquer que seja $n_0 \in \mathbb{N}^*$, podemos encontrar $m, n \in \mathbb{N}^*$, com $m \leq n$ e $m, n \geq n_0$ tais que

$$x_n - x_m = |x_n - x_m| \geq \varepsilon.$$

Em particular, para $n_0 = 1 \in \mathbb{N}^*$, $\exists m_1, n_1 \in \mathbb{N}^*$ com $m_1 \leq n_1$ e $m_1, n_1 \geq 1$ tais que

$$x_{n_1} - x_{m_1} \geq \varepsilon.$$

Para $n_0 = n_1$, obtemos $m_2, n_2 \in \mathbb{N}^*$ com $m_2 \leq n_2$ e $m_2, n_2 \geq n_1$ tais que

$$x_{n_2} - x_{m_2} \geq \varepsilon.$$

Para $n_0 = n_2$, podemos encontrar $m_3, n_3 \in \mathbb{N}^*$, com $m_3 \leq n_3$ e $m_3, n_3 \geq n_2$ tais que

$$x_{n_3} - x_{m_3} \geq \varepsilon.$$

Suponhamos, por recorrência, que $\exists m_i, n_i \in \mathbb{N}^*$, com $m_i \leq n_i$ e $m_{i+1}, n_{i+1} \geq n_i$ tais que

$$x_{n_i} - x_{m_i} \geq \varepsilon, \forall i = 1, ..., k.$$

Tome $n_0 = n_k$. Então, $\exists m_{k+1}, n_{k+1} \in \mathbb{N}^*$, com $m_{k+1} \leq n_{k+1}$ e $m_{k+1}, n_{k+1} \geq n_k$ tais que

$$x_{n_{k+1}} - x_{m_{k+1}} \geq \varepsilon.$$

Portanto, $\exists m_i, n_i \in \mathbb{N}^*$ com $m_i \leq n_i$ e $m_{i+1}, n_{i+1} \geq n_i$ tais que

$$x_{n_i} - x_{m_i} \geq \varepsilon, \forall i \in \mathbb{N}^*. \tag{4.8}$$

Afirmação: $x_{n_i} \geq x_{m_1} + i\varepsilon, \forall i \in \mathbb{N}^*$.

Provaremos a desigualdade acima por indução sobre i. Assim sendo, seja

$$X = \{i \in \mathbb{N}^* / x_{n_i} \geq x_{m_1} + i\varepsilon\}.$$

Note que $1 \in X$, pois

$$x_{n_1} \geq x_{m_1} + \varepsilon = x_{m_1} + 1 \cdot \varepsilon,$$

por (4.8).

Suponhamos que $k \in X$, isto é, $x_{n_k} \geq x_{m_1} + k\varepsilon$. Daí, encontramos

$$x_{n_{k+1}} \geq x_{m_{k+1}} + \varepsilon = (x_{m_{k+1}} - x_{n_k}) + x_{n_k} + \varepsilon \geq x_{n_k} + \varepsilon \geq x_{m_1} + k\varepsilon + \varepsilon = x_{m_1} + (k+1)\varepsilon,$$

por (4.8) e $m_{k+1} \geq n_k$. Isto prova que $X = \mathbb{N}^*$.

Tendo em vista a propriedade Arquimediana dos números reais, podemos tomar $k_0 \in \mathbb{N}$ de modo que

$$k_0\varepsilon > a - x_{m_1}.$$

Se $k_0 = 0$, teríamos que $x_{m_1} > a$. Um absurdo, pois $x_n \leq a$, para todo $n \in \mathbb{N}^*$. Assuma, então, que $k_0 \in \mathbb{N}^*$. Por isso, podemos escrever

$$x_{n_{k_0}} \geq x_{m_1} + k_0\varepsilon > x_{m_1} + a - x_{m_1} = a.$$

Deste modo, existe pelo menos um elemento de (x_n) que é maior do que a. Isto contradiz o fato de que $x_n \leq a$, para todo $n \in \mathbb{N}^*$. Portanto (x_n) é uma sequência de Cauchy de números reais. A demonstração para os outros casos possíveis de sequência monótonas é análoga. □

Relacionando sequências monótonas e limitadas com convergência, temos o seguinte corolário.

Corolário 4.44. *Se (x_n) é uma sequência monótona e limitada de números reais, então esta é uma sequência convergente.*

Demonstração. É fato, pela proposição acima, que (x_n) é uma sequência de Cauchy em $\mathbb{R}$. Daí, como toda sequência de Cauchy é convergente (ver Teorema 4.43), então (x_n) é uma sequência convergente. □

O resultado a seguir, será útil para provarmos que todo subconjunto de $\mathbb{R}$ não vazio e limitado superiormente admite supremo.

Teorema 4.45. *Sejam (x_n) e (y_n) duas sequências de números reais tais que:*

i) *(x_n) é monótona não decrescente;*

ii) *(y_n) é monótona não crescente;*

iii) *$x_m < y_n, \forall m, n \in \mathbb{N}^*$;*

iv) *dado $\varepsilon \in \mathbb{R}_+^*, \exists n_0 \in \mathbb{N}^*$ tal que para todo $n \geq n_0$, tem-se $y_n - x_n < \varepsilon$.*

Então, existe um único número real que pertence a todos os intervalos $[x_m, y_n]$, com $m, n \in \mathbb{N}^*$.

Demonstração. Como as hipóteses do teorema nos diz que (x_n) e (y_n) são monótonas e limitadas (por y_1 e x_1), então temos que (x_n) e (y_n) são sequências de Cauchy em $\mathbb{R}$. Deste modo estas sequências são convergentes em $\mathbb{R}$. Consideremos, então, que

$$\lim_{n\to\infty} x_n = x \text{ e } \lim_{n\to\infty} y_n = y,$$

onde $x = [x_n], y = [y_n] \in \mathbb{R}$.

O item **iii)** do enunciado do teorema nos diz que, $x_m < y_n, \forall m, n \in \mathbb{N}^*$. Daí, passando ao limite, quando $m \to \infty$, obtemos

$$x = \lim_{m\to\infty} x_m \leq y_n, \forall n \in \mathbb{N}^*.$$

Agora passando ao limite, quando $n \to \infty$, encontramos

$$x \leq \lim_{n\to\infty} y_n = y.$$

Não pode ocorrer $x < y$. De fato, pelo item **iv)**, com $\varepsilon = y - x > 0$ tem-se que existe $n_0 \in \mathbb{N}^*$ tal que para todo $n \geq n_0$, obtém-se $y_n - x_n < \varepsilon = y - x$.

Afirmação: $x_m \leq x, \forall m \in \mathbb{N}^*$.

De fato, suponhamos que $\exists m_0 \in \mathbb{N}^*$ tal que $x_{m_0} > x$. Como $x_{m_0} \leq x_m, \forall m \geq m_0$, então, passando ao limite, quando $m \to \infty$, encontramos

$$x = \lim_{m\to\infty} x_m \geq x_{m_0} > x.$$

Isto é uma contradição.

Analogamente, temos que $y_n \geq y, \forall n \in \mathbb{N}^*$ (já que (y_n) é não crescente e $\lim_{n\to\infty} y_n = y$). Logo, chegamos a

$$x_n + y \leq y_n + x, \forall n \in \mathbb{N}^*,$$

isto é,

$$y - x \leq y_n - x_n, \forall n \in \mathbb{N}^*.$$

Contradizendo o fato de que $y_n - x_n < y - x$ para todo $n \geq n_0$. Assim, $x = y$. Por fim, pelo que foi provado acima, encontramos $x_m \leq x \leq y_n$, para todo $m, n \in \mathbb{N}^*$. □

Para concluir este capítulo, provaremos que conjuntos gozam da propriedade de admitirem supremo (o que não ocorre em $\mathbb{Q}$).

Teorema 4.46. *Seja X um conjunto não vazio e limitado superiormente de números reais. Então, o supremo de X existe em $\mathbb{R}$.*

Demonstração. Consideremos y_1 uma cota superior de X (X é limitado superiormente). Seja $x_1 \in \mathbb{R}$ tal que x_1 não seja cota superior de X. Note que $x_1 < y_1$. Designemos por:

y_2 : o menor dos números $\frac{y_1+x_1}{2}$ e y_1, que seja cota superior de X.

x_2 : o maior dos números $\frac{y_1+x_1}{2}$ e x_1, que não seja cota superior de X.

Observemos que se $y_2 = \frac{y_1+x_1}{2}$, então $x_2 = x_1$ e se $y_2 = y_1$, então $x_2 = \frac{y_1+x_1}{2}$ (pois $\frac{y_1+x_1}{2} > x_1$). Em ambos os casos, temos $y_2 - x_2 = \frac{y_1-x_1}{2}$. Observe que $x_2 < y_2$, desde que $x_1 < y_1$. Denote por:

y_3 : o menor dos números $\frac{y_2+x_2}{2}$ e y_2 que seja cota superior de X.

x_3 : o maior dos números $\frac{y_2+x_2}{2}$ e x_2 que não seja cota superior de X.

Observemos que se $y_3 = \frac{y_2+x_2}{2}$, então $x_3 = x_2$ e se $y_3 = y_2$, então $x_3 = \frac{y_2+x_2}{2}$(pois $\frac{y_2+x_2}{2} > x_2$). Em ambos os casos, encontramos $y_3 - x_3 = \frac{y_1-x_1}{2^2}$. Também temos que $x_3 < y_3$.

