UNIVERSIDADE FEDERAL DA PARAÍBA

Centro de Ciências Exatas e da Natureza

Departamento de Matemática

Curso de Licenciatura em Matemática

NÚMEROS

Dos Axiomas de Peano ao Corpo dos Complexos

LEVI MICKAEL DA COSTA

João Pessoa

Dezembro de 2025

LEVI MICKAEL DA COSTA

NÚMEROS

Dos Axiomas de Peano ao Corpo dos Complexos

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. José Naéliton Marques da Silva

João Pessoa

Dezembro de 2025

Catalogação na publicação
Seção de Catalogação e Classificação

C838n Costa, Levi Mickael da.
Números: dos axiomas de Peano ao corpo dos complexos / Levi Mickael da Costa. - João Pessoa, 2025.
260 f. : il.

Orientação: José Naéliton Marques da Silva.
TCC (Curso de Licenciatura em Matemática) - UFPB/CCEN.

1. Conjuntos numéricos. 2. Construção algébrica. 3. Relações de equivalência. 4. Isomorfismo de corpos. 5. Sequências de Cauchy. 6. Corpo ordenado arquimediano completo. 7. Teorema fundamental da álgebra. I. Silva, José Naéliton Marques da. II. Título.

UFPB/CCEN CDU 51(043.2)

Elaborado por David Kilder Gomes da Silva - CRB-15/887

LEVI MICKAEL DA COSTA

NÚMEROS

Dos Axiomas de Peano ao Corpo dos Complexos

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. José Naéliton Marques da Silva

Aprovado em: 02/12/2025

BANCA EXAMINADORA

Prof. Dr. José Naéliton Marques da Silva
Orientador - UFPB - Campus I

Prof. Dr. Napoleón Caro Tuesta
Avaliador - UFPB - Campus I

Prof. Dr. Ricardo Burity Croccia Macedo
Avaliador - UFPB - Campus I

Ao meu avô, por me ensinar a ser curioso.

AGRADECIMENTOS

Ao Professor Dr. José Naéliton, minha profunda gratidão por sua infinita paciência e por sua constante disposição em ajudar, sempre compartilhando comigo um pouco do seu conhecimento. Tê-lo como orientador, tanto neste trabalho quanto na Iniciação Científica, foi um privilégio que contribuiu para formar a pessoa que sou hoje e moldou o profissional que aspiro ser.

"Sinto medo. Não da vida, ou da morte, ou do nada, mas de desperdiçar minha existência como se eu nunca tivesse estado aqui." (Tradução livre)

KEYES, Daniel. ***Flores para Algernon.*** *(Fala de Charlie Gordon).*

RESUMO

Este Trabalho de Conclusão de Curso apresenta a construção dos sistemas numéricos, partindo dos Axiomas de Peano para estabelecer $\mathbb{N}$ como um monoide ordenado, culminando no Teorema Fundamental da Aritmética. A insuficiência de inversos aditivos motiva a construção de $\mathbb{Z}$ como um domínio de integridade, usando relações de equivalência. Esta etapa fundamenta conceitos centrais da teoria de grupos, como subgrupos normais, quocientes e o Teorema Fundamental dos Homomorfismos, usando $(\mathbb{Z}, +)$ como exemplo.

A ausência de inversos multiplicativos em $\mathbb{Z}$ leva à construção do corpo $\mathbb{Q}$, que, apesar de ser um corpo densamente ordenado e arquimediano, demonstra ser incompleto, por exemplo, pela inexistência de $q \in \mathbb{Q}$ tal que $q^2 = 2$. Para resolver esta incompletude, $\mathbb{R}$ é construído algebricamente como o anel quociente das sequências de Cauchy $(\mathcal{C}(\mathbb{Q}))$ pelo ideal das sequências nulas (I). Demonstra-se que $\mathbb{R}$ é o único corpo ordenado Arquimediano e completo, no sentido de que toda sequência de Cauchy em $\mathbb{R}$ converge.

A incapacidade de $\mathbb{R}$ em resolver equações como $x^2 = -1$ motiva a construção do corpo $\mathbb{C}$ a partir de $\mathbb{R} \times \mathbb{R}$. Conclui-se provando que $\mathbb{C}$ não pode ser um corpo ordenado.

O trabalho encerra-se com um capítulo dedicado ao Teorema Fundamental da Álgebra, onde se utiliza a teoria dos polinômios simétricos para provar que todo polinômio de grau positivo com coeficientes complexos possui ao menos uma raiz em $\mathbb{C}$, estabelecendo-o como um corpo algebricamente fechado.

Palavras-chave: Conjuntos Numéricos. Construção Algébrica. Relações de Equivalência. Isomorfismo de Corpos. Sequências de Cauchy. Corpo Ordenado Arquimediano Completo. Teorema Fundamental da Álgebra.

ABSTRACT

This Undergraduate Thesis presents the construction of numerical systems, starting from the Peano Axioms to establish $\mathbb{N}$ as an ordered monoid, culminating in the Fundamental Theorem of Arithmetic. The insufficiency of additive inverses motivates the construction of $\mathbb{Z}$ as an integral domain, utilizing equivalence relations. This stage grounds central concepts of group theory, such as normal subgroups, quotients, and the Fundamental Homomorphism Theorem, using $(\mathbb{Z}, +)$ as an example.

The absence of multiplicative inverses in $\mathbb{Z}$ leads to the construction of the field $\mathbb{Q}$, which, despite being a densely ordered and Archimedean field, proves to be incomplete, as demonstrated by the non-existence of $q \in \mathbb{Q}$ such that $q^2 = 2$. To resolve this incompleteness, $\mathbb{R}$ is algebraically constructed as the quotient ring of Cauchy sequences $(\mathcal{C}(\mathbb{Q}))$ by the ideal of null sequences (I). It is demonstrated that $\mathbb{R}$ is the unique complete Archimedean ordered field, in the sense that every Cauchy sequence in $\mathbb{R}$ converges.

The inability of $\mathbb{R}$ to solve equations such as $x^2 = -1$ motivates the construction of the field $\mathbb{C}$ from $\mathbb{R} \times \mathbb{R}$. The work concludes by proving that $\mathbb{C}$ cannot be an ordered field.

The work ends with a chapter dedicated to the Fundamental Theorem of Algebra, employing the theory of symmetric polynomials to prove that every polynomial of positive degree with complex coefficients possesses at least one root in $\mathbb{C}$, establishing it as an algebraically closed field.

Keywords: Numerical Sets. Algebraic Construction. Equivalence Relations. Field Isomorphism. Cauchy Sequences. Complete Archimedean Ordered Field. Fundamental Theorem of Algebra.

Lista de Símbolos

Símbolo	**Descrição**
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{N}^*$	Conjunto dos números naturais não nulos
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Z}^*$	Conjunto dos números inteiros não nulos
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{Q}*$	Conjunto dos números racionais não nulos
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{R}^*$	Conjunto dos números reais não nulos
$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{C}^*$	Conjunto dos números complexos não nulos
$\mathbb{Z}_n$	Conjunto dos inteiros módulo n
$n\mathbb{Z}$	Conjunto dos inteiros múltiplos de n
$\emptyset$	Conjunto vazio
$\mid$	Tal que (em notação de conjuntos)
$\in$	Pertence
$\notin$	Não pertence
$\subset$	Está contido (subconjunto próprio)
$\subseteq$	Está contido ou é igual (subconjunto)
$\cup$	União de conjuntos
$\cap$	Interseção de conjuntos
$A \times B$	Produto cartesiano entre os conjuntos A e B
$\forall$	Para todo (quantificador universal)
$\exists$	Existe (quantificador existencial)
$\exists!$	Existe um único
$\implies$	Implica (se... então)
$\iff$	Se, e somente se
$\wedge$	E (conjunção lógica)
$\vee$	Ou (disjunção lógica)
$f : A \to B$	Função f de A em B

Símbolo	**Descrição**
$x \mapsto y$	O elemento x é mapeado no elemento y
$g \circ f$	Composição de funções (g após f)
$\approx$	Aproximadamente igual
$<, >$	Menor que, Maior que
$\leq, \geq$	Menor ou igual a, Maior ou igual a
$\preceq$	Relação de ordem genérica em um conjunto
$a \mid b$	a divide b
$a \nmid b$	a não divide b
$a \equiv b \pmod{m}$	a é congruente a b módulo m
$\sim$	Relação de equivalência
$\overline{a}$ ou $[a]$	Classe de equivalência do elemento a
$\cong$	Isomorfo a
$\lvert n \rvert$	Valor absoluto (módulo) do número n
$\langle a \rangle$	Subgrupo gerado pelo elemento a
gH	Classe lateral à esquerda de H em G
Hg	Classe lateral à direita de H em G
$\lvert G \rvert$	Cardinalidade do grupo G
$\texttt{ord}(a)$	Ordem do elemento a (em um grupo)
$\lvert gH \rvert$	Ordem da classe lateral gH
$[G : H]$	Índice do subgrupo H em G
$\mathbb{Q}^{\mathbb{N}}$	Anel das sequências de números racionais
$\mathcal{C}(\mathbb{Q})$	Anel das sequências de Cauchy racionais
$\deg(P)$ ou ∂P	Grau do polinômio P
$\mathbb{K}[x]$	Anel de polinômios na variável x com coeficientes em $\mathbb{K}$

Sumário

Introdução

Os sistemas numéricos são a fundação sobre a qual se ergue o edifício da análise matemática. Na prática elementar, os conjuntos dos números Naturais ($\mathbb{N}$), Inteiros ($\mathbb{Z}$), Racionais ($\mathbb{Q}$), Reais ($\mathbb{R}$) e Complexos ($\mathbb{C}$) são frequentemente apresentados como um dado, com suas propriedades e operações — adição, multiplicação, ordem — aceitas intuitivamente. No entanto, o rigor matemático exige mais do que intuição; exige uma construção lógica e formal, onde cada propriedade possa ser provada e cada novo sistema numérico justificado como uma extensão necessária do anterior.

Este trabalho tem como objetivo apresentar essa construção formal. Partimos do alicerce mais fundamental, os Axiomas de Peano, que definem a própria essência do conjunto dos números naturais e o princípio da indução finita. A partir desta base axiomática, definimos indutivamente as operações de adição e multiplicação em $\mathbb{N}$ e provamos, passo a passo, suas propriedades familiares, como associatividade, comutatividade e distributividade. Estabelecemos também as relações de ordem e divisibilidade, culminando na demonstração de um dos pilares da aritmética: o Teorema Fundamental da Aritmética.

Uma vez estabelecida a estrutura de $\mathbb{N}$, encontramos sua primeira grande deficiência algébrica: a operação de adição não possui inversos, tornando a subtração uma operação não fechada. Para solucionar este problema, empregamos o formalismo das relações de equivalência para construir o anel dos Números Inteiros ($\mathbb{Z}$) a partir de pares de números naturais. Nesta nova estrutura, $(\mathbb{Z}, +)$ é um grupo abeliano cíclico, e $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade, garantindo o fechamento da subtração. Esta construção nos permite, ainda, aprofundar o estudo das estruturas algébricas, explorando os conceitos de subgrupos, classes laterais, grupos quocientes e o Teorema de Lagrange.

A estrutura de $\mathbb{Z}$, embora robusta, falha em garantir o fechamento da divisão. A ausência de inversos multiplicativos para a maioria de seus elementos nos motiva a repetir o processo de construção. Utilizando novamente classes de equivalência, desta vez sobre pares de inteiros, erigimos o corpo dos Números Racionais ($\mathbb{Q}$). Demonstramos que $(\mathbb{Q}, +, \cdot, \leq)$ é um corpo ordenado, denso e que satisfaz a Propriedade Arquimediana. Nele, todas as quatro operações aritméticas básicas são bem-definidas.

Contudo, a densidade de $\mathbb{Q}$ é ilusória. Demonstramos sua profunda limitação — sua incompletude — ao provar que não existe número racional q tal que $q^2 = 2$. Esta

descoberta revela que a reta racional é repleta de buracos, pontos para os quais sequências de racionais podem convergir, mas cujo limite não pertence ao próprio conjunto. Para preencher estas lacunas, introduzimos o conceito de Sequências de Cauchy e construímos o corpo dos Números Reais ($\mathbb{R}$) como o conjunto quociente de todas as sequências de Cauchy de racionais. Demonstramos que $\mathbb{R}$ é um corpo ordenado arquimediano completo, e provamos sua unicidade como tal.

A jornada se aproxima de seu desfecho ao confrontarmos a limitação algébrica de $\mathbb{R}$: embora analiticamente completo, o corpo dos reais falha em prover soluções para equações polinomiais elementares, como $x^2 + 1 = 0$. Esta deficiência motiva a construção do corpo dos Números Complexos ($\mathbb{C}$) como o produto cartesiano $\mathbb{R} \times \mathbb{R}$. Ao definirmos a unidade imaginária i e as operações sobre este conjunto, demonstramos que esta nova estrutura constitui um corpo que soluciona o problema inicial, ainda que ao custo de perder a propriedade de ser um corpo ordenado.

Por fim, o trabalho encerra-se com um capítulo dedicado ao Teorema Fundamental da Álgebra. Utilizando a teoria dos polinômios simétricos e as propriedades demonstramos que $\mathbb{C}$ é um corpo algebricamente fechado. Provamos que todo polinômio de grau positivo com coeficientes complexos possui ao menos uma raiz em $\mathbb{C}$, confirmando que não há necessidade de novas extensões numéricas para a resolução de equações polinomiais e completando, assim, a narrativa lógica da construção dos números.

Capítulo 1

Naturais

De forma direta, um número, em sua essência, é um conceito abstrato que representa quantidade, ordem ou medida. Embora usemos símbolos (como 1, 2, 3) para representá-los, os números em si são ideias. Eles não existem fisicamente no mundo mas são ferramentas que nossa mente utiliza para quantificar e organizar o mundo ao nosso redor.

A ideia de número surge da necessidade humana fundamental de contar e comparar. Imagine nossos ancestrais. Eles precisavam saber quantas frutas colheram, quantos animais havia em um rebanho ou quantos membros formavam seu grupo. A percepção de três ovelhas, três pedras ou três dias é a mesma: a abstração da quantidade. O número três é essa ideia comum que pode ser aplicada a qualquer conjunto de três objetos.

Inicialmente, a noção de número era puramente intuitiva. A correspondência um-a-um foi o primeiro passo: um pastor podia verificar se todas as suas ovelhas voltaram ao final do dia comparando cada animal com uma pedra em uma bolsa, sem necessariamente saber contar como fazemos hoje.

Com o tempo, a civilização precisou de um sistema mais robusto. Surgiram os símbolos (algarismos) e os nomes para os números, permitindo registrar e comunicar quantidades de forma eficiente. No entanto, do ponto de vista matemático, a pergunta "o que é um número?" exige uma resposta mais rigorosa.

No século XIX, essa questão levou à criação de uma base lógica e formal para a aritmética. A resposta mais célebre veio do matemático italiano Giuseppe Peano, que propôs um conjunto de axiomas para definir os números naturais ($\mathbb{N}$), o alicerce de todos os outros conjuntos numéricos.

Esses axiomas não nos dizem o que um número é, mas nos dizem como ele se comporta. A partir dessa estrutura, toda a aritmética dos números naturais pode ser construída de forma lógica e rigorosa, fornecendo a base para a construção dos inteiros ($\mathbb{Z}$), racionais ($\mathbb{Q}$), reais ($\mathbb{R}$) e complexos ($\mathbb{C}$), e para a análise de suas estruturas algébricas, como os monoides e grupos.

1.1 Axiomas de Peano

A estrutura axiomática se baseia em três noções primitivas:

- Um conjunto $\mathbb{N}$, cujos elementos são chamados de **números naturais**;
- Um elemento destacado $0 \in \mathbb{N}$, chamado de **zero**;
- Uma **função sucessor** $S : \mathbb{N} \to \mathbb{N}$, que a cada número natural n associa um único sucessor $S(n)$.

O conjunto $\mathbb{N}$ e a função S devem satisfazer os seguintes cinco axiomas:

Axioma 1: O zero é um número natural.

$$0 \in \mathbb{N}$$

Axioma 2: Se n é um número natural, então seu sucessor $S(n)$ também é um número natural.

$$\forall n \in \mathbb{N}, S(n) \in \mathbb{N}$$

Axioma 3: O zero não é sucessor de nenhum número natural.

$$\forall n \in \mathbb{N}, S(n) \neq 0$$

Axioma 4: Se os sucessores de dois números naturais são iguais, então os próprios números são iguais. (A função sucessor é injetiva).

$$\forall n, m \in \mathbb{N}, (S(n) = S(m) \implies n = m)$$

Axioma 5: Se um subconjunto K de $\mathbb{N}$ contém o zero e também o sucessor de cada um de seus elementos, então este subconjunto é o próprio conjunto dos números naturais.

$$(0 \in K \land (\forall n \in K, S(n) \in K)) \implies K = \mathbb{N}$$

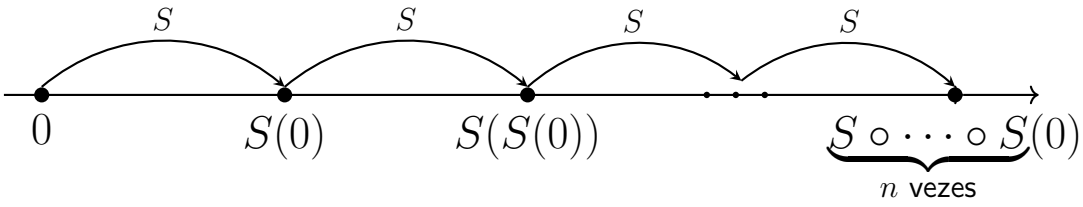
Este axioma é a base lógica para uma das ferramentas de demonstração mais poderosas da matemática, o **Princípio da Indução Finita**. Ele garante que, se uma propriedade é válida para o zero e, sempre que é válida para um número, também é para seu sucessor, então essa propriedade deve ser válida para todos os números naturais.

Podemos visualizar este princípio com uma analogia. Imagine o conjunto dos números naturais, $\mathbb{N}$, como uma fila infinita de carros, um atrás do outro. O subconjunto K representa o conjunto dos carros que serão atingidos em uma colisão em cadeia.

- A condição de que $\mathbf{0} \in \mathbf{K}$ é o gatilho inicial: garantimos que o primeiro carro da fila (o zero) acelera e colide.
- A segunda condição, $\forall \mathbf{n} \in \mathbf{K}, \mathbf{S(n)} \in \mathbf{K}$, funciona como uma lei de causa e efeito: se um carro qualquer (n) é atingido, ele inevitavelmente colidirá com o próximo $(S(n))$.