Generalizando, se temos $x_n < y_n$, com $y_n - x_n = \frac{y_1-x_1}{2^n}$, podemos determinar:

y_{n+1} : o menor dos números $\frac{y_n+x_n}{2}$ e y_n que seja cota superior de X.

x_{n+1} : o maior dos números $\frac{y_n+x_n}{2}$ e x_n que não seja cota superior de X.

Observemos que se $y_{n+1} = \frac{y_n+x_n}{2}$, então $x_{n+1} = x_n$ e se $y_n = y_{n+1}$, então $x_{n+1} = \frac{y_n+x_n}{2}$ (pois $\frac{y_n+x_n}{2} > x_n$). Em ambos os casos $y_{n+1} - x_{n+1} = \frac{y_1-x_1}{2^{n+1}}$. É fácil concluir que $x_{n+1} < y_{n+1}$, pois $x_1 < y_1$.

A sequência (y_n) como foi construída é monótona não crescente, e a sequência (x_n) monótona não decrescente. Além disso,

• Pela construção das sequências (y_n) e (x_n), temos que

$$x_1 \leq x_2 \leq x_3 \leq x_2 \leq ... \leq x_n \leq y_n \leq ... \leq y_3 \leq y_2 \leq y_1 \leq y_0, \forall n \in \mathbb{N}^*.$$

• Dado $\varepsilon \in \mathbb{R}_+^*$, basta tomar $n_1 \in \mathbb{N}^*$ tal que $\frac{y_1+x_1}{2^{n_1}} < \varepsilon$ (basta assumir $n_1 > \frac{y_1+x_1}{\varepsilon} - 1$ e usar desigualdade de Bernoulli). Daí, para qualquer $n \geq n_1$, tem-se

$$y_n - x_n = \frac{y_1 - x_1}{2^n} < \varepsilon.$$

Então são satisfeitas as hipóteses do Teorema anterior, e então existe um único número real k que pertence a todos os intervalos $[x_n, y_m]$, para todo $n, m \in \mathbb{N}^*$. Usando a prova do Teorema anterior, temos que

$$\lim_{n\to\infty} y_n = \lim_{n\to\infty} x_n = k.$$

O número real k é o supremo de X. De fato, qualquer que seja $x \in X$, tem-se $x \leq y_n$, para todo $n \in \mathbb{N}^*$ (y_n é cota superior de X). Passando ao limite, quando $n \to \infty$, obtemos

$$x \leq \lim_{n\to\infty} y_n = k.$$

Suponhamos que exista $s \in \mathbb{R}$ tal que $s < k$ e s é cota superior de X. Assim, $k - s > 0$. Como $\lim_{n\to\infty} x_n = k$, então existe $n_1 \in \mathbb{N}^*$, tal que, para todo $n \geq n_1$, tem-se

$$|x_n - k| < k - s \Rightarrow s - k < x_n - k < k - s \Rightarrow s < x_n < 2k - s.$$

Logo, $s < x_n$, para todo $n \geq n_1$. Dessa forma, $x < x_n$, $\forall x \in X$ e $n \geq n_1$ (pois, s é cota superior de X). Isto significa que x_{n_1} é cota superior de X (nenhum dos termos da sequência (x_n) é cota superior de X). Absurdo! Portanto, $k \in \mathbb{R}$ e $k = \sup X$. □

4.3 Aplicação dos reais

4.3.1 A sequência de Fibonacci

Apresentaremos um pouco da história da vida e obra de Fibonacci que foi o matemático responsável pela descoberta da sequência que leva o seu nome, bem como, o problema da reprodução

dos coelhos cuja solução é a geradora dos termos da referida sequência e sua correspondente definição formal.

Leonardo de Pisa (Fibonacci)

Leonardo de Pisa foi para muitos, o matemático europeu mais original e capaz do Período Medieval. Nascido, na década de 1170, na cidade de Pisa, na região da Toscana (Itália), era também conhecido como Leonardo Fibonacci (devido ao fato de Fibonacci ser um diminutivo de *filius Bonacci* que significa filho de Bonaccio), Leonardo Pisano ou Leonardo Bigollo (na Toscana, Bigollo significa *viajante*). Ficou conhecido pelo seu papel na introdução dos algarismos indo-arábicos na Europa e pela famosa sequência numérica que leva o seu nome. No Século XII, Pisa se destacava por ser um dos grandes centros comerciais da Itália, assim como Gênova e Veneza. Possuía vários entrepostos comerciais espalhados pelo Mediterrâneo onde passavam mercadorias importadas do interior e do ultramar, tais como, as especiarias do Extremo Oriente que circulavam com destino à Europa Ocidental. Leonardo Fibonacci era filho de Guglielmo dei Bonacci, um destacado mercador pisano e representante dos comerciantes de Pisa que atuava como uma espécie de fiscal alfandegário em Bugia (atualmente Bejaia, na Argélia). Devido às viagens do seu pai por quase todo o Mediterrâneo, Fibonacci teve oportunidade de visitar a Sicília, o Egito, a Espanha mulçumana, a Grécia e, dessa forma, de conhecer, nestes lugares, as diversas culturas, assim como, de aprender com professores islâmicos a matemática árabe que era mais desenvolvida que a matemática praticada na Europa Ocidental. Após concluir que o sistema de numeração indo-arábicos, o qual incluía o princípio do valor de lugar, era bem mais prático que todos os outros sistemas de numeração, inclusive, o sistema de algarismos romanos, Fibonacci escreveu o seu primeiro livro, *Liber Abaci* (Livro do Ábaco), título que não condiz com o conteúdo da obra, publicado em 1202, no qual descreve em seus primeiros capítulos, as nove cifras indianas (nove algarismos), o zero e as operações elementares envolvendo tais algarismos (incluindo o zero). Segundo Lívio (2011, p. 111), Fibonacci inicia o Liber Abaci da seguinte forma: *os nove números indianos são: 9 8 7 6 5 4 3 2 1. Com esses nove números e com o 0... qualquer número pode ser escrito...* E para Boyer (1974, p. 185), *o Liber Abaci é um tratado muito completo sobre métodos e problemas algébricos em que o uso dos numerais indo-arábicos é fortemente recomendado.* Nos seus problemas são incluídas questões úteis aos mercadores, como conversões monetárias, cálculo de juros, médias, entre outras. Além desses problemas de ordem prática, existem outros tantos, tais como, o problema do resto chinês, a regra da falsa posição, e mais outros que são resolvidos através do uso de equações quadráticas. A obra também apresenta justificativas geométricas de fórmulas quadráticas e métodos para se obter somas de séries. Após essa obra, Fibonacci gozou de muito sucesso e prestígio a ponto do

Imperador Frederico II tê-lo convidado para participar de uma competição matemática, onde foi apresentado vários problemas considerados difíceis pelo matemático da Corte, Johannes Palermo. Fibonacci resolveu todos os problemas os quais a solução de dois deles apresentou em um livro chamado Flos (Flor), publicado em 1225. Além do Liber Abaci e do Flos, Fibonacci escreveu outros dois livros: o Practica Geometriae, publicado em 1220, onde ele apresentou os conhecimentos de Geometria e Trigonometria da época e o Liber Quadratorum, publicado em 1225, que é considerado a sua obra mais avançada, pois trata da Teoria dos Números. No entanto, Fibonacci ficou conhecido não exatamente pelos seus livros, mas pelo fato de Edouard Lucas, na sua Coleção Récréations mathématiques, ter dado o nome fibonacci a uma sequência que aparece como solução de um problema do Liber Abaci, que descreveremos a seguir.

O problema da reprodução de coelhos

"Um homem pôs um par de filhotes de coelhos num lugar cercado de muro por todos os lados. Quantos pares de coelhos podem ser gerados a partir desse par em um ano se, supostamente, todo mês cada par dá à luz a um novo par, que é fértil a partir do segundo mês?"

Solução: Segue abaixo o processo de reprodução em cada mês:
• No 1º mês, temos apenas um par de coelhos (ainda filhotes).
• No 2º mês, continuamos com um par de coelhos (agora adultos).
• No 3º mês, nasce um par de filhotes. Logo, temos dois pares de coelhos (um par de adultos e um par de filhotes).
• No 4º mês, o par inicial gera o seu segundo par de filhotes, ficando um total de três pares de coelhos (o par inicial, o primeiro par de filhotes, agora adultos, e o segundo par de filhotes).
• No 5º mês, o par inicial gera o seu terceiro par de filhotes; o segundo par de adultos gera o seu primeiro par de filhotes e o par de filhotes gerado no mês anterior, agora adulto. Logo, temos cinco pares de coelhos (três pares de adultos mais dois pares de filhotes).
• Etc.

Notamos que num determinado mês, o número de pares de coelhos será igual ao número de pares do mês anterior mais o número de pares do mês anterior ao anterior, pois serão esses últimos que contribuirão com o acréscimo do número de pares de filhotes.

A Figura abaixo mostra a reprodução dos coelhos até o sexto mês.

Na Tabela abaixo, segue a solução resumida até o 12º mês, onde haverá 144 pares de coelhos.

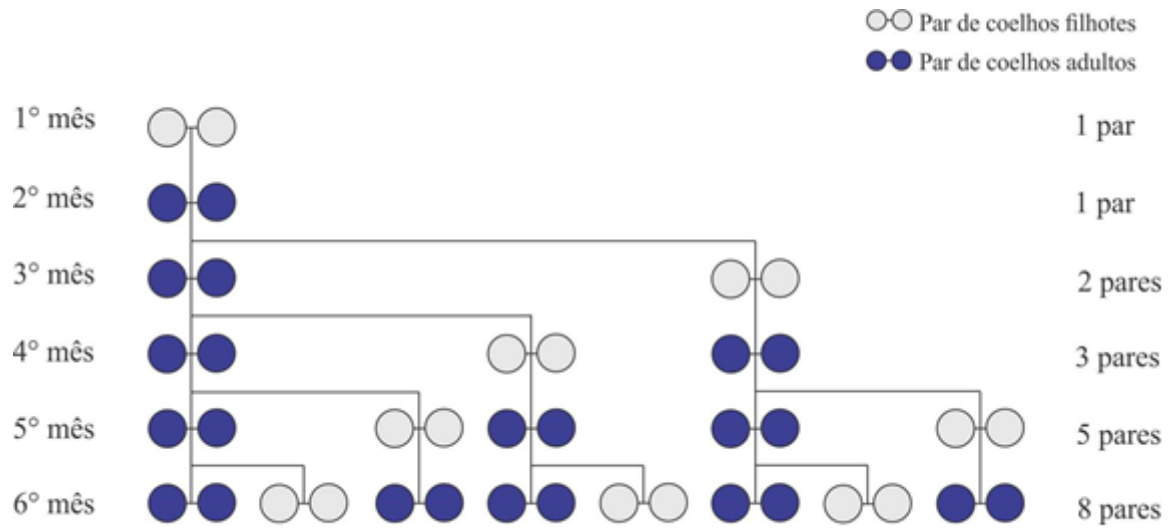


Figura 4.1: figura 1 reais coelhos de fibonacci

Mês	Nº de pares de adultos	Nº de pares de filhotes	Total
1º	0	1	1
2º	1	0	1
3º	1	1	2
4º	2	1	3
5º	3	2	5
6º	5	3	8
7º	8	5	13
8º	13	8	21
9º	21	13	34
10º	34	21	55
11º	55	34	89
12º	89	55	144

Tabela 1.1: Solução resumida do problema da reprodução de coelhos.

Considerando que no problema anterior não haja morte e nem migração de coelhos (nem de dentro pra fora e nem de fora pra dentro), sua generalização é dada por:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots, f_n, f_{n+1}, f_{n+2}, \ldots,$$

onde,

$$f_{n+2} = f_{n+1} + f_n, \text{ com } n \geq 0 \text{ e } f_0 = f_1 = 1$$

Essa relação define, por recorrência, uma sequência de números naturais, chamada *Sequência de Fibonacci*, cujos termos são chamados de *Números de Fibonacci*. Os Números de Fibonacci apresentam propriedades aritméticas notáveis que são, até hoje, objeto de investigação. Existe até uma revista intitulada *The Fibonacci Quarterly*, fundada em 1963, dedicada à pesquisa em torno desses números. Mas o que mais nos impressiona é o fato de que esses números aparecem na geometria, na Teoria dos Números, na genética, assim como surgem, inesperadamente, em fenômenos aparentemente desconexos, tais como, na distribuição das sementes dentro de um girassol, na árvore genealógica de um zangão e na relação com o Número de Ouro, como veremos mais adiante.

Problema: Determine o número de Fibonacci F_n

Utilizaremos Recorrências Lineares de Segunda ordem para solucionar o problema. A cada recorrência linear de segunda ordem homogênea, com coeficientes constantes, da forma $x_{n+2} + px_{n+1} + qx_n = 0$, associaremos uma equação do segundo grau, $r^2 + pr + q = 0$, chamada equação característica. A nossa suposição preliminar de ser $q \neq 0$ implica 0 não ser raiz da equação característica.

Teorema 4.47. *Se t_1 e t_2 são raízes da equação $t^2 - pt - q = 0$, então $x_n = c_1 t_1^n + c_2 t_2^n$ é solução da recorrência $a_n - pa_{n-1} - qa_{n-2} = 0$ para quaisquer valores de c_1 e c_2 .*

Demonstração: Substituindo $x_n = c_1 t_1^n + c_2 t_2^n$ em $a_n - pa_{n-1} - qa_{n-2}$ e agrupando os termos, obtemos:

$$\begin{gathered} c_1 t_1^n + c_2 t_2^n - p(c_1 t_1^{n-1} + c_2 t_2^{n-1}) - q(c_1 t_1^{n-2} + c_2 t_2^{n-2}) = \\ c_1(t_1^n - pt_1^{n-1} - qt_1^{n-2}) + c_2(t_2^n - pt_2^{n-1} - qt_2^{n-2} = \\ c_1 t_1^{n-2}(t_1^2 - pt_1 - q) + c_2 t_2^{n-2}(t_2^2 - pt_2 - q) = \\ c_1 t_1^{n-2} \cdot 0 + + c_2 t_2^{n-2} \cdot 0 = 0 \end{gathered}$$

Então x_n é solução.

4.3.2 Resolução de recorrências de segunda ordem

Teorema 4.48. *Se t_1 e t_2 com $t_1 \neq t_2$ e t_1, $t_2 \neq 0$, são raízes da equação característica , então todas as soluções da recorrência $a_n - pa_{n-1} - qa_{n-2} = 0$ são da forma $x_n = c_1 t_1^n + c_2 t_2^n$ com c_1 e c_2 constantes.*

Demonstração: Seja u_n uma solução qualquer de $a_n - pa_{n-1} - qa_{n-2} = 0$.

Vamos primeiro tentar escrever u_1 e u_2 na forma desejada. Ou seja, vamos tentar determinar c_1 e c_2 tais que u_n seja da forma $c_1 t_1^n + c_2 t_2^n$.

Escrevendo igualdades para u_1 e u_2, podemos formar um sistema de equações do qual as constantes c_1 e c_2 sejam as soluções:

$$\begin{cases} c_1 t_1 + c_2 t_2 = u_1 \\ c_1 t_1^2 + c_2 t_2^2 = u_2 \end{cases}$$

Ou seja,

$$c_1 = \frac{u_1 t_2 - u_2}{t_1(t_2 - t_1)} \text{ e } c_2 = \frac{u_2 - u_1 t_1}{t_2(t_2 - t_1)}$$

Note que, estas soluções são possíveis já que $t_1 \neq t_2$ e t_1, $t_2 \neq 0$.

Tomemos $v_n = u_n - c_1 t_1^n - c_2 t_2^n$. Vamos provar que $v_n = 0$ para todo n.

Temos,

$$v_n - pv_{n-1} - qv_{n-2} = (u_n - pu_{n-1} - qu_{n-2}) - c_1 t_1^{n-2}(t_1^2 - pt_1 - q) - c_2 t_2^{n-2}(t_2^2 - pt_2 - q).$$

O primeiro parêntese é igual a zero já que u_n é solução de $a_n - pa_{n-1} - qa_{n-2} = 0$ e os dois últimos parênteses são iguais a zero pois t_1 e t_2 são raízes da equação $t^2 - pt - q = 0$. Assim, $v_n - pv_{n-1} - qn_{n-2} = 0$.

Além disso, como $c_1 t_1 + c_2 t_2 = u_1$ e $c_1 t_1^2 + c_2 t_2^2 = u_2$, temos $v_1 = v_2 = 0$. Entretanto, se $v_n - pv_{n-1} - qn_{n-2} = 0$ e $v_1 = v_2 = 0$ então $v_n = 0$ para todo n.

4.3.3 A solução do problema (F_n)

A equação da recorrência pode ser reescrita como $F_{n+2} - F_{n+1} - F_n = 0$, cuja equação característica é $x^2 - x - 1 = 0$, que por sua vez tem como raízes:

$$\alpha = \frac{1 + \sqrt{5}}{2} \text{ e } \beta = \frac{1 - \sqrt{5}}{2}$$

As soluções de uma recorrência com tal expressão são da forma:

$$F_n = A \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + B \cdot \left((\frac{1-\sqrt{5}}{2}\right)^n$$

Além disso, a sequência de Fibonacci tem $F_1 = F_2 = 1$. E assim podemos montar o sistema:

$$\begin{cases} A \cdot \left(\frac{1+\sqrt{5}}{2}\right) + B \cdot \left(\frac{1-\sqrt{5}}{2}\right) = 1 \\ A \cdot \left(\frac{1+\sqrt{5}}{2}\right)^2 + B \cdot \left(\frac{1-\sqrt{5}}{2}\right)^2 = 1 \end{cases}$$

Resolvendo o sistema chegamos às constantes

$$A = \frac{1}{\sqrt{5}} \text{ e } B = -\frac{1}{\sqrt{5}}$$

Portanto, a solução da recorrência é dada por:

$$F_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Esta fórmula é conhecida por fórmula de Binet, que a descobriu em 1843.

Observemos que o resultado obtido é uma solução para um caso particular da recorrência $x_{n+2} = x_{n+1} + x_n$. Caso esse, que chamamos de sequência de Fibonacci. Note que a solução da equação característica, $\alpha = \frac{1+\sqrt{5}}{2}$, é o chamdo número de ouro, obtido através da razão áurea.