O axioma nos diz que, se essas duas condições forem satisfeitas, a colisão se propagará por toda a fila. Se o primeiro carro colide e a regra da colisão em cadeia é válida, então não há como um carro na fila infinita escapar da colisão. O conjunto dos carros atingidos, K, será o conjunto de todos os carros, $\mathbb{N}$.

A partir desses 5 axiomas, podemos entender o conjunto dos números naturais como o conjunto de todos os elementos que podem ser formados partindo-se do zero e aplicando a função sucessor um número infinito de vezes. Esses axiomas garantem que não existem outros elementos em $\mathbb{N}$ além daqueles gerados por este processo. Assim, construímos a sequência familiar dos números naturais, onde cada novo número é simplesmente o sucessor do anterior:



Desta forma, todo número natural diferente de zero é o sucessor de outro número natural, e o conjunto $\mathbb{N} = \{0, S(0), S(S(0)), \dots\}$ é gerado por completo.

Proposição 1.1.1 (Todo Natural Não-Nulo é um Sucessor)**.** Todo número natural diferente de zero é o sucessor de algum outro número natural. Formalmente:

$$\forall n \in \mathbb{N}, (n \neq 0 \implies \exists k \in \mathbb{N} \text{ tal que } n = S(k))$$

Demonstração. A demonstração será feita utilizando o Axioma 5 (Princípio da Indução Finita). Para isso, vamos definir um subconjunto $K \subseteq \mathbb{N}$ da seguinte forma:

$$K = \{0\} \cup \{n \in \mathbb{N} \mid \exists k \in \mathbb{N}, n = S(k)\}$$

Em palavras, K é o conjunto que contém o zero e todos os números naturais que são sucessores. Nosso objetivo é usar o Axioma 5 para provar que $K = \mathbb{N}$. Para isso, precisamos verificar as duas condições do axioma.

Caso Base ($0 \in K$): Por definição, o conjunto K foi construído como a união do conjunto $\{0\}$ com o conjunto de todos os sucessores. Portanto, 0 pertence a K por construção. A condição base é satisfeita.

Passo Indutivo ($\forall n \in K, S(n) \in K$): Nossa hipótese de indução é que n é um elemento qualquer de K. Devemos provar que seu sucessor, $S(n)$, também pertence a K.

Para que $S(n)$ pertença a K, ele deve ser ou o zero, ou o sucessor de algum número natural.

- Pelo Axioma 3, sabemos que $S(n) \neq 0$ para qualquer $n \in \mathbb{N}$.
- Pela própria forma como $S(n)$ é escrito, ele é, por definição, o sucessor do número natural n.

Como $S(n)$ é o sucessor de n, ele se encaixa na definição de pertencimento ao conjunto de todos os sucessores, que por sua vez está contido em K. Portanto, $S(n) \in K$. Isso mostra que, se um número n está em K, seu sucessor $S(n)$ também está.

Como o conjunto K contém o zero e também o sucessor de cada um de seus elementos, pelo Axioma 5, concluímos que $K = \mathbb{N}$. Se $K = \mathbb{N}$, significa que todo número natural ou é o zero, ou é o sucessor de algum outro número natural. Ou seja, se um número natural n não é zero, ele deve necessariamente ser o sucessor de algum $k \in \mathbb{N}$. □

Definimos:

$$
\begin{aligned}
1 &:= S(0) \\
2 &:= S(1) = S(S(0)) \\
3 &:= S(2) = S(S(S(0))) \\
4 &:= S(3) = S(S(S(S(0)))) \\
5 &:= S(4) = S(S(S(S(S(0))))) \\
6 &:= S(5) = S(S(S(S(S(S(0)))))) \\
7 &:= S(6) = S(S(S(S(S(S(S(0))))))) \\
8 &:= S(7) = S(S(S(S(S(S(S(S(0)))))))) \\
9 &:= S(8) = S(S(S(S(S(S(S(S(S(0))))))))) \\
&\vdots
\end{aligned}
$$

Este processo de criar um novo símbolo para o sucessor de cada número é, teoricamente, infinito. No entanto, tal abordagem exigiria uma memória infinita para um número infinito de símbolos, tornando a representação dos números impraticável.

Primeiro, estabelecemos um conjunto finito de símbolos básicos, os **algarismos**: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. A questão fundamental surge ao tentarmos representar o sucessor

do último algarismo, $S(9)$. Como esgotamos nosso conjunto de símbolos únicos, a convenção dita que "reiniciemos a contagem".

Para representar $S(9)$, o algarismo da direita retorna ao símbolo inicial, o **0**. Para registrar que um ciclo completo de algarismos foi percorrido, introduzimos uma nova posição à esquerda, e nela colocamos a quantidade de vezes que o conjunto de símbolos foi utilizada. Essa notação é simplesmente uma regra para continuar a sequência. O símbolo **10** significa que todos os algarismos básicos já foram usados 1 vez, e a contagem reiniciou. A partir daqui, a aplicação da função sucessor continua a afetar o algarismo mais à direita: $S(10)$ é representado por **11**, $S(11)$ por **12**, e assim por diante, até que o algarismo da direita se torne 9 novamente, forçando um novo "reinício"e um incremento na posição à sua esquerda. O símbolo **20** significa que todos os algarismos básicos já foram usados 2 vezes, e a contagem reiniciou. O símbolo **30** significa que todos os algarismos básicos já foram usados 3 vezes, e a contagem reiniciou. E assim sucessivamente.

1.2 Adição

A intuição por trás da soma $n + m$ é a de iniciar com o número m e aplicar a função sucessor S um total de n vezes. Para formalizar este processo, primeiro definimos uma família de funções $\sigma_n : \mathbb{N} \to \mathbb{N}$ para cada $n \in \mathbb{N}$.

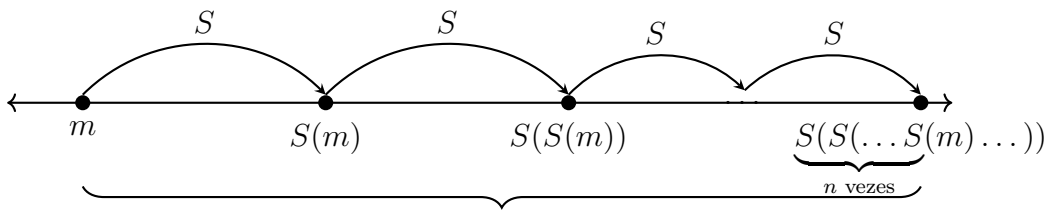
A função σ_n é definida como:

$$\sigma_n = \begin{cases} \text{a função identidade} & \text{se } n = 0 \\ \underbrace{S \circ S \circ \cdots \circ S}_{n \text{ vezes}} & \text{se } n \neq 0 \end{cases}$$

onde S representa a função sucessor e $\circ$ denota a composição de funções. Assim, $\sigma_0(m) = m$ e $\sigma_n(m) = \underbrace{S(S(...S}_{n\text{vezes}}(m)...))$.

Definição 1.2.1. Dados dois números naturais $n, m \in \mathbb{N}$, definimos sua **soma** como o número natural:

$$n + m = \sigma_n(m)$$



A partir desta definição, podemos encontrar algumas propriedades elementares da adição.

Proposição 1.2.1 (Elemento Neutro à Esquerda)**.** O número 0 é o elemento neutro à esquerda para a adição. Para todo $n \in \mathbb{N}$, temos:

$$0 + n = n$$

Demonstração. Pela definição de adição, $0 + n = \sigma_0(n)$. Conforme definido, σ_0 é a função identidade, que por sua vez mapeia todo elemento para si mesmo. Portanto, $\sigma_0(n) = n$. □

Proposição 1.2.2 (Adição do Sucessor)**.** Para quaisquer $n, m \in \mathbb{N}$, somar o sucessor de n a m é o mesmo que encontrar o sucessor da soma de n e m.

$$S(n) + m = S(n + m)$$

Demonstração. Iniciamos a prova aplicando a definição de adição ao termo da esquerda, $S(n) + m$:

$$S(n) + m = \sigma_{S(n)}(m)$$

O ponto central da demonstração é entender o significado da função $\sigma_{S(n)}$. Por definição, σ_k é a composição da função sucessor S um total de k vezes. Portanto, $\sigma_{S(n)}$ representa a composição de S por $S(n)$ vezes.

Segue da definição que compor S por $S(n)$ vezes é o mesmo que compor S por n vezes (o que resulta em σ_n) e, em seguida, compor com a função S mais uma vez. Esta relação pode ser expressa como:

$$\sigma_{S(n)} = S \circ \sigma_n$$

Utilizando esta identidade, podemos reescrever a demonstração com a seguinte cadeia de igualdades, onde cada passo é justificado:

$$\begin{aligned} S(n) + m &= \sigma_{S(n)}(m) && \text{(Pela definição de adição)} \\ &= (S \circ \sigma_n)(m) && \text{(Pela relação mostrada acima)} \\ &= S(\sigma_n(m)) && \text{(Pela de composição de funções)} \\ &= S(n + m) && \text{(Substituindo } \sigma_n(m) \text{ pela sua definição, } n + m) \end{aligned}$$

Assim, a igualdade $S(n) + m = S(n + m)$ está provada.

□

Proposição 1.2.3. Se a soma de dois números naturais é zero, então ambos os números devem ser zero.

$$\forall n, m \in \mathbb{N}, (n + m = 0 \implies n = 0 \land m = 0)$$

Demonstração. Vamos provar por contradição. Suponha que $n \neq 0$. Como todo Natural

não nulo é sucessor de algum número, n deve ser o sucessor de algum $p \in \mathbb{N}$, ou seja, $n = S(p)$. Neste caso, a soma $n + m = S(p) + m = S(p + m)$. Se $n + m = 0$, então teríamos $S(p+m) = 0$. Isso contradiz o Axioma 3, que afirma que zero não é sucessor de nenhum número natural. Logo, a nossa suposição inicial de que $n \neq 0$ é falsa. Portanto, n deve ser 0.

Agora que sabemos que $n = 0$, a equação se torna $0 + m = 0$. Pela propriedade do elemento neutro, $0 + m = m$. Assim, concluímos que $m = 0$. □

Proposição 1.2.4 (Lei do Cancelamento à Esquerda)**.** Para quaisquer $n, x, y \in \mathbb{N}$, se $n + x = n + y$, então $x = y$.

$$n + x = n + y \implies x = y$$

Demonstração. A prova se baseia na injetividade da função σ_n.

- Se $n = 0$, σ_0 é a função identidade, que é trivialmente injetiva.
- Se $n \neq 0$, σ_n é uma composição de n funções sucessoras ($S \circ S \circ \cdots \circ S$). Como a função S é injetiva (Axioma 4) e a composição de funções injetivas resulta em uma função injetiva, σ_n é injetiva para todo $n \neq 0$.

Dada a equação $n + x = n + y$, podemos reescrevê-la usando a definição de soma como $\sigma_n(x) = \sigma_n(y)$. Uma vez que σ_n é uma função injetiva, podemos concluir diretamente que $x = y$. □

Proposição 1.2.5. Para cada $n \in \mathbb{N}$, a função sucessor S comuta com a função σ_n.

$$S \circ \sigma_n = \sigma_n \circ S$$

Demonstração. Usaremos o Princípio da Indução Finita sobre n. Seja A o subconjunto dos números naturais que satisfazem a condição $S \circ \sigma_n = \sigma_n \circ S$.

$$A = \{n \in \mathbb{N} \mid S \circ \sigma_n = \sigma_n \circ S\}$$

Precisamos mostrar que $A = \mathbb{N}$.

Caso Base ($n = 0$): Devemos verificar se $0 \in A$, ou seja, se $S \circ \sigma_0 = \sigma_0 \circ S$.
Por definição, σ_0 é a função identidade. Assim, temos:
$S \circ \sigma_0 = S \circ id = S$.
$\sigma_0 \circ S = id \circ S = S$.
Como ambos os lados são iguais a S, a afirmação é verdadeira para $n = 0$.

Passo Indutivo: Nossa hipótese de indução é que $n \in A$ para $n \in \mathbb{N}$, isto é:

$$S \circ \sigma_n = \sigma_n \circ S$$

Devemos provar que $S(n) \in A$, ou seja, que $S \circ \sigma_{S(n)} = \sigma_{S(n)} \circ S$.

Lembrando que $\sigma_{S(n)} = \sigma_{1+n} = S \circ \sigma_n$, vamos trabalhar com o lado esquerdo da equação que queremos provar:

$$S \circ \sigma_{S(n)} = S \circ (S \circ \sigma_n) = (S \circ S) \circ \sigma_n \quad (LE)$$

Agora, vamos trabalhar com o lado direito, usando a associatividade da composição e a nossa hipótese de indução:

$$\sigma_{S(n)} \circ S = (S \circ \sigma_n) \circ S = S \circ (\sigma_n \circ S) \quad (LD)$$

Pela hipótese de indução, podemos substituir $\sigma_n \circ S$ por $S \circ \sigma_n$:

$$S \circ (\sigma_n \circ S) = S \circ (S \circ \sigma_n) = (S \circ S) \circ \sigma_n \quad (LD)$$

Como o lado esquerdo e o lado direito são ambos iguais a $(S \circ S) \circ \sigma_n$, provamos que $S \circ \sigma_{S(n)} = \sigma_{S(n)} \circ S$.

Isso mostra que se a propriedade vale para n, ela também vale para $S(n)$. Portanto, $S(n) \in A$.

Pelo Princípio da Indução Finita, concluímos que $A = \mathbb{N}$, e a propriedade $S \circ \sigma_n = \sigma_n \circ S$ é válida para todo número natural n. □

Proposição 1.2.6 (Comutatividade da Adição)**.** Para quaisquer $n, m \in \mathbb{N}$, a adição é comutativa.

$$n + m = m + n$$

Demonstração. Fixemos um $m \in \mathbb{N}$ arbitrário e provemos por indução sobre n que $n + m = m + n$.

Caso Base ($n = 0$):
Precisamos provar que $0 + m = m + 0$. Já sabemos que $0 + m = m$ (elemento neutro à esquerda). Resta provar que $m + 0 = m$ para todo $m \in \mathbb{N}$.
Lema: *$m + 0 = m$ para todo $m \in \mathbb{N}$.*
Prova do Lema *(por indução sobre m):*

- *Base ($m = 0$):* A afirmação é $0 + 0 = 0$. Pela definição, $0 + 0 = \sigma_0(0) = 0$. Verdadeiro.
- *Hipótese de Indução:* Suponha que $k + 0 = k$ para algum $k \in \mathbb{N}$.
- *Passo Indutivo:* Devemos mostrar que $S(k) + 0 = S(k)$. Usando a propriedade da adição do sucessor e a hipótese de indução:

$$S(k) + 0 = S(k + 0) = S(k)$$

Como $0 + m = m$ e $m + 0 = m$, concluímos que $0 + m = m + 0$. A afirmação é válida para o caso base.

Passo Indutivo: Nossa hipótese de indução é que $n + m = m + n$ para algum $n \in \mathbb{N}$. Devemos provar que a propriedade vale para seu sucessor, $S(n)$, ou seja, $S(n) + m = m + S(n)$.

Partindo do lado esquerdo e usando as definições e proposições anteriores:

$$S(n) + m = S(n + m)$$

Usando a Hipótese de Indução ($n + m = m + n$):

$$S(n + m) = S(m + n)$$

Agora, usamos a propriedade de que o sucessor comuta com a função σ_m, o que nos fornece:

$$S(m + n) = S(\sigma_m(n)) = \sigma_m(S(n)) = m + S(n)$$

Juntando os passos, temos $S(n) + m = m + S(n)$, o que completa o passo indutivo.

Como a propriedade vale para o caso base e o passo indutivo foi provado, pelo Princípio da Indução, concluímos que $n + m = m + n$ para todos $n, m \in \mathbb{N}$. □

Proposição 1.2.7 (Elemento Neutro da Adição)**.** O número 0 é o elemento identidade (ou neutro) para a adição no conjunto dos números naturais. Para todo $m \in \mathbb{N}$, a seguinte identidade é válida:

$$0 + m = m + 0 = m$$

Demonstração. A demonstração desta proposição decorre diretamente de dois resultados já provados: a Proposição do Elemento Neutro à esquerda ($0 + m = m$) e o lema utilizado na prova da Comutatividade da Adição, que estabeleceu o elemento neutro à direita ($m + 0 = m$). □

Proposição 1.2.8 (Associatividade da Adição)**.** Para quaisquer $n, p, q \in \mathbb{N}$, a adição é associativa.

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

Demonstração. A demonstração desta propriedade fica mais clara ao provarmos primeiro um lema fundamental sobre a função σ.

Lema: *Para todo $n, p \in \mathbb{N}$, temos $\sigma_{n+p} = \sigma_n \circ \sigma_p$.*

Prova do Lema: Faremos indução sobre n.

- **Base ($n = 0$):** $\sigma_{0+p} = \sigma_p$, e $\sigma_0 \circ \sigma_p = id \circ \sigma_p = \sigma_p$. Válido.
- **Hipótese de Indução:** Suponha $\sigma_{n+p} = \sigma_n \circ \sigma_p$.

- **Passo Indutivo:** Queremos mostrar que $\sigma_{S(n)+p} = \sigma_{S(n)} \circ \sigma_p$. O lado esquerdo é $\sigma_{S(n)+p} = \sigma_{S(n+p)} = S \circ \sigma_{n+p}$. Usando a Hipótese de Indução, temos $S \circ (\sigma_n \circ \sigma_p)$. O lado direito é $\sigma_{S(n)} \circ \sigma_p = (S \circ \sigma_n) \circ \sigma_p$. Pela associatividade da composição de funções, $S \circ (\sigma_n \circ \sigma_p) = (S \circ \sigma_n) \circ \sigma_p$. Assim, o lema está provado.

Com o lema demonstrado, a prova da associatividade é direta:

$$(n + p) + q = \sigma_{n+p}(q)$$

Pelo nosso lema, $\sigma_{n+p}(q) = (\sigma_n \circ \sigma_p)(q) = \sigma_n(\sigma_p(q))$. Pela definição de soma, $\sigma_p(q) = p + q$. Substituindo, temos:

$$\sigma_n(\sigma_p(q)) = \sigma_n(p + q)$$

Novamente pela definição de soma, $\sigma_n(p + q) = n + (p + q)$. Portanto, concluímos que $(n + p) + q = n + (p + q)$. □

1.3 Multiplicação

Com a adição e suas propriedades estabelecidas, podemos definir a segunda operação fundamental sobre os números naturais, a **multiplicação**. Intuitivamente, o produto $n \cdot m$ pode ser visto como a soma do número m consigo mesmo, um total de n vezes.

Definição 1.3.1 (Multiplicação de Naturais)**.** Dados dois números naturais $n, m \in \mathbb{N}$, definimos seu **produto**, denotado por $n \cdot m$, como:

$$n \cdot m = \begin{cases} 0, & \text{se } n = 0 \\ \underbrace{m + m + \cdots + m}_{n \text{ vezes}}, & \text{se } n \neq 0 \end{cases}$$

Proposição 1.3.1 (Distributividade da Multiplicação sobre a Adição)**.** Para quaisquer $n, p, q \in \mathbb{N}$, a multiplicação distribui sobre a adição:

$$n \cdot (p + q) = n \cdot p + n \cdot q \quad \text{(Distributividade à esquerda)}$$

$$(p + q) \cdot n = p \cdot n + q \cdot n \quad \text{(Distributividade à direita)}$$

Demonstração. **Distributividade à Esquerda**

- **Caso 1:** $n = 0$. Temos $0 \cdot (p + q) = 0$. E, no outro lado, $0 \cdot p + 0 \cdot q = 0 + 0 = 0$. A igualdade se verifica.
- **Caso 2:** $n \neq 0$. Usando a definição da multiplicação, n é o número de vezes que

somamos o termo $(p+q)$:

$$n \cdot (p+q) = \underbrace{(p+q) + (p+q) + \cdots + (p+q)}_{n \text{ vezes}}$$

Usando a associatividade e a comutatividade da adição em $\mathbb{N}$, podemos reagrupar os termos:

$$\underbrace{(p+p+\cdots+p)}_{n \text{ vezes}} + \underbrace{(q+q+\cdots+q)}_{n \text{ vezes}}$$

O que, por definição, é exatamente $n \cdot p + n \cdot q$.

Distributividade à Direita

- **Caso 1:** $p = 0$ **e** $q = 0$. O lado esquerdo é $(0+0) \cdot n = 0 \cdot n = 0$. O lado direito é $(0 \cdot n) + (0 \cdot n) = 0 + 0 = 0$. A igualdade se verifica.
- **Caso 2: Pelo menos** p **ou** q **é diferente de zero**. Neste caso, o fator $p+q$ é diferente de zero. Usando a definição da multiplicação, $(p+q)$ é o número de vezes que somamos o termo n:

$$(p+q) \cdot n = \underbrace{n + n + \cdots + n}_{p+q \text{ vezes}}$$

Pela associatividade da adição, podemos separar esta longa soma em duas partes: a primeira contendo p termos e a segunda contendo q termos (se $p = 0$ ou $q = 0$, uma dessas somas é 0).

$$\left(\underbrace{n + n + \cdots + n}_{p \text{ vezes}}\right) + \left(\underbrace{n + n + \cdots + n}_{q \text{ vezes}}\right)$$

O que, por definição, é exatamente $p \cdot n + q \cdot n$.

Com ambas as propriedades demonstradas, a prova está completa. □

Proposição 1.3.2 (Relação Recursiva da Multiplicação)**.** Para quaisquer $n, m \in \mathbb{N}$, o produto do sucessor de n por m é igual ao produto de n por m, somado a m.

$$S(n) \cdot m = (n \cdot m) + m$$

Demonstração. A demonstração segue diretamente da distributividade da multiplicação sobre a adição.

$$S(n) \cdot m = (1+n)m = m + nm$$

□

Proposição 1.3.3 (Elemento Neutro da Multiplicação)**.** O número 1 é o elemento identidade para a multiplicação em $\mathbb{N}$. Para todo $m \in \mathbb{N}$, temos:

$$1 \cdot m = m \quad \text{e} \quad m \cdot 1 = m$$

Demonstração. Segue da definição de multiplicação que $1 \cdot m = m$. Assim, basta provar que $m \cdot 1 = m$.
Podemos construir uma prova por indução sobre m.

- **Caso Base ($m = 0$):** Devemos provar que $0 \cdot 1 = 0$. Pela definição de multiplicação, o produto é zero se o primeiro termo for zero. Portanto, a base é válida.
- **Passo Indutivo:** Nossa hipótese de indução é que $k \cdot 1 = k$ para $k \in \mathbb{N}$. Devemos provar que $S(k) \cdot 1 = S(k)$.

  Partindo do lado esquerdo:

$$\begin{aligned} S(k) \cdot 1 &= (k \cdot 1) + 1 && \text{(Pela Relação Recursiva da Multiplicação)} \\ &= k + 1 && \text{(Pela hipótese de indução)} \\ &= S(k) \end{aligned}$$

Como a propriedade vale para o caso base e o passo indutivo foi provado, concluímos por indução que $m \cdot 1 = m$ para todo $m \in \mathbb{N}$. □

Proposição 1.3.4 (Comutatividade da Multiplicação)**.** Para cada $n, m \in \mathbb{N}$, a multiplicação é comutativa.

$$n \cdot m = m \cdot n$$

Demonstração. A prova será feita por indução sobre n.

Caso Base ($n = 0$): Precisamos mostrar que $0 \cdot m = m \cdot 0$.
Pela definição, $0 \cdot m = 0$. Resta provar que $m \cdot 0 = 0$ para todo $m \in \mathbb{N}$.
Lema: $m \cdot 0 = 0$ *para todo* $m \in \mathbb{N}$.
Prova do Lema *(por indução sobre m):*

- *Base ($m = 0$):* A afirmação é $0 \cdot 0 = 0$. Pela definição de multiplicação (caso $n = 0$), isso é verdadeiro.
- *Hipótese de Indução:* Suponha que $k \cdot 0 = 0$ para algum $k \in \mathbb{N}$.
- *Passo Indutivo:* Devemos mostrar que $S(k) \cdot 0 = 0$. Usando a Relação Recursiva da Multiplicação e a hipótese de indução:

$$S(k) \cdot 0 = (k \cdot 0) + 0 = 0 + 0 = 0$$

Pelo Princípio da Indução, o lema está provado.

Como $0 \cdot m = 0$ e $m \cdot 0 = 0$, concluímos que $0 \cdot m = m \cdot 0$. A afirmação é válida para o caso base.

Passo Indutivo: Nossa hipótese de indução é que $n \cdot m = m \cdot n$ para $n \in \mathbb{N}$. Devemos provar que $S(n) \cdot m = m \cdot S(n)$.

Partindo do lado esquerdo, pela definição recursiva de multiplicação:

$$S(n) \cdot m = (n \cdot m) + m \quad (LE)$$

Usando a Hipótese de Indução no termo $n \cdot m$:

$$(n \cdot m) + m = (m \cdot n) + m \quad (LE)$$

Agora, para o lado direito, $m \cdot S(n)$, sabemos que $S(n) = n + 1$.

$$m \cdot S(n) = m \cdot (n + 1) \quad (LD)$$

Usando a propriedade distributiva:

$$m \cdot (n + 1) = (m \cdot n) + (m \cdot 1) \quad (LD)$$

$$(m \cdot n) + (m \cdot 1) = (m \cdot n) + m \quad (LD)$$

Comparando os resultados do lado esquerdo e do lado direito, vemos que ambos são iguais a $(m \cdot n) + m$. Assim, $S(n) \cdot m = m \cdot S(n)$.

Pelo Princípio da Indução, a comutatividade é válida para todos $n, m \in \mathbb{N}$.

□

Proposição 1.3.5 (Associatividade da Multiplicação)**.** Para quaisquer $n, p, q \in \mathbb{N}$, a multiplicação é associativa.

$$(n \cdot p) \cdot q = n \cdot (p \cdot q)$$

Demonstração. A demonstração será feita por indução sobre n.

Caso Base ($n = 0$): Precisamos verificar se $(0 \cdot p) \cdot q = 0 \cdot (p \cdot q)$.

- Lado esquerdo: Pela definição de multiplicação, $0 \cdot p = 0$. Portanto, $(0 \cdot p) \cdot q = 0 \cdot q = 0$.
- Lado direito: Pela mesma definição, $0 \cdot (p \cdot q) = 0$.

A propriedade é válida para o caso base.

Passo Indutivo: Nossa hipótese de indução é que a propriedade vale para $n \in \mathbb{N}$:

$$(n \cdot p) \cdot q = n \cdot (p \cdot q)$$

Devemos provar que a propriedade é válida para $S(n)$, ou seja:

$$(S(n) \cdot p) \cdot q = S(n) \cdot (p \cdot q)$$

Vamos analisar cada lado da equação separadamente.

- Lado esquerdo: Começamos usando a relação recursiva da multiplicação no termo $(S(n) \cdot p)$:

  $$(S(n) \cdot p) \cdot q = ((n \cdot p) + p) \cdot q$$

  Agora, usamos a distributividade da multiplicação sobre a adição:

  $$((n \cdot p) + p) \cdot q = (n \cdot p) \cdot q + (p \cdot q)$$

- Lado direito: Usamos a relação recursiva da multiplicação, tratando $(p \cdot q)$ como um único elemento:

  $$S(n) \cdot (p \cdot q) = (n \cdot (p \cdot q)) + (p \cdot q)$$

Agora, comparamos os resultados dos dois lados. O lado esquerdo é $(n \cdot p) \cdot q + (p \cdot q)$ e o lado direito é $n \cdot (p \cdot q) + (p \cdot q)$.

Pela nossa Hipótese de Indução, sabemos que $(n \cdot p) \cdot q = n \cdot (p \cdot q)$. Portanto, as duas expressões são de fato iguais. Isso completa o passo indutivo.

Pelo Princípio da Indução Finita, concluímos que a associatividade da multiplicação é válida para todos $n, p, q \in \mathbb{N}$. □

1.4 Estruturas algébricas construídas com Naturais

Até agora, dedicamo-nos a construir o conjunto dos números naturais ($\mathbb{N}$) e a estabelecer as propriedades de suas operações de adição e multiplicação. A próxima etapa é abstrair essas propriedades. Em vez de olharmos apenas para os números, vamos analisar a própria **estrutura** que um conjunto e uma operação formam.

1.4.1 Operação Binária

O primeiro conceito que precisamos para generalizar nossas ideias é o de operação binária.

Definição 1.4.1 (Operação Binária)**.** Dado um conjunto não vazio G, uma **operação binária** (ou lei de composição interna) sobre G é uma função $* : G \times G \to G$.

Em outras palavras, uma operação binária é uma regra que recebe dois elementos quaisquer do conjunto G e produz como resultado um **único** elemento que também

pertence a G. Essa segunda condição — a de que o resultado sempre pertence do conjunto original — é conhecida como a propriedade de **fechamento**. Por convenção, em vez da notação de função $*(a, b)$, usamos a notação infixa $a * b$.

Exemplos:

- A adição, $+$, é uma operação binária em $\mathbb{N}$, pois a soma de dois números naturais é sempre um número natural.
- A multiplicação, $\cdot$, é uma operação binária em $\mathbb{N}$, pois o produto de dois números naturais é sempre um número natural.
- A subtração, $-$, **não é** uma operação binária em $\mathbb{N}$, pois o resultado pode não pertencer a $\mathbb{N}$ (ex: $3 - 5 = -2$, e $-2 \notin \mathbb{N}$). Mais detalhes sobre a subtração serão abordados no capítulo dedicado aos inteiros $\mathbb{Z}$

1.4.2 Semigrupo

A primeira estrutura algébrica que podemos definir é o semigrupo, que apenas exige o fechamento e a associatividade.

Definição 1.4.2 (Semigrupo)**.** Um **semigrupo** $(G, *)$, é uma estrutura na qual G é um conjunto não vazio e $*$ é uma operação binária sobre G que satisfaz a propriedade associativa:

$$\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$$

Exemplos:

- Como provamos que a adição é associativa em $\mathbb{N}$, então $(\mathbb{N}, +)$ é um semigrupo.
- Como também provamos que a multiplicação é associativa em $\mathbb{N}$, então $(\mathbb{N}, \cdot)$ é um semigrupo.

Um semigrupo que também apresenta a propriedade comutativa é chamado de **semigrupo comutativo** ou **abeliano**.

1.4.3 Monoide

Um monoide é um semigrupo que possui um requisito adicional: a existência de um elemento especial que não altera os outros sob a operação.

Definição 1.4.3 (Monoide)**.** Um **monoide** é um semigrupo $(G, *)$ que possui um **elemento identidade** (ou elemento neutro). Isto é, existe um elemento $e \in G$ tal que para todo $a \in G$:

$$a * e = e * a = a$$

Um monoide pode ser representado pela tripla $(G, *, e)$.

Exemplos:

- O semigrupo $(\mathbb{N}, +)$ é um monoide. O elemento identidade é o número 0, pois para qualquer $n \in \mathbb{N}$, temos que $n + 0 = 0 + n = n$. Portanto, $(\mathbb{N}, +, 0)$ é um monoide.
- O semigrupo $(\mathbb{N}, \cdot)$ também é um monoide. O elemento identidade é o número 1, pois para qualquer $n \in \mathbb{N}$, $n \cdot 1 = 1 \cdot n = n$. Portanto, $(\mathbb{N}, \cdot, 1)$ é um monoide.
- Se considerarmos o conjunto dos naturais positivos $\mathbb{N}^* = \{1, 2, 3, \dots\}$, $(\mathbb{N}^*, +)$ é um semigrupo, mas **não** é um monoide, pois o elemento neutro da soma, o 0, não pertence a $\mathbb{N}^*$.

Um monoide que também apresenta a propriedade comutativa é chamado de **monoide comutativo** ou **abeliano**.

Proposição 1.4.1 (Unicidade do Elemento Identidade)**.** Se $(G, *)$ é um monoide, seu elemento identidade é único.

Demonstração. Para provar a unicidade, vamos supor que existam dois elementos identidade em G. Vamos chamá-los de e_1 e e_2.

Por serem elementos identidade, eles devem satisfazer as seguintes condições para todo $a \in G$:

1. $a * e_1 = e_1 * a = a$
2. $a * e_2 = e_2 * a = a$

Agora, vamos considerar o resultado da operação $e_1 * e_2$.

- **Perspectiva 1:** Como e_1 é um elemento identidade, ele não altera nenhum elemento com o qual opera. Portanto, ao operar com e_2, o resultado deve ser e_2.

$$e_1 * e_2 = e_2$$

- **Perspectiva 2:** Por outro lado, como e_2 é um elemento identidade, ele também não altera nenhum elemento com o qual opera. Portanto, ao operar com e_1, o resultado deve ser e_1.

$$e_1 * e_2 = e_1$$

Pela transitividade da igualdade, se $e_1 * e_2$ é igual a e_2 e também igual a e_1, então e_1 e e_2 devem ser iguais:

$$e_1 = e_1 * e_2 = e_2 \implies e_1 = e_2$$

Como e_1 e e_2 foram escolhidos como dois elementos identidade arbitrários, a conclusão de que $e_1 = e_2$ significa que não pode haver mais de um elemento identidade. Portanto, se um semigrupo possui um elemento identidade, ele é necessariamente único. □

Exemplo 1.4.1. Seja o conjunto $G = \mathbb{N}\times\mathbb{N}$, que consiste em todos os pares ordenados (n, m) onde n e m são números naturais. Sobre este conjunto, definimos uma operação de adição da seguinte forma:

$$\forall (n, m), (x, y) \in G, \quad (n, m) + (x, y) := (n + x, m + y)$$

Vamos demonstrar que a estrutura $(G, +)$ é um **monoide comutativo**. Para isso, verificaremos as quatro propriedades necessárias, observando que a operação em cada coordenada é simplesmente a adição em $\mathbb{N}$, cujas propriedades já estabelecemos.

1. **Fechamento (Operação Binária):** Sejam (n, m) e (x, y) elementos de G. Isso significa que $n, m, x, y \in \mathbb{N}$. A soma resulta no par $(n + x, m + y)$. Como $(\mathbb{N}, +)$ é fechado, sabemos que $n+x \in \mathbb{N}$ e $m+y \in \mathbb{N}$. Portanto, o par resultante $(n+x, m+y)$ também pertence a G. A operação é fechada.

2. **Associatividade:** Sejam $a = (n, m)$, $b = (x, y)$ e $c = (p, q)$ em G.

$$\begin{aligned}(a + b) + c &= ((n, m) + (x, y)) + (p, q)\\ &= (n + x, m + y) + (p, q)\\ &= ((n + x) + p, (m + y) + q)\end{aligned}$$

$$\begin{aligned}a + (b + c) &= (n, m) + ((x, y) + (p, q))\\ &= (n, m) + (x + p, y + q)\\ &= (n + (x + p), m + (y + q))\end{aligned}$$

   Como já provamos a associatividade para $(\mathbb{N}, +)$, sabemos que $(n+x)+p = n+(x+p)$ e $(m + y) + q = m + (y + q)$. Logo, $(a + b) + c = a + (b + c)$.

3. **Elemento Identidade:** Procuramos um elemento $e = (e_1, e_2) \in G$ tal que $(n, m)+ e = (n, m)$.

$$(n, m) + (e_1, e_2) = (n + e_1, m + e_2) = (n, m)$$

   Para que a igualdade seja verdadeira, as coordenadas devem ser iguais: $n + e_1 = n$ e $m + e_2 = m$. Como o elemento identidade para $(\mathbb{N}, +)$ é o 0, temos que $e_1 = 0$ e $e_2 = 0$. O elemento identidade de G é, portanto, o par $(0, 0)$, que pertence a G.

4. **Comutatividade:** Sejam $a = (n, m)$ e $b = (x, y)$ em G.

$$a + b = (n, m) + (x, y) = (n + x, m + y)$$

$$b + a = (x, y) + (n, m) = (x + n, y + m)$$

Como já provamos a comutatividade para $(\mathbb{N}, +)$, sabemos que $n + x = x + n$ e $m + y = y + m$. Logo, $a + b = b + a$.

Tendo verificado o fechamento, a associatividade, a existência de um elemento identidade e a comutatividade, concluímos que $(\mathbb{N} \times \mathbb{N}, +)$ é um monoide comutativo, cujo elemento neutro é o par $(0, 0)$.

1.5 Relações de Ordem nos Naturais

Além das estruturas algébricas formadas pela adição e multiplicação, o conjunto dos números naturais possui outra característica fundamental: seus elementos podem ser totalmente ordenados.

1.5.1 Definindo a Ordem a partir da Adição

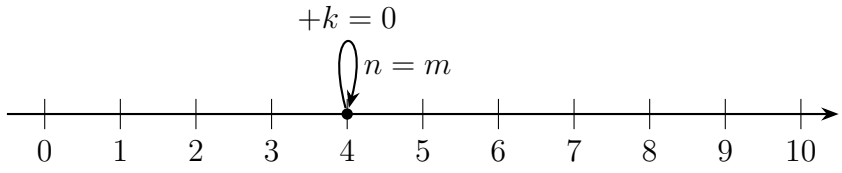
Definição 1.5.1 (Ordem em $\mathbb{N}$)**.** Sejam $n, m \in \mathbb{N}$. Dizemos que n é **menor ou igual a** m, e escrevemos $n \leq m$, se e somente se existe um número natural $k \in \mathbb{N}$ tal que:

$$n + k = m$$

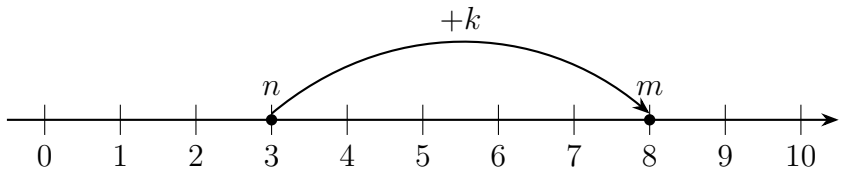
Adicionalmente, dizemos que n é **estritamente menor que** m, e escrevemos $n < m$, se $n \leq m$ e $n \neq m$. Isso é equivalente a dizer que existe um número natural não nulo $k \in \mathbb{N}^*$ tal que $n + k = m$.