4.3.4 Uma outra aplicação (O conjunto de Cantor)

Georg Ferdinand Ludwig Philipp Cantor (1845-1918) foi um matemático russo nascido no Império Russo. Conhecido por ter elaborado a moderna teoria dos conjuntos, foi a partir desta teoria que chegou ao conceito de número transfinito, incluindo as classes numéricas dos cardinais e ordinais e estabelecendo a diferença entre estes dois conceitos, que colocam novos problemas quando se referem a conjuntos infinitos. Nasceu em São Petersburgo (Rússia), filho do comerciante dinamarquês, George Waldemar Cantor, e de uma musicista russa, Maria Anna Böhm. Em 1856 sua família mudou-se para a Alemanha, continuando aí os seus estudos. Estudou no Instituto Federal

de Tecnologia de Zurique. Doutorou-se na Universidade de Berlim em 1867. Teve como professores Ernst Kummer, Karl Weierstrass e Leopold Kronecker. Em 1872 foi docente na Universidade de Halle-Wittenberg, na cidade alemã Halle an der Saale, onde obteve o título de professor em 1879. Toda a sua vida irá tentar em vão deixar a cidade, tendo acabado por pensar que era vítima de uma conspiração. Cantor provou que os conjuntos infinitos não têm todos a mesma potência (potência significando "tamanho"). Fez a distinção entre conjuntos numeráveis (ou enumeráveis) (em inglês chamam-se countable - que se podem contar) e conjuntos contínuos (ou não-enumeráveis) (em inglês uncountable - que não se podem contar). Provou que o conjunto dos números racionais é enumerável, enquanto que o conjunto dos números reais é contínuo (logo, maior que o anterior). Na demonstração foi utilizado o célebre argumento da diagonal de Cantor ou método diagonal. Nos últimos anos de vida tentou provar, sem o conseguir, a "hipótese do contínuo", ou seja, que não existem conjuntos de potência intermédia entre os numeráveis e os contínuos - em 1963, Paul Cohen demonstrou a indemonstrabilidade desta hipótese. Em 1897, Cantor descobriu vários paradoxos suscitados pela teoria dos conjuntos. Foi ele que utilizou pela primeira vez o símbolo $s \in \mathbb{R}$ para representar o conjunto dos números reais. Durante a última metade da sua vida sofreu repetidamente de ataques de depressão, o que comprometeu a sua capacidade de trabalho e o forçou a ficar hospitalizado várias vezes. Provavelmente ser-lhe-ia diagnosticado, hoje em dia, um transtorno bipolar - vulgo maníaco-depressivo. A descoberta do Paradoxo de Russell conduziu-o a um esgotamento nervoso do qual não chegou a se recuperar. Começou, então, a se interessar por literatura e religião. Desenvolveu o seu conceito de Infinito Absoluto, que identificava a Deus. Ficou na penúria durante a Primeira Guerra Mundial, morrendo num hospital psiquiátrico em Halle.

O conjunto de Cantor

O conjunto de Cantor,em homenagem ao matemático Georg Cantor (1845 - 1918), é construído como a seguir.

Começamos com o intervalo fechado $[0, 1]$ e removemos o intervalo aberto $\left(\frac{1}{3}, \frac{2}{3}\right)$. Isso nos leva a dois intervalos, $\left[0, \frac{1}{3}\right]$ e $\left[\frac{2}{3}, 1\right]$. Dividimos novamente cada intervalo em três e removemos cada terço intermediário aberto. Quatro intervalos permanecem, e novamente repetimos o processo. Continuamos esse procedimento indefinidamente, em cada passo removendo o terço do meio de cada intervalo aberto que permanece do passo anterior. O conjunto de Cantor consiste nos números que permanecem em $[0, 1]$ depois de todos os intervalos terem sidos removidos.

(a)Mostre que o comprimento total de todos os intervalos que foram removidos é 1. Apesar

disso, o conjunto de Cantor contém infinitos números. Dê exemplos de alguns números no conjunto de Cantor.

Solução:

Na primeira etapa, somente o intervalo$\left(\frac{1}{3};\frac{2}{3}\right)$(comprimento $\frac{1}{3}$) é removido.

Na segunda etapa, removemos $\left(\frac{1}{9};\frac{2}{9}\right)$ e $\left(\frac{7}{9};\frac{8}{9}\right)$, no qual o comprimento total é 2. $\left(\frac{1}{3}\right)^2$.

Na terceira etapa removemos 2^2 intervalos de comprimento $\left(\frac{1}{3}\right)^3$. Em geral, na enésima etapa removemos 2^{n-1} intervalos, com comprimento $\left(\frac{1}{3}\right)^n$ cada.

Logo removemos $2^{n-1}\cdot\left(\frac{1}{3}\right)^n = \frac{1}{3}\cdot\left(\frac{2}{3}\right)^{n-1}$. Portanto o total de todos comprimentos removidos é $A_R = \sum_{n=1}^{\infty}\frac{1}{3}\cdot\left(\frac{2}{3}\right)^{n-1} = \frac{\frac{1}{3}}{1-\frac{2}{3}} = 1$.

(b) **O carpete de Sierpinsk** é o correspondente bidimensional do conjunto de Cantor. Ele é construído pela remoção do nono subquadrado central de um quadrado de lado 1 dividido em nove subquadrados. A etapa seguinte consiste em remover os subquadrados centrais dos oito quadrados menores que permaneceram, e assim por diante. (A figura apresenta as três primeirras etapas da construção). Mostre que a soma das áreas dos quadrados removidos é 1. Isso implica que o carpete de Sierpinski tem área 0.

?

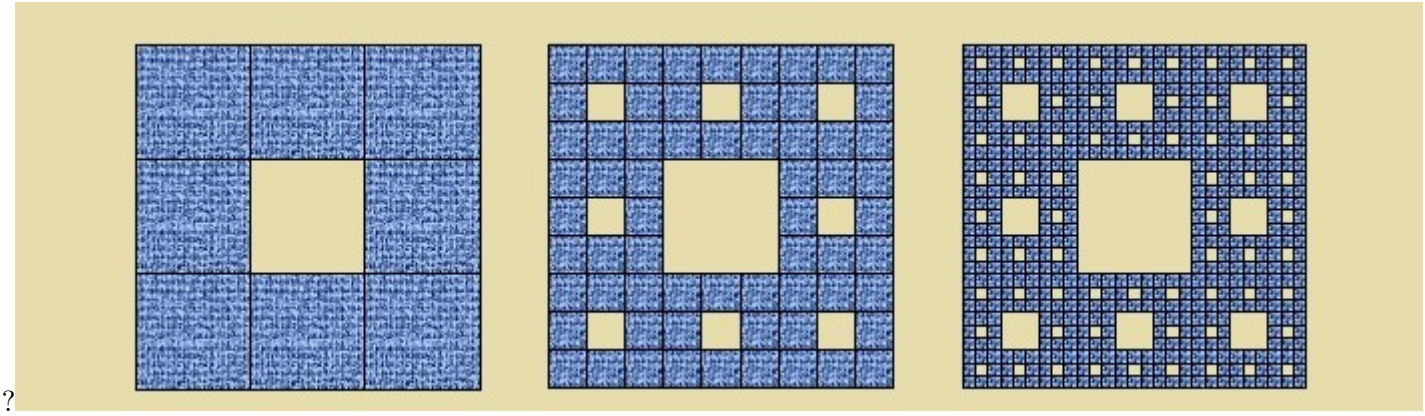


Figura 4.2: figura 2 reais carpete

Solução:

A área removida na 1º etapa é $\frac{1}{9}$. Já na segunda etapa $8\cdot\left(\frac{1}{9}\right)^2$. Na terceira etapa $8^2\cdot\left(\frac{1}{9}\right)^3$.

Em geral, na enésima etapa temos $8^{n-1} \cdot \left(\frac{1}{9}\right)^n = \frac{1}{9} \cdot \left(\frac{8}{9}\right)^{n-1}$. Assim o total da área removida é dada por

$$A_R = \sum \frac{1}{9} \left(\frac{8}{9}\right)^{n-1} = \frac{\frac{1}{9}}{1 - \frac{8}{9}} = 1$$

Capítulo 5

Construção de Conjuntos Imaginários

Neste capítulo, usaremos o conjunto dos números reais para obter, de forma precisa, a definição, e algumas propriedades aritméticas básicas, dos números complexos.

5.1 Construção dos Números Complexos

No ensino elementar, os números complexos são introduzidos a partir da chamada "unidade imaginária", i, com a propriedade de que $i^2 = -1$. Este mesmos números são definidos através de uma expressão da forma $a + bi$, onde $a, b \in \mathbb{R}$, sujeitas às regras operacionais conhecidas dos números reais.

Nesta seção, será feita a construção rigorosa dos números complexos. A referência que serviu como base nesta seção está apresentada em [3].

5.1.1 Operações Elementares em $\mathbb{C}$

Aprendemos, no ensino básico, que dois números complexos da forma $a + bi$ e $c + di$, são iguais apenas quando $a = c$ e $b = d$. O que nos lembra a igualdade entre os pares ordenados (a, b) e (c, d) em $\mathbb{R}^2$ (aqui $\mathbb{R}^2 = \{(x, y)/x, y \in \mathbb{R}\}$). Assim sendo, vamos estabelecer nossa definição dos números complexos através de $\mathbb{R}^2$. Mais precisamente, temos o seguinte conceito.