Exemplo: $4 \leq 9$ porque existe o número $5 \in \mathbb{N}$ tal que $4 + 5 = 9$. Como $5 \neq 0$, também podemos afirmar que $4 < 9$.

Interpretação Geométrica: A definição de ordem tem uma interpretação geométrica direta na reta numérica. A condição $n \leq m$ significa que podemos **partir** do ponto que representa n e, após **avançar** um número k de passos para a direita, chegamos exatamente ao ponto m. Se $k > 0$, demos pelo menos um passo, o que corresponde à noção de que n está estritamente à esquerda de m. Quando o número de passos a avançar é $k = 0$, a definição $n + k = m$ se torna $n + 0 = m$, o que implica $n = m$. Geometricamente, isso significa que o ponto de partida n e o ponto de chegada m são idênticos. A ida de n até m é um avanço nulo; não damos nenhum passo para a direita.



Neste caso, como $k = 0$, temos $n = m = 4$.



Neste exemplo, $n = 3$, $m = 8$ e $k = 5$.

Proposição 1.5.1 (Todo Natural Não-Nulo é Maior ou Igual a 1)**.** Seja $n \in \mathbb{N}$. Se $n \neq 0$, então $n \geq 1$.

Demonstração. Seja $n \in \mathbb{N}$ com a hipótese de que $n \neq 0$. Como todo Natural não nulo é sucessor de algum número, então um número natural diferente de zero deve ser o sucessor de algum outro natural. Portanto, existe um $k \in \mathbb{N}$ tal que $n = S(k)$.

Nosso objetivo é provar que $n \geq 1$, o que, por definição, equivale a provar que $1 \leq n$. Para isso, devemos encontrar um $p \in \mathbb{N}$ que satisfaça a equação $1 + p = n$.

Conforme demonstrado anteriormente, sabemos que $S(k) = 1 + k$ Como já estabelecemos que $n = S(k)$, podemos substituir para obter:

$$n = 1 + k$$

Escolhendo $p = k$, encontramos o número natural que satisfaz a condição da definição de ordem. Logo, concluímos que $1 \leq n$, o que prova a proposição.

□

1.5.2 Relação de Ordem

Definição 1.5.2 (Relação de Ordem)**.** Uma relação $\preceq$ sobre um conjunto A é chamada de **relação de ordem** se, para quaisquer elementos $a, b, c \in A$, ela for simultaneamente:

1. **Reflexiva:** Todo elemento está relacionado a si mesmo.

$$\forall a \in A, \quad a \preceq a$$

2. **Antissimétrica:** Se um elemento a está relacionado a b e b está relacionado a a,

então a e b devem ser o mesmo elemento.

$$\forall a, b \in A, \quad (a \preceq b \land b \preceq a) \implies a = b$$

3. **Transitiva:** Se a está relacionado a b e b está relacionado a c, então a está relacionado a c.

$$\forall a, b, c \in A, \quad (a \preceq b \land b \preceq c) \implies a \preceq c$$

Adicionalmente, se a relação satisfaz a propriedade de que quaisquer dois elementos são comparáveis (isto é, $\forall a, b \in A$, temos $a \preceq b$ ou $b \preceq a$), ela é chamada de **relação de ordem total**.

Proposição 1.5.2. A relação $\leq$ definida sobre o conjunto dos números naturais, $\mathbb{N}$, é uma **relação de ordem total**.

Demonstração. Para demonstrar que $\leq$ é uma relação de ordem, devemos provar que ela satisfaz as propriedades de reflexividade, antissimetria e transitividade, usando a definição $n \leq m \iff \exists p \in \mathbb{N}$ tal que $n + p = m$.

1. Reflexividade $(n \leq n)$

Devemos mostrar que, para todo $n \in \mathbb{N}$, vale $n \leq n$. Pela definição, isso significa que devemos encontrar um número $p \in \mathbb{N}$ tal que $n + p = n$. Sabemos que o número 0 é o elemento identidade da adição, ou seja, $n + 0 = n$. Como $0 \in \mathbb{N}$, encontramos o p desejado, neste caso, $p = 0$. Portanto, a relação é reflexiva.

2. Antissimetria $(n \leq m \land m \leq n \implies n = m)$

Devemos mostrar que, se $n \leq m$ e $m \leq n$, então necessariamente $n = m$. Assumimos as duas hipóteses:

1. $n \leq m$ implica que existe um $p \in \mathbb{N}$ tal que $n + p = m$.
2. $m \leq n$ implica que existe um $q \in \mathbb{N}$ tal que $m + q = n$.

Vamos substituir a primeira equação na segunda:

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

Pela associatividade da adição, temos:

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

Pela lei do cancelamento da adição, podemos simplificar a equação para:

$$p + q = 0$$

Como p e q são números naturais, a única forma de sua soma ser zero é se ambos forem zero. Logo, $p = 0$ e $q = 0$. Substituindo $p = 0$ na nossa primeira equação, obtemos:

$$n + 0 = m \implies n = m$$

Portanto, a relação é antissimétrica.

3. Transitividade ($n \leq m \wedge m \leq q \implies n \leq q$)

Devemos mostrar que, se $n \leq m$ e $m \leq q$, então $n \leq q$. Assumimos as duas hipóteses:

1. $n \leq m$ implica que existe um $p_1 \in \mathbb{N}$ tal que $n + p_1 = m$.
2. $m \leq q$ implica que existe um $p_2 \in \mathbb{N}$ tal que $m + p_2 = q$.

Nosso objetivo é mostrar que $n \leq q$, ou seja, que existe um $p_3 \in \mathbb{N}$ tal que $n + p_3 = q$.

Vamos substituir a primeira equação na segunda:

$$(n + p_1) + p_2 = q$$

Pela associatividade da adição:

$$n + (p_1 + p_2) = q$$

Seja $p_3 = p_1 + p_2$. Como p_1 e p_2 são números naturais, e a adição é fechada em $\mathbb{N}$, sabemos que p_3 também é um número natural. Encontramos, assim, um $p_3 \in \mathbb{N}$ tal que $n+p_3 = q$. Isso, por definição, significa que $n \leq q$. Portanto, a relação é transitiva.

4. Totalidade ($\forall n, m \in \mathbb{N}$, ou $n \leq m$ ou $m \leq n$)

A prova será feita por indução sobre n. Seja m um número natural qualquer.

Base ($n = 0$): Devemos mostrar que ou $0 \leq m$ ou $m \leq 0$. Como vimos na prova da reflexividade, $0 + m = m$, o que implica que $0 \leq m$ é sempre verdadeiro para qualquer $m \in \mathbb{N}$. Logo, a condição é satisfeita.

Passo Indutivo: Assumimos como hipótese de indução que, para um certo n, a propriedade é válida, ou seja, ou $n \leq m$ ou $m \leq n$ para todo m. Devemos provar que ou $S(n) \leq m$ ou $m \leq S(n)$.

Pela hipótese de indução, temos dois casos:

- *Caso 1:* $n \leq m$. Isso significa que $\exists p \in \mathbb{N}$ tal que $n + p = m$. Se $p = 0$, então $n = m$. Sabemos que $m \leq m + 1 = S(m) = S(n)$, logo a condição $m \leq S(n)$ é satisfeita. Como todo Natural não nulo é sucessor de algum número, se $p \neq 0$, ele deve ser o sucessor de algum outro natural, então $p = S(q)$ para algum $q \in \mathbb{N}$. A equação fica $n + S(q) = m \implies S(n + q) = m \implies S(n) + q = m$. Como $q \in \mathbb{N}$, isso implica, por definição, que $S(n) \leq m$.

- *Caso 2:* $m \leq n$. Sabemos que $n \leq S(n)$, pois $n + 1 = S(n)$. Como $m \leq n$ e $n \leq S(n)$, pela transitividade (já provada), concluímos que $m \leq S(n)$.

Em todos os casos possíveis, mostramos que ou $S(n) \leq m$ ou $m \leq S(n)$. O passo indutivo está completo.

Como a relação $\leq$ é reflexiva, antissimétrica e transitiva e total, provamos que ela é uma relação de ordem total sobre o conjunto dos números naturais.

□

Proposição 1.5.3. Para qualquer $n \in \mathbb{N}$, não existe nenhum número natural m que satisfaça a relação $n < m < S(n)$.

Demonstração. A prova será feita por contradição. Suponha que exista um $m \in \mathbb{N}$ tal que $n < m < S(n)$.

Pela definição de ordem estrita, esta dupla desigualdade nos fornece duas condições:

- $n < m$: Isso significa que existe um $k \in \mathbb{N}^*$ (ou seja, $k \neq 0$) tal que $n + k = m$.
- $m < S(n)$: Isso significa que existe um $l \in \mathbb{N}^*$ (ou seja, $l \neq 0$) tal que $m + l = S(n)$.

Substituindo a primeira equação na segunda, obtemos:

$$(n + k) + l = S(n)$$

Pela associatividade da adição:

$$n + (k + l) = S(n)$$

Substituindo $S(n)$ por $n + 1$:

$$n + (k + l) = n + 1$$

Pela Lei do Cancelamento para a Adição:

$$k + l = 1$$

Agora, vamos analisar as implicações desta igualdade. Como k e l são números naturais, a equação $k + l = 1$ implica que $k \leq 1$.

Ao mesmo tempo, a nossa hipótese inicial é que $k \in \mathbb{N}^*$, ou seja, $k \neq 0$. Como provado na proposição anterior, a condição $k \neq 0$ implica $k \geq 1$.

Agora, temos simultaneamente $k \leq 1$ e $k \geq 1$. Pela propriedade Antissimétrica da relação de ordem $\leq$, a única possibilidade é:

$$k = 1$$

Substituindo $k = 1$ na equação $k + l = 1$, temos $1 + l = 1$. Pela Lei do Cancelamento para a Adição, concluímos que:

$$l = 0$$

Este resultado ($l = 0$) contradiz diretamente a nossa hipótese inicial de que $l \in \mathbb{N}^*$.

A contradição surgiu da nossa suposição de que tal m existia. Portanto, a suposição é falsa, e concluímos que não existe nenhum número natural m entre n e seu sucessor $S(n)$. □

Proposição 1.5.4 (Lei da Tricotomia)**.** Para quaisquer dois números naturais n e m, exatamente uma das três seguintes relações é verdadeira:

1. $n < m$
2. $n = m$
3. $n > m$ (o que é equivalente a $m < n$)

Demonstração. A demonstração desta lei consiste em duas partes: primeiro, provar que pelo menos uma das condições deve ser verdadeira (Existência) e, segundo, provar que apenas uma pode ser verdadeira (Unicidade).

1. Existência (Pelo menos uma condição é verdadeira)

Esta parte é uma consequência direta da propriedade da **Ordem Total** da relação $\leq$, que já demonstramos. A propriedade da totalidade afirma que, para quaisquer $n, m \in \mathbb{N}$, temos:

$$n \leq m \quad \vee \quad m \leq n$$

Vamos analisar os dois casos:

- **Caso 1:** Se $n \leq m$ é verdadeiro, pela própria definição da relação de ordem não estrita, isso significa que ou $n < m$ ou $n = m$. Em ambos os cenários, uma das três condições da tricotomia é satisfeita.
- **Caso 2:** Se $m \leq n$ é verdadeiro, isso significa que ou $m < n$ (o que é o mesmo que $n > m$) ou $m = n$. Novamente, em ambos os cenários, uma das três condições da tricotomia é satisfeita.

Como a totalidade garante que estamos sempre em um desses dois casos, garantimos que pelo menos uma das três relações é sempre verdadeira.

2. Unicidade (Apenas uma condição é verdadeira)

Para provar a unicidade, devemos mostrar que é impossível que duas das condições ocorram simultaneamente. Faremos isso por contradição, analisando todos os pares possíveis.

- **Podem $n = m$ e $n < m$ ocorrerem juntos?** Não. Por definição, $n < m$ implica que $n \leq m$ e $n \neq m$. Isso contradiz diretamente a condição $n = m$.

- **Podem $n = m$ e $n > m$ ocorrerem juntos?** Não. A condição $n > m$ (ou $m < n$) implica que $m \leq n$ e $m \neq n$. Isso também contradiz diretamente a condição $n = m$.

- **Podem $n < m$ e $n > m$ ocorrerem juntos?** Suponha que sim. Se $n < m$, então $n \leq m$. Se $n > m$, então $m < n$, o que implica $m \leq n$. Então, teríamos simultaneamente $n \leq m$ e $m \leq n$. Pela propriedade da **Antissimetria** da relação $\leq$, a única forma de isso ser verdade é se $n = m$. No entanto, as premissas $n < m$ e $n > m$ exigem que $n \neq m$. Chegamos a uma contradição.

Como nenhuma das três condições pode ocorrer em conjunto com qualquer outra, a condição que for verdadeira deve ser única.

Com a existência e a unicidade provadas, a Lei da Tricotomia está demonstrada. □

Agora que estabelecemos que $(\mathbb{N}, \leq)$ é um conjunto totalmente ordenado, o próximo passo é investigar como essa ordem interage com as operações de adição e multiplicação.

Proposição 1.5.5. A relação de ordem $\leq$ em $\mathbb{N}$ é compatível com a adição e a multiplicação. Isto é, para quaisquer $n, m, p, q \in \mathbb{N}$:

1. Se $n \leq m$ e $p \leq q$, então $n + p \leq m + q$.

2. Se $n \leq m$ e $p \leq q$, então $n \cdot p \leq m \cdot q$.

Demonstração. Usaremos a definição de ordem $a \leq b \iff \exists k \in \mathbb{N}, a + k = b$.

1. **Prova para a Adição:** Por hipótese, $n \leq m$ e $p \leq q$. Isso implica que existem $r, s \in \mathbb{N}$ tais que:

   $$n + r = m \quad \text{e} \quad p + s = q$$

   Somando as duas equações, obtemos:

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

   Pela associatividade e comutatividade da adição, podemos reorganizar o lado esquerdo:

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

   Seja $t = r + s$. Como $\mathbb{N}$ é fechado para a adição, $t \in \mathbb{N}$. Encontramos um número natural t que, somado a $(n + p)$, resulta em $(m + q)$. Pela definição de ordem, isso significa que $n + p \leq m + q$.

2. **Prova para a Multiplicação:** Partimos das mesmas hipóteses: $n + r = m$ e $p + s = q$. Vamos analisar o produto $m \cdot q$:

$$m \cdot q = (n + r) \cdot (p + s)$$

Usando a distributividade da multiplicação sobre a adição:

$$m \cdot q = (n + r) \cdot p + (n + r) \cdot s = (n \cdot p + r \cdot p) + (n \cdot s + r \cdot s)$$

Seja $t = r \cdot p + n \cdot s + r \cdot s$. Como $\mathbb{N}$ é fechado para adição e multiplicação, $t \in \mathbb{N}$. A equação se torna:

$$m \cdot q = n \cdot p + t$$

Isso mostra que existe um número natural t que, somado a $n \cdot p$, resulta em $m \cdot q$. Pela definição de ordem, concluímos que $n \cdot p \leq m \cdot q$.

□

Proposição 1.5.6 (Propriedade do Produto Nulo)**.** Sejam $n, m \in \mathbb{N}$. Se $n \cdot m = 0$, então $n = 0$ ou $m = 0$.

Demonstração. Usaremos a propriedade de compatibilidade da ordem com a multiplicação. Se $n \geq 1$ e $m \geq 1$, então:

$$n \cdot m \geq 1 \cdot 1 \implies n \cdot m \geq 1$$

Isso nos leva à conclusão de que o produto $n \cdot m$ deve ser maior ou igual a 1. No entanto, nossa hipótese inicial é de que $n \cdot m = 0$. A conclusão $n \cdot m \geq 1$ contradiz diretamente a hipótese $n \cdot m = 0$. A contradição surgiu de nossa suposição de que n e m eram ambos não nulos. Portanto, a suposição é falsa, e concluímos que pelo menos um deles deve ser zero. □

Proposição 1.5.7 (Lei do Cancelamento para a Ordem)**.** Sejam $n, m, p \in \mathbb{N}$.

1. **Adição:** $n \leq m \iff n + p \leq m + p$.
2. **Multiplicação:** Para $p \neq 0$, $n \leq m \iff n \cdot p \leq m \cdot p$.

Demonstração. Como são equivalências ($\iff$), precisamos provar a ida e a volta para cada caso.

1. Prova para a adição:

($\Rightarrow$) Suponha $n \leq m$. Então $\exists r \in \mathbb{N}$ tal que $n + r = m$. Somando p a ambos os lados, temos $(n + r) + p = m + p$. Reorganizando, $(n + p) + r = m + p$. Isso significa, por definição, que $n + p \leq m + p$.

($\Leftarrow$) Suponha $n+p \leq m+p$. Então $\exists r \in \mathbb{N}$ tal que $(n+p)+r = m+p$. Reorganizando, $(n+r)+p = m+p$. Pela lei do cancelamento para a adição, podemos cancelar o p, resultando em $n+r = m$. Isso significa, por definição, que $n \leq m$.

2. Prova para a multiplicação:

($\Rightarrow$) Suponha $n \leq m$. Então $\exists r \in \mathbb{N}$ tal que $n+r = m$. Multiplicando por p em ambos os lados, temos $(n+r) \cdot p = m \cdot p$. Pela distributividade, $n \cdot p + r \cdot p = m \cdot p$. Como $r \cdot p \in \mathbb{N}$, isso significa, por definição, que $n \cdot p \leq m \cdot p$.

($\Leftarrow$) Agora, suponha, por hipótese, que $n \cdot p \leq m \cdot p$ (com $p \neq 0$). Queremos provar que $n \leq m$.

Considere que a conclusão $n \leq m$ é falsa. Se n não é menor ou igual a m, então a única alternativa possível é que m seja estritamente menor que n. Ou seja:

$$m < n$$

Se $m < n$, pela definição de ordem estrita, sabemos que existe um número natural $s \neq 0$ tal que $m + s = n$.