Definição 5.1. Sejam $(a, b), (c, d) \in \mathbb{R}^2$. Definimos a operação $+ : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$, chamada adição, como sendo

$$(a, b) + (c, d) = (a + c, b + d), \forall (a, b), (c, d) \in \mathbb{R}^2.$$

Exemplo 5.1. É fácil ver que

$$(\sqrt{2}, 1) + (-1, 3) = (\sqrt{2} + (-1), 1 + 3) = (\sqrt{2} - 1, 4).$$

Nossa meta principal com a adição é apresentar as propriedades elementares que esta satisfaz em $\mathbb{R}^2$.

Comecemos com a comutatividade.

Teorema 5.1 (Comutatividade)**.** *Sejam* $(a, b), (c, d) \in \mathbb{R}^2$*. Então,* $(a, b) + (c, d) = (c, d) + (a, b)$.

Demonstração. É fácil checar que

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

Isto completa a prova do teorema em questão. □

Agora, verifiquemos a associatividade.

Teorema 5.2 (Associatividade)**.** *Sejam* $(a, b), (c, d), (e, f) \in \mathbb{R}^2$*. Então,*

$$[(a, b) + (c, d)] + (e, f) = (a, b) + [(c, d) + (e, f)].$$

Demonstração. Note que

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

Isto prova o teorema em questão. □

Agora, permita-nos mostrar que $(0, 0)$ é o único elemento neutro de $\mathbb{R}^2$.

Teorema 5.3 (Elemento Neutro)**.** *Seja* $(a, b) \in \mathbb{R}^2$*. Então,* $(a, b) + (0, 0) = (a, b)$*. Além disso,* $(0, 0)$ *é o único elemento de* $\mathbb{R}^2$ *que satisfaz esta igualdade.*

Demonstração. É fácil ver que

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b).$$

Agora, considere que $(c,d) \in \mathbb{R}^2$ é tal que $(a,b)+(c,d) = (a,b)$, para todo $(a,b) \in \mathbb{R}^2$. Dessa forma, chegamos a

$$(0,0) = (0,0) + (c,d) = (0+c, 0+d) = (c,d).$$

Como queríamos demonstrar. □

Vejamos, agora, como provar a existência única do simétrico para cada elemento de $\mathbb{R}^2$.

Teorema 5.4 (Simétrico)**.** *Seja $(a,b) \in \mathbb{R}^2$. Então, $(a,b)+(-a,-b) = (0,0)$. Além disso, $(-a,-b)$ é o único elemento de $\mathbb{R}^2$ que satisfaz esta igualdade.*

Demonstração. Note que

$$(a,b) + (-a,-b) = (a+(-a), b+(-b)) = (0,0).$$

Suponha que existe $(c,d) \in \mathbb{R}^2$ tal que $(a,b)+(c,d) = (0,0)$. Assim, chegamos a

$$\begin{aligned}(c,d) &= (c,d) + (0,0) = (c,d) + [(a,b) + (-a,-b)] \\ &= [(c,d) + (a,b)] + (-a,-b) = [(a,b) + (c,d)] + (-a,-b) \\ &= (0,0) + (-a,-b) = (-a,-b).\end{aligned}$$

□

O Teorema 5.4 nos permite definir a subtração entre dois elementos de $\mathbb{R}^2$ da seguinte forma:

$$(a,b) - (c,d) := (a,b) + (-c,-d) = (a-c, b-d),\ \forall (a,b),(c,d) \in \mathbb{R}^2.$$

O resultado abaixo estabelece a famosa lei do cancelamento em $\mathbb{R}^2$.

Teorema 5.5. *Sejam $(a,b),(c,d),(e,f) \in \mathbb{R}^2$. Então,*

$$(a,b) + (e,f) = (c,d) + (e,f) \Leftrightarrow (a,b) = (c,d).$$

Demonstração. A partir das propriedades de $\mathbb{R}$, concluímos que

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

□

Agora, vamos estabelecer a definição da multiplicação entre dois elementos de $\mathbb{R}^2$.

Definição 5.2. Sejam $(a,b),(c,d) \in \mathbb{R}^2$. Definimos a operção $\cdot : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$, chamada multiplicação, como sendo

$$(a,b)\cdot(c,d) = (ac - bd, ad + bc),\ \forall (a,b),(c,d) \in \mathbb{R}^2.$$

Abaixo destacamos as provas das propriedades aritméticas para a multiplicação em $\mathbb{R}^2$.

Comecemos com a comutatividade.

Teorema 5.6 (Comutatividade)**.** *Sejam* $(a,b),(c,d) \in \mathbb{R}^2$*. Então,* $(a,b)\cdot(c,d) = (c,d)\cdot(a,b)$.

Demonstração. É fácil checar que

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

Isto completa a prova do teorema em questão. □

Verifiquemos a associatividade.

Teorema 5.7 (Associatividade)**.** *Sejam* $(a,b),(c,d),(e,f) \in \mathbb{R}^2$*. Então,*

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

Demonstração. Note que

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

Isto prova o teorema em questão. □

Agora, permita-nos mostrar que $(1,0)$ é o único elemento neutro de $\mathbb{R}^2$.

Teorema 5.8 (Elemento Neutro)**.** *Seja* $(a,b) \in \mathbb{R}^2$*. Então,* $(a,b)\cdot(1,0) = (a,b)$*. Além disso,* $(1,0)$ *é o único elemento de* $\mathbb{R}^2$ *que satisfaz esta igualdade.*

Demonstração. É fácil ver que

$$(a,b)\cdot(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b).$$

Agora, considere que $(c,d)\in\mathbb{R}^2$ é tal que $(a,b)\cdot(c,d) = (a,b)$, para todo $(a,b)\in\mathbb{R}^2$. Dessa forma, chegamos a

$$(1,0) = (1,0)\cdot(c,d) = (c,d)\cdot(1,0) = (c,d).$$

Como queríamos demonstrar. □

Vejamos, agora, como provar a existência única do inverso para cada elemento não nulo de $\mathbb{R}^2$.

Teorema 5.9 (Inverso)**.** *Seja $(a,b)\in\mathbb{R}^2$ tal que $(a,b)\neq(0,0)$. Então,*

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

Além disso, $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ é o único elemento de $\mathbb{R}^2$ que satisfaz esta igualdade.

Demonstração. Note que

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) &= \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ba}{a^2+b^2}\right)\\ &= \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right)\\ &= (1,0).\end{aligned}$$

Suponha que existe $(c,d)\in\mathbb{R}^2$ tal que $(a,b)\cdot(c,d) = (1,0)$. Assim, chegamos a

$$\begin{aligned}(c,d) &= (c,d)\cdot(1,0) = (c,d)\cdot\left[(a,b)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)\right]\\ &= [(c,d)\cdot(a,b)]\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = [(a,b)\cdot(c,d)]\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)\\ &= (1,0)\cdot\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).\end{aligned}$$

□

Em muitos casos, o inverso de um elemento $(a,b)\in\mathbb{R}^2$ é denotado por $(a,b)^{-1}$.

O Teorema 5.9 nos permite definir a divisão entre dois elementos de $\mathbb{R}^2$ da seguinte forma:

$$(a,b):(c,d) := (a,b)\cdot\left(\frac{c}{c^2+d^2}, \frac{-d}{c^2+d^2}\right) = \left(\frac{ac+bd}{c^2+d^2}, \frac{-ad+bc}{c^2+d^2}\right), \forall (a,b),(c,d)\in\mathbb{R}^2,$$

onde $(c,d)\neq(0,0)$.

Exemplo 5.2. Temos que

$$\left(\frac{1}{3},-2\right)^{-1}=\left(\frac{\frac{1}{3}}{(\frac{1}{3})^2+(-2)^2},\frac{-(-2)}{(\frac{1}{3})^2+(-2)^2}\right)=\left(\frac{\frac{1}{3}}{\frac{37}{9}},\frac{2}{\frac{37}{9}}\right)=\left(\frac{3}{37},\frac{18}{37}\right).$$

Consequentemente,

$$\begin{aligned}(3,2):\left(\frac{1}{3},-2\right)&=(3,2)\cdot\left(\frac{3}{37},\frac{18}{37}\right)=\left(3\frac{3}{37}-2\frac{18}{37},3\frac{18}{37}+2\frac{3}{37}\right)\\&=\left(\frac{9-36}{37},\frac{54+6}{37}\right)=\left(-\frac{27}{37},\frac{60}{37}\right).\end{aligned}$$

É também verdade que a propriedade distributiva, envolvendo a adição e a multiplicação, é válida em $\mathbb{R}^2$.

Teorema 5.10 (Distributividade)**.** *Sejam* $(a,b),(c,d),(e,f)\in\mathbb{R}^2$*. Então,*

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

Demonstração. Este resultado segue diretamente da igualdades abaixo:

$$\begin{aligned}(a,b)\cdot[(c,d)+(e,f)]&=(a,b)\cdot(c+e,d+f)=(a(c+e)-b(d+f),a(d+f)+b(c+e))\\&=(ac+ae-bd-bf,ad+af+bc+be)=(ac-bd+ae-bf,ad+bc+af+be)\\&=(ac-bd,ad+bc)+(ae-bf,af+be)=(a,b)\cdot(c,d)+(a,b)\cdot(e,f).\end{aligned}$$

□

Permita-nos, agora, provar a lei do corte em $\mathbb{R}^2$.