Multiplicando por p em ambos os lados, temos $(m + s) \cdot p = n \cdot p$. Pela distributividade, $m \cdot p + s \cdot p = n \cdot p$. Pela Propriedade do Produto Nulo $s \cdot p \in \mathbb{N}^*$, isso significa, por definição, que $m \cdot p < n \cdot p$.

Chegamos a duas afirmações conflitantes:
A nossa hipótese inicial nos diz que: $n \cdot p \leq m \cdot p$.
A nossa suposição de que $n \leq m$ era falso nos levou logicamente à conclusão de que: $m \cdot p < n \cdot p$.

É impossível que $m \cdot p$ seja estritamente menor que $n \cdot p$ e, ao mesmo tempo, que $n \cdot p$ seja menor ou igual a $m \cdot p$. Estas duas afirmações são mutuamente exclusivas. Portanto, somos forçados a descartar nossa suposição e concluir que a tese $n \leq m$ deve ser verdadeira.

□

Proposição 1.5.8 (Lei do Cancelamento para a Multiplicação)**.** Sejam $n, m, p \in \mathbb{N}$ com $p \neq 0$. Então:

$$n = m \iff n \cdot p = m \cdot p$$

Demonstração. ($\Rightarrow$) A implicação de ida é direta e válida independentemente de p ser diferente de zero. Se $n = m$ a aplicação da operação de multiplicação por p a ambos os lados deve produzir o mesmo resultado.

($\Leftarrow$) Para a volta, suponha $n \cdot p = m \cdot p$ com $p \neq 0$. Pela Lei da Tricotomia, apenas um dos casos é possível: $n < m$, $n = m$ ou $n > m$.

- Se tivéssemos $n < m$, a Lei do Cancelamento para a Ordem implicaria que $n \cdot p < m \cdot p$, o que contradiz a nossa hipótese de que $n \cdot p = m \cdot p$.
- Se tivéssemos $n > m$, a mesma lei implicaria que $n \cdot p > m \cdot p$, o que também contradiz a hipótese.

A única possibilidade que não leva a uma contradição é $n = m$. Portanto, a equivalência é verdadeira.

□

Definição 1.5.3 (Menor Elemento de um Subconjunto)**.** Seja A um conjunto totalmente ordenado pela relação $\leq$ e seja B um subconjunto de A ($B \subseteq A$). Dizemos que um elemento m é o **menor elemento** (ou **mínimo**) de B se ele satisfaz simultaneamente duas condições:

1. O elemento deve pertencer ao subconjunto: $m \in B$.
2. O elemento deve ser menor ou igual a todos os outros elementos do subconjunto: $\forall b \in B, m \leq b$.

Proposição 1.5.9 (Princípio da Boa Ordem)**.** Todo subconjunto não vazio do conjunto dos números naturais admite um menor elemento.

Demonstração. Suponha, por contradição, que exista um subconjunto $B \subset \mathbb{N}$ que seja **não vazio** e que **não possua** um menor elemento.

Vamos construir um outro conjunto, A, da seguinte forma:

$$A = \{n \in \mathbb{N} \mid n \notin B \text{ e } \forall b \in B, n < b\}$$

Em palavras, A é o conjunto de todos os números naturais que são estritamente menores que *todos* os elementos de B. Note que A está contido no complementar de B em relação a $\mathbb{N}$. Nosso objetivo é mostrar, por indução, que $A = \mathbb{N}$, o que forçaria o conjunto B a ser o conjunto vazio.

Caso Base ($n = 0$): Devemos mostrar que $0 \in A$. Para que $0 \in A$, é preciso que $0 < b$ para todo $b \in B$. Analisemos se 0 pode estar em B. Se $0 \in B$, como $0 \leq k$ para todo $k \in \mathbb{N}$, o 0 seria necessariamente o menor elemento de B. Isso contradiz nossa suposição de que B não tem menor elemento. Logo, $0 \notin B$. Como todo elemento $b \in B$ é um número natural e $b \neq 0$, então $b > 0$. Assim, $0 < b$ para todo $b \in B$, o que prova que $0 \in A$.

Passo Indutivo: Assumimos como hipótese de indução que $n \in A$ para um n arbitrário. Devemos provar que $S(n) \in A$. A hipótese $n \in A$ significa que $\forall b \in B, n < b$.

Isso implica que $n \leq b$ e $n \neq b$. A condição $n \leq b$ nos diz que $\exists p \in \mathbb{N}$ tal que $n + p = b$. Como $n \neq b$, temos $p \neq 0$, logo $p \geq 1$. Assim, podemos escrever $p = S(q)$ para algum $q \in \mathbb{N}$. A equação se torna $n + S(q) = b$, que é o mesmo que $S(n+q) = b$, ou $S(n) + q = b$. Esta última equação significa que $S(n) \leq b$. Como b era um elemento arbitrário de B, esta relação é válida para todos os elementos $b \in B$.

Agora, precisamos nos certificar de que $S(n) \neq b$. Se tivéssemos $S(n) = b$ para algum $b \in B$, como já sabemos que $n < b'$ para todo $b' \in B$, teríamos que $S(n)$ seria o menor elemento de B, pois, $S(n) \in B$ e, como estabelecido anteriormente, $S(n) \leq b'$ para todo $b' \in B$, sendo essas exatamente as condições da definição de menor elemento.

Isso, novamente, contradiz nossa premissa fundamental de que B não possui menor elemento. Logo, $S(n) \neq b$.

Tendo provado que $S(n) \leq b$ e $S(n) \neq b$, concluímos que $S(n) < b$. Como b era um elemento arbitrário de B, isso vale para todos os elementos de B. Assim, $S(n) \in A$.

Pelo Princípio da Indução Finita, provamos que $A = \mathbb{N}$. Isso significa que *todo* número natural é menor que *todos* os elementos de B. Assim, chegamos à conclusão de que B é vazio. Isso contradiz nossa suposição inicial de que B era um conjunto não vazio. A contradição nos força a rejeitar a suposição. Portanto, todo subconjunto não vazio de $\mathbb{N}$ deve, necessariamente, possuir um menor elemento. □

1.5.3 Relação de Divisibilidade

Anteriormente, definimos a relação de ordem $n \leq m$ a partir da existência de um k tal que $n + k = m$. Uma pergunta natural surge: que tipo de relação obteríamos se trocarmos a adição pela multiplicação? Essa investigação nos leva à fundamental noção de divisibilidade.

Para manter a consistência da estrutura, vamos analisar essa nova relação sobre o conjunto dos números naturais diferentes de zero, $\mathbb{N}^* = \{1, 2, 3, \dots\}$, que forma um monoide com a multiplicação $(\mathbb{N}^*, \cdot, 1)$.

Definição 1.5.4 (Relação de Divisibilidade)**.** Sejam $n, m \in \mathbb{N}^*$. Dizemos que n **divide** m, e escrevemos $n|m$, se existe um número natural positivo $k \in \mathbb{N}^*$ tal que:

$$n \cdot k = m$$

Quando $n|m$, também dizemos que n é um **divisor** de m, ou que m é um **múltiplo** de n.

Exemplo: $4|12$ porque existe o número $3 \in \mathbb{N}^*$ tal que $4 \cdot 3 = 12$. No entanto, 4 não divide 13, pois não existe um natural positivo k que satisfaça $4 \cdot k = 13$.

Proposição 1.5.10. A relação de divisibilidade | definida sobre o conjunto $\mathbb{N}^*$ é uma **relação de ordem parcial**.

Demonstração. Para demonstrar esta proposição, devemos provar que a relação | satisfaz as propriedades de reflexividade, antissimetria e transitividade.

1. Reflexividade $(n|n)$

Devemos mostrar que todo elemento de $\mathbb{N}^*$ divide a si mesmo. Pela definição, isso significa que devemos encontrar um $k \in \mathbb{N}^*$ tal que $n \cdot k = n$. Sabemos que 1 é o elemento identidade da multiplicação, ou seja, $n \cdot 1 = n$. Como $1 \in \mathbb{N}^*$, encontramos o k desejado. Portanto, a relação é reflexiva.

2. Antissimetria $(n|m \wedge m|n \implies n = m)$

Assumimos como hipótese que $n|m$ e $m|n$.

- $n|m$ implica que existe um $k_1 \in \mathbb{N}^*$ tal que $n \cdot k_1 = m$.
- $m|n$ implica que existe um $k_2 \in \mathbb{N}^*$ tal que $m \cdot k_2 = n$.

Substituindo a primeira equação na segunda:

$$(n \cdot k_1) \cdot k_2 = n$$

Pela associatividade da multiplicação, temos $n \cdot (k_1 \cdot k_2) = n$. Como estamos em $\mathbb{N}^*$, $n \neq 0$, e podemos usar a Lei do Cancelamento para a multiplicação, obtendo:

$$k_1 \cdot k_2 = 1$$

Lema: Sejam $k_1, k_2 \in \mathbb{N}^*$. Se o produto $k_1 \cdot k_2 = 1$, então necessariamente $k_1 = 1$ e $k_2 = 1$.

Prova do Lema:

A prova será feita por contradição. Assumimos como hipótese que $k_1, k_2 \in \mathbb{N}^*$ e $k_1 \cdot k_2 = 1$. Agora, suponha que a conclusão seja falsa. A negação da conclusão $k_1 = 1$ e $k_2 = 1$ é $k_1 \neq 1$ ou $k_2 \neq 1$.

Sem perda de generalidade, devido à comutatividade da multiplicação, vamos assumir que $k_1 \neq 1$. Como k_1 pertence ao conjunto dos naturais positivos $\mathbb{N}^* = \{1, 2, 3, \dots\}$, a condição $k_1 \neq 1$ implica, pela Lei da Tricotomia, que $k_1 > 1$. Sendo k_1 um número natural, $k_1 > 1$ é equivalente a $k_1 \geq 2$, já que $S(1) = 2$, e, para todo $n \in \mathbb{N}$ não existe $m \in \mathbb{N}$ tal que $n < m < S(n)$.

Ao mesmo tempo, sabemos que $k_2 \in \mathbb{N}^*$, o que implica $k_2 \geq 1$.

Agora, utilizamos a propriedade de compatibilidade da ordem com a multiplicação, que já foi provada. Se $k_1 \geq 2$ e $k_2 \geq 1$, então o produto deve satisfazer:

$$k_1 \cdot k_2 \geq 2 \cdot 1$$

$$k_1 \cdot k_2 \geq 2$$

Este resultado ($k_1 \cdot k_2 \geq 2$) contradiz diretamente a nossa hipótese inicial de que $k_1 \cdot k_2 = 1$. A contradição surgiu da nossa suposição de que pelo menos um dos fatores era diferente de 1. Portanto, a suposição é falsa, e a única possibilidade é que ambos os fatores sejam iguais a 1. Logo, $k_1 = 1$ e $k_2 = 1$.
Com o lema provado, podemos continuar a demonstração.

Substituindo $k_1 = 1$ na nossa primeira equação, obtemos:

$$n \cdot 1 = m \implies n = m$$

Portanto, a relação é antissimétrica.

3. Transitividade $(n|m \wedge m|q \implies n|q)$

Assumimos como hipótese que $n|m$ e $m|q$.

- $n|m$ implica que existe um $k_1 \in \mathbb{N}^*$ tal que $n \cdot k_1 = m$.
- $m|q$ implica que existe um $k_2 \in \mathbb{N}^*$ tal que $m \cdot k_2 = q$.

Substituindo a primeira equação na segunda:

$$(n \cdot k_1) \cdot k_2 = q$$

Pela associatividade, $n \cdot (k_1 \cdot k_2) = q$. Seja $k_3 = k_1 \cdot k_2$. Como $\mathbb{N}^*$ é fechado sob a multiplicação, $k_3 \in \mathbb{N}^*$. Encontramos, assim, um $k_3 \in \mathbb{N}^*$ tal que $n \cdot k_3 = q$, o que, por definição, significa que $n|q$. Portanto, a relação é transitiva. □

Uma Ordem Parcial, mas não Total

Provamos que a relação de divisibilidade é uma relação de ordem parcial. A questão agora é: ela é uma ordem total? Para isso, quaisquer dois elementos de $\mathbb{N}^*$ precisariam ser comparáveis.

Isso não é verdade. Considere os números 2 e 3 em $\mathbb{N}^*$.

- 2 divide 3? Não. Para provar isso, devemos mostrar que não existe $k \in \mathbb{N}^*$ tal que $2 \cdot k = 3$. Usaremos uma prova por contradição. Suponha que tal $k \in \mathbb{N}^*$ exista.

  Como $k \in \mathbb{N}^*$, sabemos que $k \geq 1$. Vamos analisar os dois casos possíveis para k:

  - **Caso 1:** $k = 1$**.** A equação se torna $2 \cdot 1 = 3 \Rightarrow 2 = 3$. O que é uma contradição.

– **Caso 2:** $k > 1$**.** Como não há naturais entre 1 e $S(1) = 2$, a condição $k > 1$ implica $k \geq 2$. Agora, usamos a Compatibilidade da Ordem com a Multiplicação:

$$k \geq 2 \implies 2 \cdot k \geq 2 \cdot 2$$

Sabemos que $2 \cdot 2 = \sigma_2(2) = S(S(2)) = S(3) = 4$. Assim, $2 \cdot k \geq 4$. Nossa suposição inicial era $2 \cdot k = 3$. Isso implicaria $3 \geq 4$. Isso é uma contradição, pois $4 = S(3)$, o que significa $3 < 4$ (pela definição de ordem, $3 + 1 = 4$, e $1 \neq 0$).

Como ambos os casos possíveis ($k = 1$ e $k > 1$) levam a uma contradição, concluímos que tal k não pode existir.

- 3 divide 2? Não. Devemos provar que não existe $k \in \mathbb{N}^*$ tal que $3 \cdot k = 2$. Suponha que tal $k \in \mathbb{N}^*$ exista.

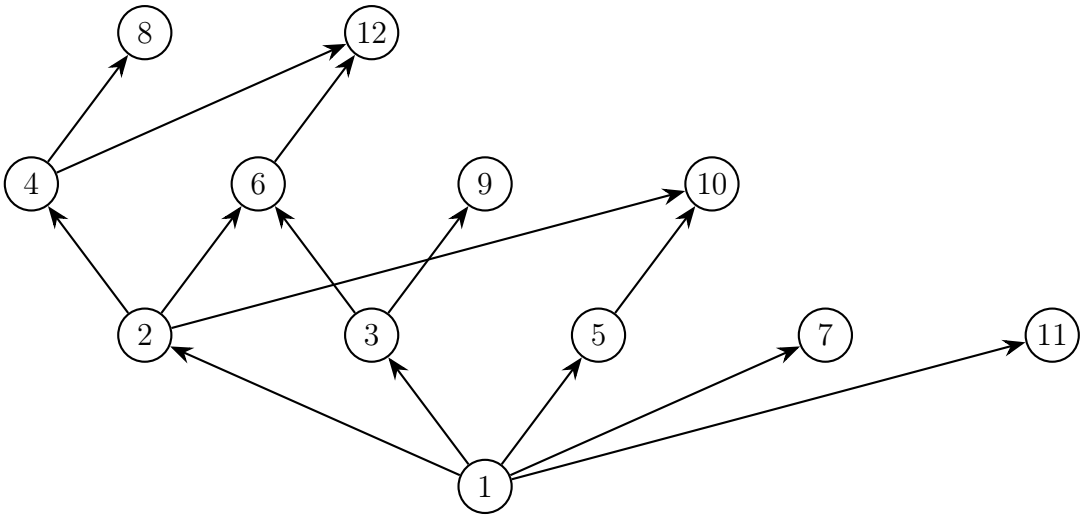
  Como $k \in \mathbb{N}^*$, sabemos que $k \geq 1$. Usando a Compatibilidade da Ordem com a Multiplicação:

$$k \geq 1 \implies 3 \cdot k \geq 3 \cdot 1 \implies 3 \cdot k \geq 3$$

  Nossa suposição era $3 \cdot k = 2$. Isso implicaria $2 \geq 3$. Isso contradiz o fato de que $2 < 3$ (pois $2 + 1 = 3$). Portanto, tal k não pode existir.

Como encontramos um par de elementos $(2, 3)$ para o qual nem $2|3$ nem $3|2$ é verdadeiro, a propriedade da totalidade falha.

A relação de divisibilidade $|$ é uma **relação de ordem parcial** sobre $\mathbb{N}^*$, mas não é uma relação de ordem total. Isso a diferencia fundamentalmente da relação $\leq$, que ordena todos os números naturais em uma única fila. A divisibilidade, por sua vez, cria uma estrutura de ordem mais complexa, com múltiplas ramificações.



1.6 Homomorfismo e Isomorfismo

Definição 1.6.1 (Homomorfismo)**.** Sejam $(G, *)$ e $(H, \#)$ duas estruturas algébricas. Uma função (ou mapeamento) $f : G \to H$ é chamada de **homomorfismo** se ela preserva a operação. Isso significa que, para quaisquer dois elementos $a, b \in G$, a seguinte igualdade é satisfeita:

$$f(a * b) = f(a)\#f(b)$$

Em outras palavras, operar os elementos em G e depois aplicar a função f ao resultado é o mesmo que aplicar f a cada elemento primeiro e depois operar os resultados em H.

Enquanto um homomorfismo estabelece uma relação que preserva a estrutura entre dois conjuntos, um isomorfismo vai além: ele estabelece que duas estruturas são, para todos os efeitos, algebricamente idênticas.

Definição 1.6.2 (Isomorfismo)**.** Um **isomorfismo** é um homomorfismo $f : G \to H$ que também é uma **bijeção**. Isto é, a função f deve satisfazer três condições simultaneamente:

1. **Homomorfismo:** Preserva a operação, $f(a * b) = f(a)\#f(b)$.
2. **Injetividade:** Mapeia elementos distintos para resultados distintos. Se $f(a) = f(b)$, então $a = b$.
3. **Sobrejetividade:** Todo elemento em H é a imagem de algum elemento em G.

Quando existe um isomorfismo entre duas estruturas, dizemos que elas são **isomórficas**.

Exemplo 1.6.1 (Um Homomorfismo da Adição para a Multiplicação)**.** Vamos construir um exemplo de homomorfismo entre os dois monoides que definimos sobre os números naturais:

- O monoide da adição: $(\mathbb{N}, +, 0)$
- O monoide da multiplicação: $(\mathbb{N}, \cdot, 1)$

Seja $a \in \mathbb{N}$ um número natural fixo, com $a > 1$. Definimos a função de exponenciação $\phi_a : \mathbb{N} \to \mathbb{N}$ da seguinte forma:

$$\phi_a(n) := a^n$$

Onde a^n representa $\underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ vezes}}$, e definimos $a^0 = 1$.

Vamos provar que ϕ_a é um homomorfismo do monoide $(\mathbb{N}, +)$ para o monoide $(\mathbb{N}, \cdot)$.

Demonstração. Para que ϕ_a seja um homomorfismo, devemos verificar se $\phi_a(n + m) = \phi_a(n) \cdot \phi_a(m)$ para todos $n, m \in \mathbb{N}$.

Iniciaremos a prova considerando o caso em que $n, m \in \mathbb{N}^*$ (ambos não nulos).

- **Lado Esquerdo:** Pela definição da função, a operação no domínio é a adição:

$$\phi_a(n+m) = a^{n+m}$$

- **Lado Direito:** Pela definição da função, a operação no contradomínio é a multiplicação:

$$\phi_a(n) \cdot \phi_a(m) = a^n \cdot a^m = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ vezes}} \cdot \underbrace{a \cdot a \cdot \cdots \cdot a}_{m \text{ vezes}} = a^{n+m}$$

Precisamos agora verificar os casos que envolvem o elemento neutro 0.

- **Se $n = 0$:** O lado esquerdo da equação do homomorfismo é $\phi_a(0+m) = \phi_a(m) = a^m$. O lado direito é $\phi_a(0) \cdot \phi_a(m) = a^0 \cdot a^m = 1 \cdot a^m = a^m$. A igualdade se mantém.

- **Se $m = 0$:** O lado esquerdo é $\phi_a(n+0) = \phi_a(n) = a^n$. O lado direito é $\phi_a(n) \cdot \phi_a(0) = a^n \cdot a^0 = a^n \cdot 1 = a^n$. A igualdade também se mantém.

Como para todos $n, m \in \mathbb{N}$, o lado esquerdo é igual ao lado direito, a função ϕ_a preserva a operação e é, portanto, um homomorfismo.

Este homomorfismo é um isomorfismo?

- **Injetividade:** Queremos provar que, se $a \in \mathbb{N}$ com $a > 1$, a função $\phi_a(n) = a^n$ é injetiva. Isto é, $\forall n, m \in \mathbb{N}$, se $a^n = a^m$, então $n = m$.

  Assumimos, por hipótese, que $a^n = a^m$. Para provar que $n = m$, usaremos a Lei da Tricotomia. Exatamente uma das três condições é verdadeira: $n < m$, $n > m$, ou $n = m$. Vamos provar por contradição que os dois primeiros casos são impossíveis.

  - **Caso 1: Suponha $n > m$.** Pela definição de ordem em $\mathbb{N}$, se $n > m$, então existe um $k \in \mathbb{N}^*$ (ou seja, $k \geq 1$) tal que $n = m + k$. Substituindo n na nossa hipótese $a^n = a^m$:

    $$a^{m+k} = a^m$$

    Como provado na verificação do homomorfismo, $a^{m+k} = a^m \cdot a^k$. A equação se torna:

    $$a^m \cdot a^k = a^m$$

    Como $a > 1$, temos que $a \geq 2$. Se $m = 0$, $a^m = a^0 = 1$. Se $m > 0$, $a^m = \underbrace{a \cdot \cdots \cdot a}_{m \text{ vezes}} \geq 2$. Em ambos os casos, $a^m \geq 1$. Podemos, portanto, aplicar a Lei do Cancelamento para a Multiplicação à equação $a^m \cdot a^k = a^m \cdot 1$:

    $$a^k = 1$$

Esta é a contradição. Como $k \geq 1$ e $a \geq 2$, o produto $\underbrace{a \cdot a \cdot \cdots \cdot a}_{k \text{ vezes}}$ deve ser maior ou igual a 2. (Formalmente: $a \geq 2$ e $k \geq 1$. Pela compatibilidade da ordem com a multiplicação, $a^k \geq 2^k$. Como $k \geq 1$, $2^k \geq 2^1 = 2$. Logo, $a^k \geq 2$, o que contradiz $a^k = 1$). Portanto, a suposição $n > m$ é falsa.

– **Caso 2: Suponha** $m > n$**.** O argumento é idêntico ao Caso 1, por simetria, e também leva a uma contradição.

Como $n > m$ e $m > n$ são falsos, a única possibilidade restante pela Lei da Tricotomia é $n = m$. Portanto, a função é injetiva.

- **Sobrejetividade:** A função **não** é sobrejetiva. Por exemplo, se $a = 2$, o número 3 pertence ao contradomínio $\mathbb{N}$, mas não existe nenhum número natural n tal que $\phi_2(n) = 2^n = 3$.

Como a função não é sobrejetiva, ela é um homomorfismo injetivo (um monomorfismo), mas não um isomorfismo. □

Exemplo 1.6.2 (Isomorfismo entre os Naturais e os Pares)**.** Vamos provar que o monoide dos números naturais com a adição, $(\mathbb{N}, +, 0)$, é isomórfico ao monoide dos números naturais pares com a adição.

Seja $\mathbb{P} = \{2k \mid k \in \mathbb{N}\} = \{0, 2, 4, 6, \dots\}$ o conjunto dos números naturais pares. A estrutura $(\mathbb{P}, +, 0)$ é um monoide, pois herda a associatividade e o elemento neutro dos Naturais, e é fechado pois a soma de dois números pares é sempre um número par.

Definimos a função $f : \mathbb{N} \to \mathbb{P}$ da seguinte forma:

$$f(n) := 2n$$

Agora, vamos provar que f é um isomorfismo.

Demonstração. **A função é um Homomorfismo:** Devemos verificar se $f(n + m) = f(n) + f(m)$ para todos $n, m \in \mathbb{N}$.

- **Lado Esquerdo:** $f(n + m) = 2(n + m) = 2n + 2m$.
- **Lado Direito:** $f(n) + f(m) = (2n) + (2m) = 2n + 2m$.

Como os lados são iguais, f é um homomorfismo.

A função é Injetiva: Suponha que $f(n) = f(m)$ para $n, m \in \mathbb{N}$.

$$2n = 2m$$

Pela Lei do Cancelamento da Multiplicação, podemos concluir que $n = m$. Portanto, a função é injetiva.

A função é Sobrejetiva: Devemos mostrar que todo elemento do contradomínio $\mathbb{P}$ é a imagem de algum elemento do domínio $\mathbb{N}$.

Seja p um elemento arbitrário de $\mathbb{P}$. Pela definição do conjunto $\mathbb{P}$, sabemos que p é um número par. Isso significa que existe um número natural $k \in \mathbb{N}$ tal que $p = 2k$.

Para que a função seja sobrejetiva, precisamos encontrar um $n \in \mathbb{N}$ tal que $f(n) = p$. Escolhendo $n = k$, temos:

$$f(k) = 2k = p$$

Como para todo $p \in \mathbb{P}$ encontramos um $n \in \mathbb{N}$, que o mapeia, a função é sobrejetiva.

Como a função f é um homomorfismo bijetivo (injetivo e sobrejetivo), ela é um isomorfismo. Isso prova que os monoides $(\mathbb{N}, +)$ e $(\mathbb{P}, +)$ são isomórficos. Embora um conjunto seja um subconjunto próprio do outro, eles possuem exatamente a mesma estrutura aditiva. □

1.7 Teorema Fundamental da Aritmética

1.7.1 Definição de Número Primo

Definição 1.7.1 (Número Primo e Composto)**.** Seja $n \in \mathbb{N}$ um número natural maior que 1 ($n > 1$).

- Dizemos que n é um **número primo** se seus únicos divisores em $\mathbb{N}^*$ são 1 e ele mesmo. Formalmente, para todo $d \in \mathbb{N}^*$, se $d|n$, então $d = 1$ ou $d = n$.
- Dizemos que n é um **número composto** se ele não é primo. Isso significa que existe um divisor $d \in \mathbb{N}^*$ tal que $1 < d < n$.

Nota sobre o número 1: O número 1 não é classificado nem como primo, nem como composto. Ele é o elemento identidade da multiplicação, uma unidade. Excluí-lo da definição de primo é crucial para a unicidade da fatoração que veremos a seguir.

1.7.2 O Teorema Fundamental da Aritmética

Teorema 1.7.1 (Teorema Fundamental da Aritmética)**.** Todo número natural $n > 1$ pode ser escrito como um produto de números primos. Essa fatoração é **única**, desconsiderando a ordem em que os fatores primos aparecem.

Demonstração. A demonstração é tradicionalmente dividida em duas partes: a prova da **existência** da fatoração e a prova de sua **unicidade**.

Prova da Existência (Todo $n > 1$ tem uma fatoração em primos)

Usaremos o Princípio da Boa Ordem em uma prova por contradição. Suponha que exista um conjunto S de números naturais maiores que 1 que *não podem* ser escritos como um produto de primos. Se S não for vazio, pelo Princípio da Boa Ordem, ele deve ter um menor elemento. Vamos chamar esse menor elemento de m.

Se m fosse primo, ele já seria sua própria "fatoração em um produto de um primo", o que contradiz o fato de m pertencer a S. Portanto, m deve ser um número composto.

Lema: Seja m um número natural. Se m é um número composto, então existem números naturais a e b tais que $m = a \cdot b$, com $1 < a < m$ e $1 < b < m$.

Prova do Lema: Partimos da definição de um número composto. Se m é composto, significa que existe um divisor $a \in \mathbb{N}^*$ tal que $1 < a < m$.

Pela definição de divisibilidade, o fato de a ser um divisor de m implica que existe um número $b \in \mathbb{N}^*$ tal que $m = a \cdot b$. Já temos um fator, a, que satisfaz a condição $1 < a < m$. Resta-nos provar que o outro fator, b, também satisfaz a condição $1 < b < m$.

- $b > 1$: Vamos provar por contradição. Suponha que a conclusão seja falsa, ou seja, que $b \leq 1$. Como $b \in \mathbb{N}^*$, a única possibilidade é $b = 1$. Se $b = 1$, a equação da decomposição se torna:

  $$m = a \cdot 1 \implies m = a$$

  Isso, no entanto, contradiz a nossa condição inicial de que $a < m$. Portanto, a suposição de que $b = 1$ é falsa. Concluímos que $b > 1$.

- $b < m$: Sabemos, da condição inicial, que $a > 1$. Partindo da equação $m = a \cdot b$ e sabendo que $b \in \mathbb{N}^*$ (logo $b > 0$), podemos usar a compatibilidade da ordem com a multiplicação: Como $a > 1$, então $a \cdot b > 1 \cdot b$, o que implica $a \cdot b > b$. Substituindo $m = a \cdot b$, obtemos:

  $$m > b$$

  O que é equivalente a $b < m$.

Demonstramos a existência de dois números naturais, a e b, tais que $m = a \cdot b$ e ambos satisfazem as condições $1 < a < m$ e $1 < b < m$. O lema está provado.

Agora, como a e b são menores que m, e m é o *menor* elemento de S, isso significa que nem a nem b podem pertencer a S. Se eles não estão em S, então ambos *podem* ser escritos como um produto de primos.

Digamos que $a = p_1 \cdot p_2 \cdots p_k$ e $b = q_1 \cdot q_2 \cdots q_j$. Mas se isso é verdade, podemos escrever m da seguinte forma:

$$m = a \cdot b = (p_1 \cdot p_2 \cdots p_k) \cdot (q_1 \cdot q_2 \cdots q_j)$$

Isso mostra que m pode ser escrito como um produto de primos, o que contradiz o fato de $m \in S$. A contradição surgiu da suposição de que o conjunto S era não vazio. Logo, S deve ser vazio, e todo número $n > 1$ admite uma fatoração em primos.

Prova da Unicidade da Fatoração

Base da Indução: Para $n = 2$, a única fatoração em primos é o próprio 2. Portanto, a fatoração é única e o resultado é válido para o caso base.

Hipótese de Indução: Assuma que a fatoração em primos é única para todo inteiro k tal que $2 \leq k < n$.

Passo Indutivo: Seja $n > 2$ e suponha que n admite duas fatorações em primos. Ordenando os primos de forma crescente, podemos escrever:

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

onde $p_1 \leq p_2 \leq \cdots \leq p_r$ e $q_1 \leq q_2 \leq \cdots \leq q_s$.

Vamos analisar duas possibilidades para os menores primos, p_1 e q_1.

Caso 1: $p_1 = q_1$
Se os menores primos das duas fatorações são iguais, podemos aplicar a lei do cancelamento da multiplicação:

$$p_1(p_2 \cdots p_r) = q_1(q_2 \cdots q_s) \implies p_2 \cdots p_r = q_2 \cdots q_s$$

Seja $\alpha = p_2 \cdots p_r$. Como $p_1 \geq 2$, temos que $\alpha < n$.

Se $\alpha = 1$, ambas as fatorações originais tinham apenas um primo e eram idênticas. Temos que $\alpha = p_2 \cdots p_r = 1$. Por definição, todo número primo p_i é estritamente maior que 1. O produto de um ou mais números maiores que 1 é, necessariamente, maior que 1. A única forma de $\alpha = p_2 \cdots p_r = 1$ ser verdadeira, é se o produto for **vazio**, ou seja, se a lista de fatores $(p_2, \ldots, p_r)$ for vazia.

Isso significa que o número de fatores r na primeira fatoração era $r = 1$, e a fatoração era simplesmente $n = p_1$. Como $\alpha = q_2 \cdots q_s = 1$, a lista $(q_2, \ldots, q_s)$ também deve ser vazia, significando $s = 1$ e a segunda fatoração era $n = q_1$. Como estamos no **Caso 1**, já assumimos que $p_1 = q_1$. Portanto, as duas fatorações originais eram $n = p_1$ e $n = q_1$, e

são idênticas.

Se $\alpha > 1$, pela nossa hipótese de indução, a fatoração de α é única. Isso significa que a sequência de primos $(p_2, \ldots, p_r)$ deve ser a mesma que a sequência $(q_2, \ldots, q_s)$. Consequentemente, as duas fatorações originais de n eram idênticas.

Caso 2: $p_1 < q_1$

Assumimos que $p_1 < q_1$. Pela definição de ordem nos naturais, existe $k \in \mathbb{N}^*$ tal que $q_1 = p_1 + k$.

Sejam $\alpha = p_2 \cdots p_r$ e $\beta = q_2 \cdots q_s$. A decomposição de n é $p_1\alpha = q_1\beta$. Substituindo q_1:

$$p_1\alpha = (p_1 + k)\beta = p_1\beta + k\beta$$

Como $k\beta$ é um número natural diferente de zero, temos que $p_1\beta < p_1\alpha$. Pela lei do cancelamento para a ordem, concluímos que $\beta < \alpha$. Portanto, existe $l \in \mathbb{N}^*$ tal que $\alpha = \beta + l$.

Substituindo $\alpha = \beta + l$ na equação $p_1\alpha = p_1\beta + k\beta$:

$$p_1(\beta + l) = p_1\beta + k\beta$$

$$p_1\beta + p_1 l = p_1\beta + k\beta$$

Pela lei do cancelamento da adição, obtemos:

$$p_1 l = k\beta$$

Agora, considere o número $k\beta$. Sabemos que $k < q_1$ (pois $q_1 = p_1 + k$ e $p_1 \geq 2$). Assim:

$$k\beta < q_1\beta = q_1(q_2 \cdots q_s) = n$$

Como $k\beta < n$, pela hipótese de indução, a sua decomposição em fatores primos é única.

A igualdade $p_1 l = k\beta$ nos diz que p_1 é um dos fatores primos na decomposição única de $k\beta$. Os fatores primos de $k\beta$ são a união dos fatores primos de k e dos fatores primos de β (que são $q_2, \ldots, q_s$).

Primeiro, vamos mostramos que p_1 não pode ser um fator primo de k:
Suponha, por contradição, que p_1 divide k, então $k = p_1 m$ para algum $m \in \mathbb{N}^*$. Substituindo em $q_1 = p_1 + k$, teríamos $q_1 = p_1 + p_1 m = p_1(1 + m)$. Isso implicaria que p_1 divide q_1. Como q_1 é primo, seus únicos divisores são 1 e q_1. Como $p_1 > 1$, teríamos que ter $p_1 = q_1$, o que contradiz nossa suposição de que $p_1 < q_1$. Logo, p_1 não divide k.

Se p_1 é um fator primo de $k\beta$ mas não de k, ele deve ser um fator primo de $\beta = q_2 \cdots q_s$.

Isso implica que p_1 deve ser igual a um dos q_i para $i \in \{2, \ldots, s\}$. Pela nossa ordenação, $q_1 \leq q_2 \leq \cdots \leq q_s$. Logo, teríamos $q_1 \leq p_1$.

Isso nos leva a uma contradição. Nossa suposição inicial para este caso foi $p_1 < q_1$, e a consequência lógica foi $q_1 \leq p_1$. A suposição de que $p_1 < q_1$ deve ser falsa.

A suposição de que $p_1 \neq q_1$ leva a uma contradição. Portanto, a única possibilidade é $p_1 = q_1$, que, como mostrado no Caso 1, implica que as duas decomposições são idênticas.

Assim, a unicidade da decomposição é válida para n. Pelo princípio da indução, a unicidade é válida para todos os números naturais $n \geq 2$.

□

Corolário 1.7.1.1 (Lema de Euclides)**.** Seja p um número primo. Se p divide o produto de dois números a e b (i.e., $p \mid ab$), então p deve dividir a ou p deve dividir b.

$$\forall a, b \in \mathbb{Z}, \quad p \mid ab \implies p \mid a \vee p \mid b$$

Demonstração. A prova é uma consequência direta da unicidade da fatoração garantida pelo Teorema Fundamental da Aritmética. Se $a = 0$ ou $b = 0$, a afirmação é trivialmente verdadeira. Vamos assumir que $a, b > 1$.

Pelo Teorema Fundamental da Aritmética, a e b possuem fatorações em primos únicas (desconsiderando a ordem):

$$a = p_1 p_2 \cdots p_k$$

$$b = q_1 q_2 \cdots q_j$$

O produto ab é, portanto, o produto dessas duas listas de primos:

$$ab = (p_1 p_2 \cdots p_k) \cdot (q_1 q_2 \cdots q_j)$$

Esta é a **única** decomposição em fatores primos do número ab.

Agora, consideramos a nossa hipótese: $p \mid ab$. Isso significa que p deve ser um dos fatores na decomposição em primos de ab. Pela unicidade da fatoração, p deve ser idêntico a um dos primos da lista $(p_1, \ldots, p_k, q_1, \ldots, q_j)$.

- Se p for um dos p_i (para $i \in \{1, \ldots, k\}$), então p é um dos fatores primos de a, o que significa que $p \mid a$.
- Se p for um dos q_u (para $u \in \{1, \ldots, j\}$), então p é um dos fatores primos de b, o que significa que $p \mid b$.

Como não há outra possibilidade, concluímos que p deve dividir a ou p deve dividir b. □

1.8 A Necessidade de Expandir $\mathbb{N}$

Até este ponto, estabelecemos uma base axiomática sólida para o conjunto dos números naturais, $\mathbb{N}$. Construímos as operações de adição e multiplicação e provamos suas propriedades fundamentais, como associatividade, comutatividade e distributividade. A estrutura $(\mathbb{N}, +)$ é um monoide comutativo, assim como $(\mathbb{N}, \cdot)$.