Teorema 5.11. *Sejam* $(a,b),(c,d),(e,f)\in\mathbb{R}^2$ *tais que* $(e,f)\neq(0,0)$*. Então,*

$$(a,b)\cdot(e,f)=(c,d)\cdot(e,f)\Leftrightarrow(a,b)=(c,d).$$

Demonstração. ($\Leftarrow$) Na verdade, esta implicação vale para qualquer $(e,f)\in\mathbb{R}^2$. Note que, $(a,b)=(c,d)$ implica que $a=c$ e $b=d$. Dessa forma,

$$(a,b)\cdot(e,f)=(ae-bf,af+be)=(ce-df,cf+de)=(c,d)\cdot(e,f).$$

($\Rightarrow$) Suponha que $(a,b)\cdot(e,f)=(c,d)\cdot(e,f)$. Como $(e,f)\neq(0,0)$, então existe $(e,f)^{-1}\in\mathbb{R}^2$ tal que $(e,f)\cdot(e,f)^{-1}=(1,0)$. Consequentemente,

$$[(a,b)\cdot(e,f)]\cdot(e,f)^{-1}=[(c,d)\cdot(e,f)]\cdot(e,f)^{-1}.$$

Portanto, pelos Teoremas 5.7, 5.9 e 5.8, chegamos a $(a, b) = (c, d)$.

□

Definição 5.3. O conjunto $\mathbb{R}^2$, dotado com as operações de adição e multiplicação, definidas acima, será denominado conjunto dos números complexos e denotado por $\mathbb{C}$.

5.1.2 Caracterização Usual de $\mathbb{C}$

Nesta subseção, vamos mostrar uma maneira de garantir a inclusão do conjunto dos números reais em $\mathbb{C}$. Primeiramente, observemos como escrever um número complexo arbitrário da forma usual. Sendo assim, é sabido que

$$(a, 0) + (b, 0) \cdot (0, 1) = (a, 0) + (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (a, 0) + (0, b) = (a, b).$$

Portanto,

$$(a, b) = (a, 0) + (b, 0) \cdot (0, 1), \forall (a, b) \in \mathbb{C}.$$

Agora, vejamos como identificar os elementos da forma $(a, 0) \in \mathbb{C}$ com $a \in \mathbb{R}$.

Teorema 5.12. *Seja $f_{\mathbb{R}} : \mathbb{R} \to \mathbb{C}$ uma função dada por $f_{\mathbb{R}}(x) = (x, 0)$, para todo $x \in \mathbb{R}$. Então, os seguintes itens são válidos:*

i) *$f_{\mathbb{R}}$ é injetora;*

ii) $f_{\mathbb{R}}(x + y) = f_{\mathbb{R}}(x) + f_{\mathbb{R}}(y), \forall x, y \in \mathbb{R}$;

iii) $f_{\mathbb{R}}(xy) = f_{\mathbb{R}}(x) \cdot f_{\mathbb{R}}(y), \forall x, y \in \mathbb{R}$.

Demonstração. **i)** É fácil ver $f_{\mathbb{R}}$ é injetora, pois

$$f_{\mathbb{R}}(x) = f_{\mathbb{R}}(y) \Leftrightarrow (x, 0) = (y, 0) \Leftrightarrow x = y;$$

ii) Além disso,

$$f_{\mathbb{R}}(x) + f_{\mathbb{R}}(y) = (x, 0) + (y, 0) = (x + y, 0) = f_{\mathbb{R}}(x + y), \forall x, y \in \mathbb{R};$$

iii) Por fim,

$$f_{\mathbb{R}}(xy) = (xy, 0) = (x, 0) \cdot (y, 0) = f_{\mathbb{R}}(x) \cdot f_{\mathbb{R}}(y), \forall x, y \in \mathbb{R}.$$

□

De modo similar aos casos estudados anteriormente, aqui também temos em $\mathbb{C}$ uma cópia algébrica de $\mathbb{R}$, $f_{\mathbb{R}}(\mathbb{R})$, o que nos permite identificar $\mathbb{R}$ com $f_{\mathbb{R}}(\mathbb{R})$ e, portanto, considerar $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subset \mathbb{C}$. Admitindo essa identificação e adotando o símbolo i para o número complexo $(0,1)$, a expressão para (a,b), que é igual a $(a,0)+(b,0)\cdot(0,1)$, pode ser escrita como $a+bi$, como fazíamos no ensino elementar. Neste caso, temos

$$\mathbb{C} = \{a + bi / a, b \in \mathbb{R}\}.$$

Notemos ainda que, como no ensino básico, vale:

$$i^2 := i \cdot i = (0,1) \cdot (0,1) = (-1,0) = -1,$$

por $f_{\mathbb{R}}$.

Definição 5.4. Sob a notação acima, chamamos os elementos $bi \in \mathbb{C}$, com $b \neq 0$ imaginários puros. Já os números $a \in \mathbb{C}$ são denominados reais puros.

5.1.3 Módulos e Conjugados em $\mathbb{C}$

Nesta subseção, definiremos, de forma usual, a definição do que significa o módulo e o conjugado de um número complexo.

Definição 5.5. Dado o complexo $z = a + bi \in \mathbb{C}$, definimos o módulo de z como sendo o número real $|z| = \sqrt{a^2 + b^2}$.

Observe que quando um número complexo é real puro então a definição de módulo coincide com a de módulo de um número real.

Exemplo 5.3. É fácil notar que

$$|1 - i| = \sqrt{1^2 + (-1)^2} = \sqrt{1+1} = \sqrt{2}.$$

Definição 5.6. Dado $z = a + bi \in \mathbb{C}$, definimos o conjugado complexo de z como sendo $\overline{z} := a - bi$.

Veja que, pela definição acima, o conjugado de um número complexo é um número da mesma categoria.

Exemplo 5.4. É fácil ver que $\overline{(\sqrt{2} + 3i)} = \sqrt{2} - 3i$.

Vejamos algumas propriedades para o conjugado de um número complexo.

Proposição 5.1. *Sejam $z, w \in \mathbb{C}$. Então, valem as seguintes propriedades:*

i) $\overline{\overline{z}} = z$;

ii) $\overline{z+w} = \overline{z} + \overline{w}$;

iii) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;

iv) $z \cdot \overline{z} = |z|^2$.

Demonstração. Sejam $z = a + bi$ e $w = c + di \in \mathbb{C}$. Então,

i) $\overline{z} = a - bi$ e, então

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

ii) Também temos que $\overline{w} = c - di$ e, assim,

$$\overline{z} + \overline{w} = (a - bi) + (c - di) = (a + c) - (b + d)i = \overline{z + w};$$

iii) É fato que

$$\overline{z} \cdot \overline{w} = (a - bi) \cdot (c - di) = (ac - bd) - (ad + bc)i = \overline{z \cdot w};$$

iv) Por fim, concluímos que

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

□

5.1.4 $\mathbb{C}$ não enumerável e não Ordenável

A seguir veremos que a não enumerabilidade de $\mathbb{C}$ (o que não ocorre com $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$) segue diretamente da de $\mathbb{R}$.

Teorema 5.13. *$\mathbb{C}$ é não enumerável.*

Demonstração. Vimos que $\mathbb{R} \subset \mathbb{C}$. Pela Proposição 1.19, se $\mathbb{C}$ fosse enumerável, $\mathbb{R}$ também deveria ser, o que contradiz o que já mostramos. Portanto, $\mathbb{C}$ é não enumerável. □

É notório que as propriedades aritméticas de $\mathbb{C}$, dadas anteriormente, são as mesmas que as de $\mathbb{R}$ (que são as mesmas que as de $\mathbb{Q}$), sendo assim, podemos dizer que $\mathbb{C}$ é um corpo.

Apesar de os corpos $\mathbb{Q}$ e $\mathbb{R}$ serem dotados de uma relação de ordem compatível com suas operações e são, portanto, ambos ordenados, temos que $\mathbb{R}$ é um corpo ordenado completo e $\mathbb{Q}$ é um corpo ordenado não completo.

Intuitivamente não temos como dizer se 3 é maior do que $3i$ ou do que $2 + i$, por exemplo. Mostremos que $\mathbb{C}$ é um corpo não ordenável (o que não ocorre com $\mathbb{Q}$ e $\mathbb{R}$), ou seja, é impossível dotar $\mathbb{C}$ de uma relação de ordem compatível com suas operações aritméticas. No entanto, $\mathbb{C}$ possui uma importante informação algébrica que $\mathbb{R}$ e $\mathbb{Q}$ não têm: o *Teorema Fundamental da Álgebra*, cuja demonstração foi a tese de doutoramento do ilustre matemático, Johann Carl Friedrich Gauss(Braunschweig, 30 de abril de 1777 - Göttingen, 23 de fevereiro de 1855), o qual afirma que todo polinômio não constante com coeficientes complexos admite uma raiz em $\mathbb{C}$ (este resultado não é de nosso interesse). (A demonstração algébrica deste teorema encontra-se em [2]).