No entanto, esta estrutura possui limitações algébricas significativas. Embora algumas equações da forma $x + a = b$ possuam solução em $\mathbb{N}$ (por exemplo, $x + 3 = 5$, cuja solução é $x = 2$), muitas outras não.

Considere a seguinte equação, proposta no contexto dos números naturais:

$$x + 2 = 1$$

Podemos provar, usando os axiomas e proposições já estabelecidos, que esta equação não admite solução no conjunto $\mathbb{N}$.

Proposição 1.8.1. Não existe número natural $x \in \mathbb{N}$ que satisfaça a equação $x + 2 = 1$.

Demonstração. Vamos supor, por contradição, que exista um tal $x \in \mathbb{N}$ que satisfaça a equação.

$$x + 2 = 1$$

Das nossas definições, sabemos que $2 = S(1)$ e, como já estabelecido, $S(k) = k + 1$. Portanto, $2 = 1 + 1$. A equação torna-se:

$$x + (1 + 1) = 1$$

Pela associatividade da adição em $\mathbb{N}$, que já demonstramos:

$$(x + 1) + 1 = 1$$

Como $x \in \mathbb{N}$ e $1 \in \mathbb{N}$, o termo $k = x + 1$ é um número natural. A equação se torna:

$$k + 1 = 1$$

Pela propriedade do elemento neutro, $1 = 1 + 0$. Assim:

$$k + 1 = 1 + 0$$

Utilizando a Lei do Cancelamento para a Adição, podemos cancelar o 1:

$$k = 0$$

Substituindo de volta $k = x + 1$, obtemos:

$$x + 1 = 0$$

Sabemos que $1 = S(0)$. A equação é, portanto:

$$x + S(0) = 0$$

Usando a comutatividade da adição e a proposição da Adição do Sucessor, temos que $x + S(0) = S(0) + x = S(0 + x) = S(x)$. Isso nos leva à conclusão:

$$S(x) = 0$$

Esta é uma contradição direta do **Axioma 3**, que afirma que o zero não é sucessor de nenhum número natural.

Como nossa suposição inicial levou a uma contradição, ela deve ser falsa. Portanto, não existe nenhum número natural x que resolva a equação $x + 2 = 1$. □

Esta limitação é a motivação central para a construção do próximo conjunto numérico.

Capítulo 2

Inteiros

2.1 Relações de Equivalência

Em nossa análise anterior, exploramos as relações de ordem, como $\leq$ e $|$, que nos permitem comparar elementos e estabelecer uma hierarquia. Agora, vamos nos voltar para um tipo diferente de relação, cujo propósito não é ordenar, mas sim agrupar elementos que compartilham uma propriedade em comum. Essas são as relações de equivalência.

2.1.1 Definição de Relação de Equivalência

Uma relação de equivalência generaliza a noção de igualdade. Para ser considerada como tal, uma relação precisa satisfazer três axiomas específicos.

Definição 2.1.1 (Relação de Equivalência)**.** Uma relação $\sim$ sobre um conjunto não vazio A é chamada de **relação de equivalência** se, para quaisquer elementos $a, b, c \in A$, ela for simultaneamente:

1. **Reflexiva:** Todo elemento é equivalente a si mesmo.

$$\forall a \in A, \quad a \sim a$$

2. **Simétrica:** Se a é equivalente a b, então b é equivalente a a.

$$\forall a, b \in A, \quad (a \sim b) \implies (b \sim a)$$

3. **Transitiva:** Se a é equivalente a b e b é equivalente a c, então a é equivalente a c.

$$\forall a, b, c \in A, \quad (a \sim b \land b \sim c) \implies (a \sim c)$$

2.1.2 Classes de Equivalência e o Conjunto Quociente

A consequência mais importante de uma relação de equivalência sobre um conjunto é que ela o **particiona** em subconjuntos disjuntos, chamados de classes de equivalência.

Definição 2.1.2 (Classe de Equivalência)**.** Dada uma relação de equivalência $\sim$ sobre um conjunto A, a **classe de equivalência** de um elemento $a \in A$, denotada por $[a]$ ou $\overline{a}$, é o conjunto de todos os elementos de A que são equivalentes a a.

$$[a] = \overline{a} = \{x \in A \mid x \sim a\}$$

Definição 2.1.3 (Conjunto Quociente)**.** O conjunto de todas as classes de equivalência de A pela relação $\sim$ é chamado de **conjunto quociente**, e é denotado por $A/\sim$.

$$A/\sim = \{[a] \mid a \in A\}$$

O conjunto de todas as classes de equivalência de A forma uma **partição** de A. Isso significa que os subconjuntos (as classes) são dois a dois disjuntos e que sua união reconstrói o conjunto A original. Nenhum elemento de A fica de fora e nenhum pertence a duas classes diferentes.

Proposição 2.1.1. Dada uma relação de equivalência $\sim$ sobre um conjunto não vazio A, o conjunto quociente $A/\sim$ (o conjunto de todas as classes de equivalência) forma uma partição de A.

Demonstração. Para demonstrar que as classes de equivalência formam uma partição de A, precisamos provar duas condições fundamentais:

1. A união de todas as classes de equivalência é igual ao conjunto A.
2. Quaisquer duas classes de equivalência são ou idênticas ou disjuntas (sua interseção é vazia).

1. A união das classes de equivalência é o próprio conjunto A

Devemos provar que $\bigcup_{a\in A}[a] = A$. Para isso, provamos a inclusão em ambos os sentidos.

($\subseteq$) *Prova de que* $\bigcup_{a\in A}[a] \subseteq A$.
Seja x um elemento qualquer da união, $x \in \bigcup_{a\in A}[a]$. Por definição de união, isso significa que x pertence a pelo menos uma classe de equivalência. Ou seja, existe um $a \in A$ tal que $x \in [a]$. Pela definição de classe de equivalência, se $x \in [a]$, então $x \in A$. Portanto, todo elemento da união também é um elemento de A.

($\supseteq$) *Prova de que* $A \subseteq \bigcup_{a \in A}[a]$.

Seja a um elemento qualquer de A. Queremos mostrar que a pertence à união de todas as classes. Como $\sim$ é uma relação de equivalência, ela é **reflexiva**. Portanto, $a \sim a$. Pela definição da classe de equivalência $[a] = \{x \in A \mid x \sim a\}$, a condição $a \sim a$ implica que $a \in [a]$. Como a pertence à sua própria classe de equivalência, e a união contém todas as classes (incluindo $[a]$), concluímos que $a \in \bigcup_{a \in A}[a]$. Portanto, todo elemento de A também é um elemento da união.

Como provamos a inclusão em ambos os sentidos, concluímos que $\bigcup_{a \in A}[a] = A$.

2. Duas classes de equivalência são idênticas ou disjuntas

Devemos provar que para quaisquer $a, b \in A$, ou $[a] = [b]$ ou $[a] \cap [b] = \emptyset$. Vamos assumir que as classes **não** são disjuntas, ou seja, que sua interseção não é vazia: $[a] \cap [b] \neq \emptyset$. Nosso objetivo é provar que, sob esta condição, as classes devem ser idênticas: $[a] = [b]$.

Se a interseção não é vazia, então existe pelo menos um elemento c que pertence a ambas as classes.

$$c \in [a] \quad \text{e} \quad c \in [b]$$

Pela definição de classe de equivalência, isso nos fornece duas relações:

- $c \sim a$
- $c \sim b$

Como $\sim$ é uma relação de equivalência, ela é **simétrica**. Da primeira relação, $c \sim a$, podemos concluir que $a \sim c$. Agora, temos as relações $a \sim c$ e $c \sim b$. Como a relação é **transitiva**, podemos concluir que:

$$a \sim b$$

Agora que sabemos que a é equivalente a b, vamos provar que suas classes são idênticas:

- Seja x um elemento qualquer de $[a]$. Por definição, $x \sim a$. Como já sabemos que $a \sim b$, pela **transitividade** da relação, temos que $x \sim b$. Se $x \sim b$, então por definição $x \in [b]$. Logo, todo elemento de $[a]$ está em $[b]$.
- Seja y um elemento qualquer de $[b]$. Por definição, $y \sim b$. Como sabemos que $a \sim b$, pela **simetria** da relação, temos que $b \sim a$. Pela **transitividade**, de $y \sim b$ e $b \sim a$, concluímos que $y \sim a$. Se $y \sim a$, então por definição $y \in [a]$. Logo, todo elemento de $[b]$ está em $[a]$.

Como $[a] \subseteq [b]$ e $[b] \subseteq [a]$, concluímos que $[a] = [b]$.

Assim, mostramos que se duas classes de equivalência têm qualquer elemento em comum, elas são necessariamente a mesma classe. A única alternativa restante é que, se

não são a mesma classe, não podem ter nenhum elemento em comum, sendo portanto disjuntas.

Tendo provado ambas as condições, concluímos que o conjunto de todas as classes de equivalência forma uma partição de A. □

Exemplo 2.1.1 (A Relação de Paridade)**.** Uma das formas mais comuns de agrupar números é pela sua paridade. Podemos formalizar isso com uma relação de equivalência.

Definições:

- Dizemos que um número $n \in \mathbb{N}$ é **par** se existe um $k \in \mathbb{N}$ tal que $n = 2 \cdot k$.
- Dizemos que um número $n \in \mathbb{N}$ é **ímpar** se existe um $k \in \mathbb{N}$ tal que $n = S(2 \cdot k)$ (ou $n = 2 \cdot k + 1$).
- Dizemos que n **tem a mesma paridade que** m (e escrevemos $n \sim m$) se ocorre uma das duas condições: (1) n e m são ambos pares, ou (2) n e m são ambos ímpares.

É direta a verificação que esta relação é:

- **Reflexiva:** Todo número tem a mesma paridade que si mesmo.
- **Simétrica:** Se n tem a mesma paridade que m, então m tem a mesma paridade que n.
- **Transitiva:** Se n tem a mesma paridade que m, e m tem a mesma paridade que k, então n tem a mesma paridade que k.

Portanto, a paridade é uma relação de equivalência.

Classes de Equivalência

Esta relação divide o conjunto infinito dos números naturais em apenas **duas** classes de equivalência:

1. A classe de equivalência do 0, denotada por $[0]$. Ela contém todos os números naturais que são equivalentes ao 0, ou seja, todos os números pares.

$$[0] = \{n \in \mathbb{N} \mid n \text{ é par}\} = \{0, 2, 4, 6, 8, \dots\}$$

2. A classe de equivalência do 1, denotada por $[1]$. Ela contém todos os números naturais que são equivalentes ao 1, ou seja, todos os números ímpares.

$$[1] = \{n \in \mathbb{N} \mid n \text{ é ímpar}\} = \{1, 3, 5, 7, 9, \dots\}$$

Note que $[2] = [0]$, $[4] = [0]$, $[3] = [1]$, e assim por diante. Qualquer número par pertence à classe $[0]$ e qualquer ímpar à classe $[1]$.

Operações com as Classes de Equivalência

As operações de adição e multiplicação de classes de equivalência são definidas sobre os representantes. Para a adição de duas classes $[a]$ e $[b]$, o resultado é a classe de sua soma, $[a + b]$. O mesmo vale para a multiplicação: $[a] \cdot [b] = [a \cdot b]$. Agora, vamos investigar o que acontece quando somamos ou multiplicamos elementos pertencentes a essas classes. Para isso, lembramos que um número par pode ser escrito como $2k$ e um ímpar como $2k + 1$ para algum $k \in \mathbb{N}$.

Análise da Adição:

- **Par + Par:** Seja $a = 2k_1$ e $b = 2k_2$. A soma é $a + b = 2k_1 + 2k_2 = 2(k_1 + k_2)$. O resultado é um múltiplo de 2, logo, é **par**. Conclusão: $[0] + [0] = [0]$.

- **Ímpar + Ímpar:** Seja $a = 2k_1 + 1$ e $b = 2k_2 + 1$. A soma é $a + b = (2k_1 + 1) + (2k_2 + 1) = 2k_1 + 2k_2 + 2 = 2(k_1 + k_2 + 1)$. O resultado é um múltiplo de 2, logo, é **par**. Conclusão: $[1] + [1] = [0]$.

- **Par + Ímpar:** Seja $a = 2k_1$ e $b = 2k_2 + 1$. A soma é $a + b = 2k_1 + (2k_2 + 1) = 2(k_1 + k_2) + 1$. O resultado tem a forma de um número ímpar, logo, é **ímpar**. Conclusão: $[0] + [1] = [1]$.

  Devido à Comutatividade da Adição em $\mathbb{N}$, a soma **Ímpar + Par** $(b + a = (2k_2 + 1) + 2k_1)$ é idêntica à soma **Par + Ímpar** $(a + b)$, resultando em $2(k_2 + k_1) + 1$, que também é um número ímpar. Assim, $[1] + [0] = [1]$.

Análise da Multiplicação:

- **Par · Par:** Seja $a = 2k_1$ e $b = 2k_2$. O produto é $a \cdot b = (2k_1)(2k_2) = 4k_1k_2 = 2(2k_1k_2)$. O resultado é **par**. Conclusão: $[0] \cdot [0] = [0]$.

- **Ímpar · Ímpar:** Seja $a = 2k_1+1$ e $b = 2k_2+1$. O produto é $a \cdot b = (2k_1+1)(2k_2+1) = 4k_1k_2 + 2k_1 + 2k_2 + 1 = 2(2k_1k_2 + k_1 + k_2) + 1$. O resultado é **ímpar**. Conclusão: $[1] \cdot [1] = [1]$.

- **Par · Ímpar:** Seja $a = 2k_1$ e $b = 2k_2 + 1$. O produto é $a \cdot b = (2k_1)(2k_2 + 1) = 4k_1k_2+2k_1 = 2(2k_1k_2+k_1)$. O resultado é um múltiplo de 2, logo, é **par**. Conclusão: $[0] \cdot [1] = [0]$.

  Devido a Comutatividade da Multiplicação em $\mathbb{N}$, o produto **Ímpar · Par** $(b \cdot a = (2k_2 + 1)(2k_1))$ é idêntico ao produto **Par · Ímpar** $(a \cdot b)$, resultando na mesma expressão $2(2k_1k_2 + k_1)$, que é um número par. Assim, $[1] \cdot [0] = [0]$.

Note que não importa qual representante da classe seja tomado, o resultado é sempre o mesmo.

Partição e Conjunto Quociente

As duas classes, $[0]$ e $[1]$, formam uma partição de $\mathbb{N}$, pois são disjuntas ($[0] \cap [1] = \emptyset$) e sua união é o próprio conjunto $\mathbb{N}$ ($[0] \cup [1] = \mathbb{N}$).

O conjunto quociente é o conjunto formado por estas classes. É um novo conjunto com apenas dois elementos:

$$\mathbb{N}/\sim \quad = \quad \{[0], [1]\}$$

2.2 Construção de $\mathbb{Z}$ via Relação de Equivalência

Definição 2.2.1 (Relação de Equivalência em $\mathbb{N} \times \mathbb{N}$)**.** Seja o conjunto $\mathbb{N} \times \mathbb{N}$. Definimos a relação $\sim$ sobre este conjunto da seguinte forma: para quaisquer pares (a, b) e (c, d),

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Proposição 2.2.1. A relação $\sim$ é uma relação de equivalência.

Demonstração. Devemos verificar as três propriedades: reflexividade, simetria e transitividade.

Reflexividade: *Devemos provar que* $(a, b) \sim (a, b)$. Pela definição da relação, isso significa provar que $a + b = b + a$. Isso é verdade devido à comutatividade da adição em $\mathbb{N}$.

Simetria: *Devemos provar que se* $(a, b) \sim (c, d)$*, então* $(c, d) \sim (a, b)$. A hipótese $(a, b) \sim (c, d)$ nos diz que $a + d = b + c$. Queremos provar que $c + b = d + a$. Pela comutatividade da adição em $\mathbb{N}$, podemos reescrever a hipótese:

$$a + d = b + c \implies b + c = a + d \implies c + b = d + a$$

Isso é exatamente a condição para que $(c, d) \sim (a, b)$.

Transitividade: *Devemos provar que se* $(a, b) \sim (c, d)$ *e* $(c, d) \sim (e, f)$*, então* $(a, b) \sim (e, f)$. Temos como hipóteses:

1. $(a, b) \sim (c, d) \implies a + d = b + c$
2. $(c, d) \sim (e, f) \implies c + f = d + e$

Nosso objetivo é provar que $a + f = b + e$. Vamos somar as duas equações das hipóteses:

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

Usando a associatividade e a comutatividade da adição em $\mathbb{N}$, podemos reorganizar ambos os lados:

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

Agora, usamos a Lei do Cancelamento para a adição em $\mathbb{N}$, cancelando o termo $(c+d)$ de ambos os lados. O resultado é $a + f = b + e$. Esta é a condição para que $(a, b) \sim (e, f)$.

Como a relação $\sim$ é reflexiva, simétrica e transitiva, ela é uma relação de equivalência.

□

2.2.1 Classes de Equivalência em $\mathbb{N} \times \mathbb{N}$

Tendo estabelecido que $\sim$ é uma relação de equivalência, sabemos que ela particiona o conjunto $\mathbb{N} \times \mathbb{N}$ em classes de equivalência. Cada uma dessas classes será, por definição, um número inteiro.

Para entender a natureza dessas classes, podemos usar a Lei da Tricotomia dos números naturais, que nos diz que para qualquer par (a, b), exatamente uma de três condições é verdadeira: $a > b$, $a < b$, ou $a = b$.

O primeiro componente é maior ($a > b$)

Pela definição de ordem que estabelecemos, $a > b$ significa que existe um número natural **não nulo** $k \in \mathbb{N}^*$ tal que $a = b + k$. Isso nos diz que qualquer par nesta situação pode ser escrito na forma $(b + k, b)$.

Todo par da forma $(b + k, b)$ é equivalente ao par simplificado $(k, 0)$. Para mostrar que $(b + k, b) \sim (k, 0)$, usamos a definição da nossa relação (se $(a, b) \sim (c, d)$, então $a + d = b + c$):

$$(b + k) + 0 = b + k$$

Como a igualdade é trivialmente verdadeira, a equivalência está confirmada.

Isto nos diz que qualquer par (a, b) onde a é k unidades maior que b pertence à mesma classe de equivalência do par $(k, 0)$. Por exemplo, os pares $(5, 2)$, $(6, 3)$ e $(10, 7)$ são todos equivalentes a $(3, 0)$, pois em todos eles a primeira componente é 3 unidades maior que a segunda. Essas classes, representadas por $\overline{(k, 0)}$ com $k \in \mathbb{N}^*$, formarão os **inteiros positivos**.