Teorema 5.14. $\mathbb{C}$ *não é um corpo ordenável.*

Demonstração. Se $\mathbb{C}$ fosse um corpo ordenável, pela Proposição 3.16, teríamos que $x^2 \geq 0$, para todo $x \in \mathbb{C}$. Entretanto, é sabido que $i^2 = -1 < 0$, para $i \in \mathbb{C}$. Isto é uma contradição. Assim, $\mathbb{C}$ não é um corpo ordenável. □

5.2 Aplicação dos números complexos

5.2.1 Números Complexos e a Física

Há mais de 200 anos, a física e a matemática estão intimamente ligadas no que diz respeito a conjuntos numéricos. Embora não haja um estudo mais aprofundado, já se sabe que atualmente, na física contemporânea, a aplicação do conjunto dos números complexos é tão grande, que é até possível pensar em uma autêntica "complejificación de la física", como cita o autor Frederico de Rubio y Galy em "The Role of Mathematics in the Rise of Science". Nesta mesma obra, Dr Frederico dá aos números complexos a idéia de par ordenado: "um par ordenado de números reais, onde suas coordenadas representam a parte real e imaginária do complexo". Assim, apresenta como os números complexos podem multiplicar-se e como é simples a sua representação como vetor. Fica claro então, como o universo de complexos se expande no mundo da física, onde é utilizado pelos físicos contemporâneos de forma familiar em diversas teorias. Vejamos alguns exemplos.

Vetores e Quantidades Complexas

Dado um número complexo determinado por (a,b), onde a e b são números reais, podemos facilmente representá-lo em um plano. Tomando como base a localização de pares ordenados, localizamos o par (a,b) e formamos o vetor com origem em (0,0) e extremidade em (a,b). Para facilitar essa representação, vamos utilizar uma nova quantidade que chamaremos de operador i, embora alguns autores também o denominam operador j. Observemos a figura: O vetor H,

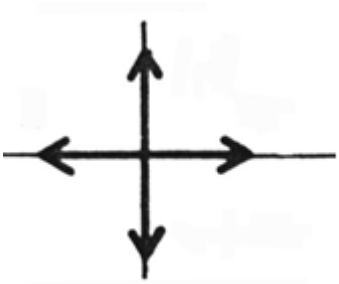


Figura 5.1: Sistema Complexo (a, b).

representado sobre o eixo de referência, à direita do eixo vertical está sofrendo uma rotação. Ao se deslocar para a esquerda do eixo vertical, temos o vetor $-$ H , que é o próprio vetor H multiplicado por -1. Então, para fazer com que o vetor gire 180° é necessário multiplicá-lo por -1, para que sua rotação seja de 90° (e o vetor se localize sobre o eixo vertical) é necessário multiplicá-lo por i , pois $i^2.i^2$ = -1. Assim, qualquer vetor multiplicado por i, sofre uma rotação de 90° . Portanto, na figura anterior temos: Esta representação onde o vetor acompanhado de +i está no eixo vertical

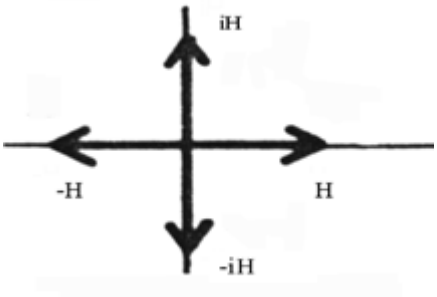


Figura 5.2: Sistema Complexo Rotacional

para cima e acompanhado de $-$i está no eixo vertical para baixo é chamada forma complexa.

Números complexos e circuitos monofásicos

No estudo de circuitos, a aplicação de números complexos aparece na forma de vetores, que determinam algumas equações importantes, com a presença da unidade imaginária. Um circuito monofásico é alimentado por uma única tensão alternada. Quando a única dificuldade que a tensão sofre é a resistência efetiva, o circuito é dito puramente resistivo. Nesse circuito, a tensão Er e a intensidade de corrente I atingem valores correspondentes ao mesmo tempo, o que faz com que os seus vetores representativos fiquem sobre o eixo de referência. Dizemos então que as grandezas estão em fase.

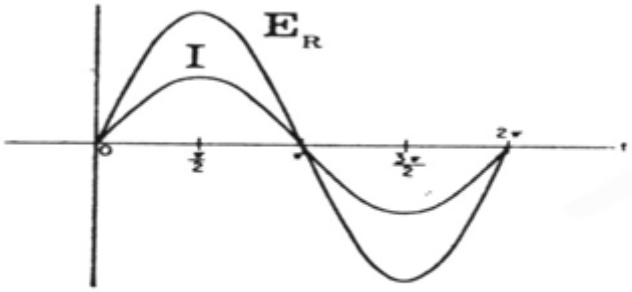


Figura 5.3: Comportamento de E e I em um circuito Resistivo.

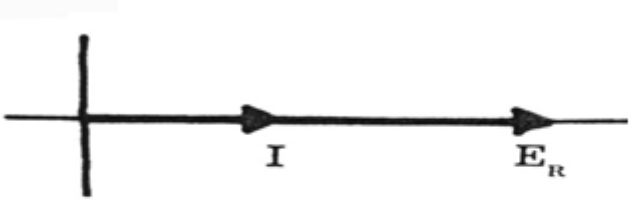


Figura 5.4: As grandezas E e I nos mesmos eixos de referências.

Quando a dificuldade que a corrente sofre é a reatância capacitiva, o circuito é chamado puramente capacitivo. Nesse circuito, Ec e I não atingem valores correspondentes ao mesmo tempo, de modo que os vetores que as representam fiquem um sobre cada eixo. Neste caso, dizemos que Ec e I estão defasadas 90° (I se antecipa aos valores de Ec). Quando o circuito apresenta como

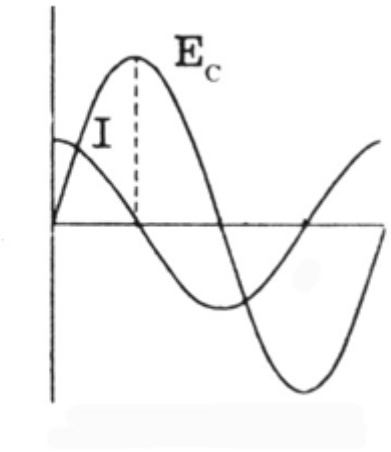


Figura 5.5: Comportamento de E e I em um circuito Capacitivo.

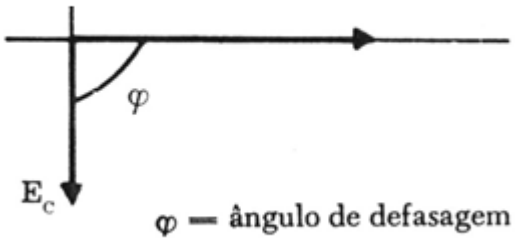


Figura 5.6: As grandezas E e I nos eixos de referências respectivos.

dificuldade à reatância indutiva, o circuito é chamado de puramente indutivo. Nesse circuito Ei e I também estão defasadas 90° (I está atrasada aos valores de Ei).

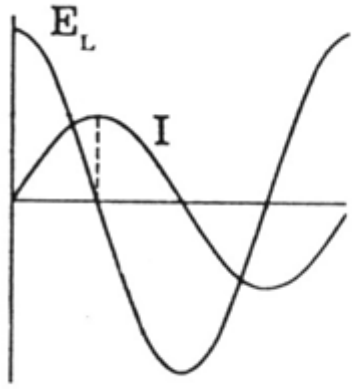


Figura 5.7: Comportamento de E e I em um circuito Indutivo.

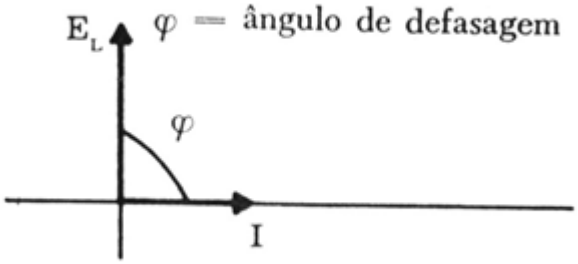


Figura 5.8: As grandezas E e I nos eixos de referências respectivos.

Circuito em fase tipo R-C

R e C simbolizam a resistência e a capacitância equivalente. Nesse circuito, a dificuldade encontrada pela fonte para estabelecer uma corrente no circuito é determinada pela soma vetorial de R e X_c.A tensão E é a soma vetorial das componentes Er e Ec. Observa-se que o ângulo de defasagem é menor que 90° , assim, podemos representar o vetor E na forma trigonométrica, onde $E = Ecos\theta - isen\theta$ ou na forma binômia $E = Er - iEc$.

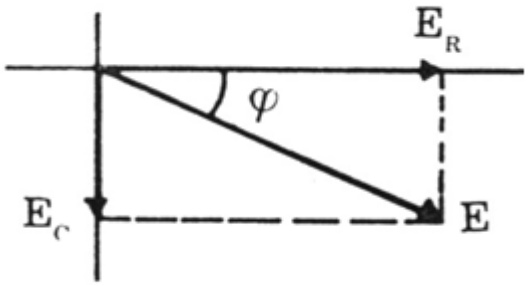


Figura 5.9: Circuito R-C.

Circuito em série tipo R-L-C

Neste tipo de circuito três situações podem ocorrer: No primeiro caso, o circuito comporta-se

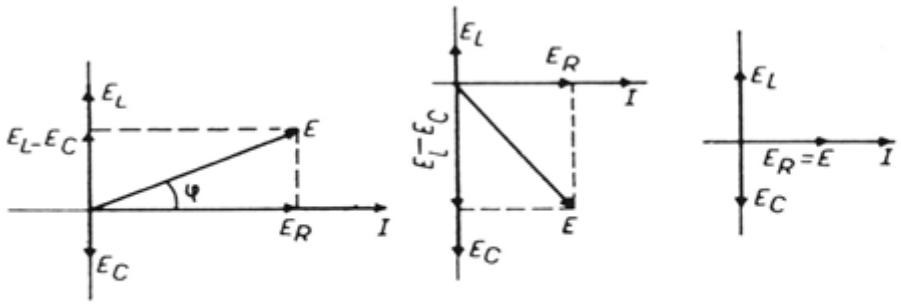


Figura 5.10: Circuito R-L-C.

como circuito indutivo, o segundo como capacitivo e o terceiro como resistivo. Nesse caso o vetor é representado na forma $E = Er + i(El - Ec) = Ecos\theta + isen\theta$.

Números complexos e sinais sinusoidais

Além das formas trigonométrica e binômial, os números complexos podem ser representado em notação exponencial, onde $Z = Pe^{i\theta}$, sendo P o módulo do complexo e θ o ângulo formado com o eixo de referência (argumento).

Esta propriedade dos complexos é muito utilizada para expressar as funções seno e cosseno em notação exponencial, onde:

$$cos(x) = \frac{e^{i(x)} + e^{-i(x)}}{2}$$
$$sen(x) = \frac{e^{i(x)} - e^{-i(x)}}{2i}$$

Assim, podemos representar as exponenciais complexas:

$$e^{i(x)} = cos(x) + isen(x)$$
$$e^{-i(x)} = cos(x) - isen(x)$$

Com isso, a resolução de uma equação com funções sinusoidais pode ser efetuada recorrendo a uma função exponencial complexa.

Números complexos e a função de onda

A equação de onda que rege o movimento dos elétrons foi obtida por Schrodinger em 1925. Erwin Rudolf Josef Alexander Schrödinger foi um físico teórico austríaco, conhecido por suas contribuições à mecânica quântica, especialmente a equação que recee o seu nome, pela qual recebeu o Nobel de Física em 1933. Propôs o experimento mental conhecido como o Gato de Schrödinger e participou da 4ª, 5ª, 7ª e 8ª Conferência de Solvay. Deu ainda grande atenção aos aspectos filosóficos da ciência, bem como a conceitos filosóficos, à ética e às religiões orientais e antigas.Sobre sua visão religiosa, ele era ateu. Em janeiro de 1926, Schrödinger publicou no Annalen der Physik o trabalho "Quantisierung als Eigenwertproblem"(Quantização como um Problema de Autovalor) em mecânica de ondas e que hoje é conhecido como a equação de Schrödinger. Neste trabalho ele deu uma "derivação"da equação de onda para sistemas independentes de tempo, e mostrou que fornecia autovalores de energia corretos para o átomo hidrogenoide. Este trabalho tem sido universalmente considerado como uma das conquistas mais importantes do século XX, criando uma revolução na mecânica quântica, e na verdade em toda a física e a química. Um segundo documento foi apresentado apenas quatro semanas depois e que resolveu o oscilador harmônico quântico, o rotor rígido e a molécula diatômica, e dá uma nova derivação da equação de Schrödinger. Um terceiro documento em maio mostrou a equivalência da sua abordagem à de Heisenberg e deu o tratamento do efeito Stark. Um quarto trabalho de sua série mais marcante mostrou como tratar os problemas nos quais o sistema muda com o tempo, como nos problemas de dispersão. Estes trabalhos foram

os principais de sua carreira e foram imediatamente reconhecidos como tendo grande importância pela comunidade científica. A mecânica quântica é a teoria física que obtém sucesso no estudo dos sistemas físicos cujas dimensões são próximas ou abaixo da escala atômica, tais como moléculas, átomos, elétrons, prótons e de outras partículas subatômicas, muito embora também possa descrever fenômenos macroscópicos em diversos casos. Trataremos aqui da equação de Schrödinger, que é considerada A equação fundamental da mecânica quântica. A Mecânica Quântica é um ramo fundamental da física com vasta aplicação. A teoria quântica fornece descrições precisas para muitos fenômenos previamente inexplicados tais como a radiação de corpo negro e as órbitas estáveis do elétron. Apesar de na maioria dos casos a Mecânica Quântica ser relevante para descrever sistemas microscópicos, os seus efeitos específicos não são somente perceptíveis em tal escala. Por exemplo, a explicação de fenômenos macroscópicos como a super fluidez e a supercondutividade só é possível se considerarmos que o comportamento microscópico da matéria é quântico. A quantidade característica da teoria, que determina quando ela é necessária para a descrição de um fenômeno, é a chamada constante de Planck, que tem dimensão de momento angular ou, equivalentemente, de ação. A mecânica quântica recebe esse nome por prever um fenômeno bastante conhecido dos físicos: a quantização. No caso dos estados ligados (por exemplo, um elétron orbitando em torno de um núcleo positivo) a Mecânica Quântica prevê que a energia (do elétron) deve ser quantizada. Este fenômeno é completamente alheio ao que prevê a teoria clássica.

Teorema 5.15. *Seja* $\Psi : I \times J \subset \mathbb{R}^2 \longrightarrow \mathbb{R}^2$. *Suponha que,* $\frac{h'^2}{2m}.k^2 = h'.w$, *onde h' (*$h' = \frac{h}{2\pi}$ *é a constante de Plank, t = tempo, m = massa, V(x) = energia potencial, e x = posição). Considere a função* Ψ, *definida pela forma:*

$$\Psi(x,t) = Ae^{i(kx-\omega t)} = A[cos(kx-\omega t) + isen(kx-\omega t)],$$

onde, ω *= frequência angular da onda, k = número de ondas (*$k = \frac{2\pi}{\lambda}$*) e A uma constante qualquer. Se, a energial potencial é igual a zero, ou seja,* $V = 0$, *(isto é, temos uma partícula livre no espaço), então a função* Ψ *definida acima satisfaz a equação de Schrödinger, dada pela equação:*

$$-\frac{h'^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + V(x)\Psi(x,t) = ih'\frac{\partial\Psi(x,t)}{\partial t}.$$

Demonstração. Temos que:

$$\frac{\partial\psi(x,t)}{\partial t} = A(-i\omega)e^{i(kx-\omega t)}$$

Logo,

$$ih' \frac{\partial \psi(x,t)}{\partial t} = ih' A(-i\omega) e^{i(kx-\omega t)} = h'\omega\psi(x,t)$$

Por outro lado, temos:

$$\frac{\partial \psi(x,t)}{\partial x} = Aike^{i(kx-\omega t)}$$

e

$$\frac{\partial^2 \psi(x,t)}{\partial x^2} = ikAike^{i(kx-\omega t)} = -k^2\psi(x,t)$$

Logo, $\frac{-h'^2}{2m}\frac{\partial^2 \psi(x,t)}{\partial x^2} = \frac{-h'^2}{2m}(-k^2)\psi(x,t) = \frac{h'^2}{2m}k^2\psi(x,t)$.

Portanto, aplicando na equanção de Schrödinger, temos:

$$\frac{h'^2}{2m}k^2\psi(x,t) = h'\omega\psi(x,t)$$

Que só satisfaz a igualdade se: $\frac{h'^2}{2m}k^2 = h'\omega$

□

De maneira apenas informativa, as funções de onda de Schrodinger não são necessariamente reais, contudo a probabilidade de encontrar um elétron é totalmente real. Para podermos encontrar essa probabilidade, mudaremos a interpretação da equação de onda de modo que ela seja real. Para isso, utilizaremos a propriedade que o complexo possui de, quando multiplicado por seu conjugado, se tornar real. Assim, a probabilidade será dada por:

$$\int_{+\infty}^{-\infty} \Psi^* \Psi dx = 1$$

,onde Ψ^* é o conjugado do complexo Ψ.

Esta equação é chamada de equação de normalização. Essa condição tem um papel importante na mecânica quântica, pois coloca uma restrição nas soluções da equação de Schrodinger que leva à quantização de energia. Uma análise profunda deste estudo ver [4].

Referências Bibliográficas

[1] DRAY, Tevian.; MANOGUE, Corinne A. **The geometry of the octonions**. World Scientific Publishing Co., USA, (2015).

[2] DUMMIT, D.S.;FOOTE, R.M. **Abstract Algebra**. Prentice Hall, Inc., (1991).

[3] FERREIRA, Jamil. **A Construção dos Números**. Coleção Textos Universitários, 2ª Edição. Rio de Janeiro: Editora da Sociedade Brasileira de Matemática, (2011).

[4] GRIFFITHS, David J. Introduction to Quantum Mechanics (2nd ed.) (em inglês). Upper Saddle River, Nova Jérsei: Prentice Hall, (2004)

[5] HALMOS, P. R. **Teoria Ingênua dos Conjuntos**; trad. Prof. Irineu Bicudo. Editora da Universidade de São Paulo e Editora Polígono, (1970).

[6] HENLE, M. **Which Numbers are Real?**. USA: The Mathematical Association of America, (2012).

[7] LIMA, E. L., **Curso de Análise**, vol. 1, Décima Segunda Edição, Rio de Janeiro, IMPA, (2008).

[8] MACHADO, G. M. **A construção dos números.** Trabalho de conclusão de curso. Departamento de Matemática. Centro de Ciências Exatas e Tecnologia. Universidade Federal de São Carlos. São Carlos - SP: UFSCar, (2014).

[9] MELO, Wilberclay Gonçalves. **Análise na Reta**. Notas de Aula, UFS, (2013).

[10] STOLL, R. R. **Set Theory and Logic**.Dover Publications, Inc, (1979).