O primeiro componente é menor ($a < b$)

Neste caso, existe um $k \in \mathbb{N}^*$ tal que $b = a + k$. O par é da forma $(a, a + k)$.

Todo par da forma $(a, a + k)$ é equivalente ao par simplificado $(0, k)$. Para mostrar que $(a, a + k) \sim (0, k)$, usamos a definição da nossa relação (se $(a, b) \sim (c, d)$, então

$a + d = b + c$):

$$a + k = (a + k) + 0$$

A igualdade é novamente verdadeira.

Pares como $(2, 5)$, $(3, 6)$ e $(7, 10)$ são todos equivalentes a $(0, 3)$, pois em todos eles a segunda componente é 3 unidades maior que a primeira. Essas classes, representadas por $\overline{(0, k)}$ com $k \in \mathbb{N}^*$, formarão os **inteiros negativos**.

Os componentes são iguais ($a = b$)

O par é da forma (a, a). Todo par da forma (a, a) é equivalente ao par $(0, 0)$:

$$a + 0 = a + 0$$

Todos os pares com componentes iguais, como $(3, 3)$ e $(5, 5)$, pertencem a uma única e mesma classe. Esta classe, representada por $\overline{(0, 0)}$, formará o **inteiro zero**.

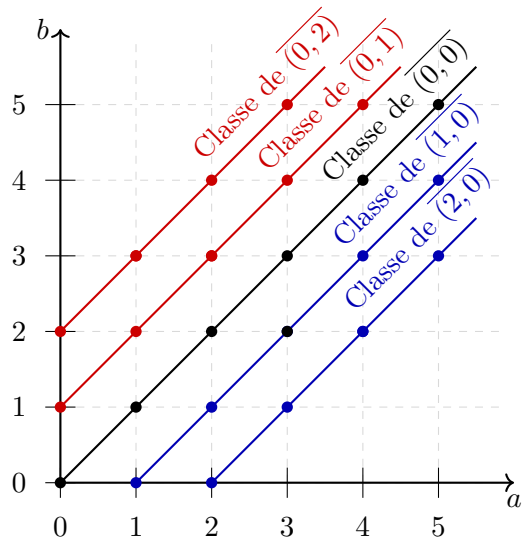
Com isso, podemos ver que todo o conjunto infinito de pares em $\mathbb{N} \times \mathbb{N}$ é particionado em três tipos de classes, cada uma com um representante canônico.

Definição 2.2.2 (O Conjunto dos Números Inteiros)**.** O conjunto dos números inteiros, denotado por $\mathbb{Z}$, é definido como o conjunto quociente de $\mathbb{N}\times\mathbb{N}$ pela relação de equivalência $\sim$.

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$$

Cada elemento de $\mathbb{Z}$ é uma classe de equivalência $\overline{(a, b)}$. Podemos representá-lo através de seus representantes canônicos:

$$\mathbb{Z} = \{\overline{(k, 0)} \mid k \in \mathbb{N}^*\} \cup \{\overline{(0, 0)}\} \cup \{\overline{(0, k)} \mid k \in \mathbb{N}^*\}$$



2.3 Adição e Multipliação em $\mathbb{Z}$

Definição 2.3.1 (Adição de Inteiros)**.** Sejam dois inteiros representados pelas classes de equivalência $\overline{(a,b)}$ e $\overline{(c,d)}$. A soma deles é definida como:

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

Proposição 2.3.1. A adição em $\mathbb{Z}$ é bem-definida.

Demonstração. Para que a operação seja bem-definida, o resultado não pode depender dos representantes escolhidos para cada classe. Suponha que $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$. Por definição de equivalência, isso nos fornece duas hipóteses:

1. $a + b' = b + a'$
2. $c + d' = d + c'$

Devemos mostrar que a soma leva à mesma classe resultante, ou seja, que $\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$. Isso é equivalente a provar que:

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

Somando nossas duas equações de hipótese, temos:

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

Usando a associatividade e a comutatividade da adição em $\mathbb{N}$ para reorganizar os termos, chegamos a:

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

Isso é exatamente o que queríamos provar. Portanto, a adição em $\mathbb{Z}$ está bem-definida. □

Definição 2.3.2 (Multiplicação de Inteiros)**.** Sejam dois inteiros representados pelas classes de equivalência $\overline{(a,b)}$ e $\overline{(c,d)}$. A multiplicação entre eles é definida como:

$$\overline{(a,b)} \cdot \overline{(c,d)} := \overline{(ac+bd, ad+bc)}$$

Proposição 2.3.2. A multiplicação em $\mathbb{Z}$ é bem-definida.

Demonstração. Para que a operação seja bem-definida, o resultado não pode depender dos representantes escolhidos para cada classe. Suponha que $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$. Por definição de equivalência, isso nos fornece duas hipóteses:

1. $a + b' = b + a'$

2. $c + d' = d + c'$

Devemos mostrar que a multiplicação leva à mesma classe resultante, ou seja, que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$.
A demonstração será feita em duas etapas para maior clareza, utilizando a transitividade. Primeiro, mostraremos que a mudança de representante na primeira classe não altera o resultado. Em seguida, mostraremos o mesmo para a segunda classe.

Etapa 1: Provar que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c,d)}$. Usando a hipótese (1), $a + b' = b + a'$, devemos mostrar que $\overline{(ac + bd, ad + bc)} = \overline{(a'c + b'd, a'd + b'c)}$. Pela definição, isso significa provar a igualdade:

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

A partir da hipótese $a + b' = b + a'$, multiplicando por c e por d (o que é permitido em $\mathbb{N}$), obtemos:

- $c(a + b') = c(b + a') \implies ac + b'c = bc + a'c$
- $d(b + a') = d(a + b') \implies bd + a'd = ad + b'd$

Somando as duas equações resultantes:

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

Pela comutatividade da adição em $\mathbb{N}$, podemos reorganizar os termos para agrupar os elementos da classe resultante:

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

Isso prova que $\overline{(ac + bd, ad + bc)} = \overline{(a'c + b'd, a'd + b'c)}$, completando a Etapa 1.

Etapa 2: Provar que $\overline{(a',b')} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$. A lógica é análoga a da Etapa 1. A hipótese agora é $c + d' = d + c'$. O objetivo é provar que $\overline{(a'c + b'd, a'd + b'c)} = \overline{(a'c' + b'd', a'd' + b'c')}$. Pela definição, é o mesmo que provar a igualdade:

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

A partir da hipótese $c + d' = d + c'$, multiplicando por a' e por b', obtemos:

- $a'(c + d') = a'(d + c') \implies a'c + a'd' = a'd + a'c'$

- $b'(d+c') = b'(c+d') \implies b'd + b'c' = b'c + b'd'$

Somando as duas equações resultantes:

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

Pela comutatividade da adição em $\mathbb{N}$, podemos reorganizar os termos de ambos os lados para agrupar os elementos da forma que desejamos:

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

Isso prova que $\overline{(a'c + b'd, a'd + b'c)} = \overline{(a'c' + b'd', a'd' + b'c')}$, completando a Etapa 2.

Pela Etapa 1, sabemos que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c,d)}$. Pela Etapa 2, sabemos que $\overline{(a',b')} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$. Pela transitividade da igualdade, concluímos que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$. Portanto, a multiplicação em $\mathbb{Z}$ está bem-definida. □

2.3.1 Propriedades das Operações em $\mathbb{Z}$

Sejam $x = \overline{(a,b)}$, $y = \overline{(c,d)}$ e $z = \overline{(e,f)}$ números inteiros arbitrários.

Proposição 2.3.3 (Comutatividade das Operações)**.** Tanto a adição quanto a multiplicação em $\mathbb{Z}$ são comutativas.

Demonstração. **Adição**
Devemos provar que $x + y = y + x$.
Calculamos os dois lados da equação usando a definição de adição em $\mathbb{Z}$:

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

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

Para mostrar que estas duas classes são iguais, devemos mostrar que os pares $(a+c, b+d)$ e $(c+a, d+b)$ são equivalentes. Pela definição da relação $\sim$, isso significa verificar se $(a+c)+(d+b) = (b+d)+(c+a)$. Como a adição em $\mathbb{N}$ é comutativa e associativa, as duas somas são claramente iguais. Portanto, $x + y = y + x$.

Multiplicação
Devemos provar que $x \cdot y = y \cdot x$.
Calculamos os dois lados da equação usando a definição de multiplicação em $\mathbb{Z}$:

$$x \cdot y = \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac + bd, ad + bc)}$$

$$y \cdot x = \overline{(c,d)} \cdot \overline{(a,b)} = \overline{(ca + db, cb + da)}$$

Devemos mostrar que as classes são iguais, ou seja, que $(ac+bd, ad+bc) \sim (ca+db, cb+da)$. Isso requer verificar se:

$$(ac + bd) + (cb + da) = (ad + bc) + (ca + db)$$

Como a adição e a multiplicação em $\mathbb{N}$ são comutativas e associativas, os dois lados da equação são claramente iguais. Portanto, $x \cdot y = y \cdot x$.

□

Proposição 2.3.4 (Associatividade das Operações)**.** Tanto a adição quanto a multiplicação em $\mathbb{Z}$ são associativas.

Demonstração. **Adição**
Devemos provar que $(x + y) + z = x + (y + z)$.
Calculamos o Lado Esquerdo (LE):

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

Calculamos o Lado Direito (LD):

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

Pela associatividade da adição em $\mathbb{N}$, sabemos que $(a + c) + e = a + (c + e)$ e $(b + d) + f = b + (d + f)$. Portanto, os pares resultantes são idênticos, e $(LE) = (LD)$.

Multiplicação
Devemos provar que $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
Calculamos o Lado Esquerdo (LE):

$$\begin{aligned}(LE) &= (\overline{(a, b)} \cdot \overline{(c, d)}) \cdot \overline{(e, f)} \\ &= \overline{(ac + bd, ad + bc)} \cdot \overline{(e, f)} \\ &= \overline{((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)} \\ &= \overline{(ace + bde + adf + bcf, acf + bdf + ade + bce)}\end{aligned}$$

Calculamos o Lado Direito (LD):

$$\begin{aligned}(LD) &= \overline{(a, b)} \cdot (\overline{(c, d)} \cdot \overline{(e, f)}) \\ &= \overline{(a, b)} \cdot \overline{(ce + df, cf + de)} \\ &= \overline{(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))} \\ &= \overline{(ace + adf + bcf + bde, acf + ade + bce + bdf)}\end{aligned}$$

Usando a comutatividade da adição em $\mathbb{N}$ para reordenar os termos nas componentes, vemos que os pares resultantes são idênticos. Portanto, $(LE) = (LD)$. □

Proposição 2.3.5 (Distributividade da Multiplicação sobre a Adição)**.** A multiplicação em $\mathbb{Z}$ distribui sobre a adição.

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

Demonstração. Calculamos o Lado Esquerdo (LE):

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

Calculamos o Lado Direito (LD):

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

Usando a comutatividade da adição em $\mathbb{N}$ para reordenar os termos nas componentes, vemos que os pares resultantes são idênticos. Portanto, $(LE) = (LD)$. □

Proposição 2.3.6 (Elementos Identidade em $\mathbb{Z}$)**.**

1. A classe de equivalência $\overline{(0,0)}$ é o elemento identidade aditivo em $\mathbb{Z}$.
2. A classe de equivalência $\overline{(1,0)}$ é o elemento identidade multiplicativo em $\mathbb{Z}$.

Demonstração. Seja $\overline{(a,b)}$ um elemento arbitrário de $\mathbb{Z}$.

1. Identidade Aditiva

Devemos provar que $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$ e $\overline{(0,0)} + \overline{(a,b)} = \overline{(a,b)}$. Aplicando a definição de adição em $\mathbb{Z}$:

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

Como 0 é o elemento identidade da adição em $\mathbb{N}$, sabemos que $a + 0 = a$ e $b + 0 = b$.

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

Assim, $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$. A igualdade $\overline{(0,0)} + \overline{(a,b)} = \overline{(a,b)}$ segue da Comutatividade da Adição em $\mathbb{Z}$, já demonstrada.

2. Identidade Multiplicativa

Devemos provar que $\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a,b)}$ e $\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(a,b)}$. Aplicando a definição de multiplicação em $\mathbb{Z}$:

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

Utilizando as propriedades do elemento identidade multiplicativo (1) e do elemento absorvente (0) da multiplicação em $\mathbb{N}$:

- $a \cdot 1 = a$
- $b \cdot 0 = 0$
- $a \cdot 0 = 0$
- $b \cdot 1 = b$

Substituindo estes resultados e usando a propriedade da identidade aditiva $n + 0 = n$:

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

Assim, $\overline{(a,b)} \cdot \overline{(1,0)} = \overline{(a,b)}$. A igualdade $\overline{(1,0)} \cdot \overline{(a,b)} = \overline{(a,b)}$ segue da Comutatividade da Multiplicação em $\mathbb{Z}$ já demonstrada.

Portanto, as classes $\overline{(0,0)}$ e $\overline{(1,0)}$ atuam como as identidades aditiva e multiplicativa em $\mathbb{Z}$, respectivamente. □

Proposição 2.3.7 (Elemento Absorvente)**.** O elemento identidade aditivo de $\mathbb{Z}$, a classe $\overline{(0,0)}$, é o elemento absorvente para a multiplicação em $\mathbb{Z}$. Para todo $x \in \mathbb{Z}$, temos:

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

Demonstração. Como já provamos que a multiplicação é comutativa, basta analisar o caso $x \cdot \overline{(0,0)}$. Seja $x = \overline{(a,b)}$ um inteiro arbitrário.

Aplicamos a definição de multiplicação em $\mathbb{Z}$:

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

Pelas propriedades do zero em $\mathbb{N}$ (onde $n \cdot 0 = 0$ e $0 + 0 = 0$), as coordenadas se tornam:

$$\overline{(0 + 0, 0 + 0)} = \overline{(0,0)}$$

Concluímos que a classe $\overline{(0,0)}$ é um elemento absorvente para a multiplicação. □

2.4 Identificando os Naturais Dentro dos Inteiros

Até agora, construímos os inteiros $\mathbb{Z}$ como um conjunto de classes de equivalência, $\overline{(a,b)}$. Esta notação é formalmente correta, mas inconveniente. Queremos justificar o uso da notação usual, como $-2, 0, 3$, e entender como (ou onde?) os números naturais estão dentro dessa nova estrutura.

Faremos isso mostrando que o subconjunto dos inteiros não-negativos se comporta exatamente da mesma maneira que o conjunto dos números naturais.

Proposição 2.4.1. Existe um isomorfismo entre o monoide dos números naturais $(\mathbb{N}, +)$ e o subconjunto dos inteiros não-negativos.

Demonstração. Para provar isso, vamos definir uma função (um mapeamento) $\phi : \mathbb{N} \to \mathbb{Z}_{\geq 0}$ que leva cada número natural para a sua classe de equivalência correspondente a um inteiro não-negativo.

$$\phi(n) := \overline{(n,0)}$$

Agora, vamos mostrar que este mapeamento preserva a estrutura.

O Mapeamento é Injetivo

Devemos mostrar que se dois números naturais são mapeados para a mesma classe, eles devem ser o mesmo número. Suponha que $\phi(n) = \phi(m)$ para $n, m \in \mathbb{N}$.

$$\overline{(n,0)} = \overline{(m,0)}$$

Pela definição da nossa relação de equivalência, isso significa:

$$n + 0 = m + 0 \implies n = m$$

Como o mapeamento leva números diferentes a classes diferentes, ele é injetivo.

O Mapeamento é Sobrejetivo

Devemos mostrar que todo inteiro não-negativo é a imagem de algum número natural através de ϕ.

Seja $\mathbb{Z}_{\geq 0}$ o subconjunto dos inteiros não-negativos. Um elemento arbitrário $z \in \mathbb{Z}_{\geq 0}$ é uma classe de equivalência $\overline{(a,b)}$ com $a, b \in \mathbb{N}$ e $a \geq b$.

Pela definição da relação de ordem em $\mathbb{N}$, se $a \geq b$, então existe um único número natural k tal que $a = b + k$.

Assim, podemos reescrever a classe z:

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

Para que o mapeamento seja sobrejetivo, precisamos encontrar um $n \in \mathbb{N}$ tal que $\phi(n) = z = \overline{(k,0)}$. Escolhendo $n = k$, temos:

$$\phi(k) = \overline{(k,0)}$$

Como para todo elemento z no contradomínio encontramos um elemento no domínio que o mapeia, a função ϕ é sobrejetiva.

O Mapeamento Preserva a Adição

Devemos mostrar que somar dois naturais e depois mapear o resultado é o mesmo que mapeá-los primeiro e depois somar as classes. Queremos provar que $\phi(n+m) = \phi(n) + \phi(m)$.

- **Lado Esquerdo:** $\phi(n+m) = \overline{(n+m,0)}$.
- **Lado Direito:** $\phi(n) + \phi(m) = \overline{(n,0)} + \overline{(m,0)} = \overline{(n+m,0+0)} = \overline{(n+m,0)}$.

Como os dois lados são iguais, a estrutura da adição é preservada.

O Mapeamento Preserva a Multiplicação

De forma análoga, queremos provar que $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

- **Lado Esquerdo:** $\phi(n \cdot m) = \overline{(nm,0)}$.
- **Lado Direito:** $\phi(n) \cdot \phi(m) = \overline{(n,0)} \cdot \overline{(m,0)} = \overline{(n \cdot m + 0 \cdot 0, n \cdot 0 + 0 \cdot m)} = \overline{(nm,0)}$.

A estrutura da multiplicação também é preservada. □

Como o mapeamento ϕ é bijetivo e preserva todas as operações (é um homomorfismo), ele estabelece que o conjunto dos naturais $(\mathbb{N}, +, \cdot)$ e o subconjunto de inteiros $\{\overline{(n,0)} \mid n \in \mathbb{N}\}$ são estruturalmente idênticos (isomórficos).

Isso nos permite, sem prejuízos, simplificar nossa notação e **identificar** o número natural com sua classe correspondente:

- A classe $\overline{(m,m)} = \overline{(0,0)}$ será denotada simplesmente por $\mathbf{0}$.
- Cada classe $\overline{(m,0)}$, para $m \in \mathbb{N}^*$, será denotada simplesmente por $\mathbf{m}$.

Com a identificação dos números naturais dentro de $\mathbb{Z}$, resta-nos atribuir um significado às classes restantes, da forma $\overline{(0,m)}$ para $m \in \mathbb{N}^*$. A identidade destes elementos está intrinsecamente ligada à noção de um oposto aditivo, um conceito que a estrutura dos números naturais não possuía e que agora podemos formalizar.

Definição 2.4.1 (Elemento Inverso Aditivo)**.** Para uma classe de equivalência $\overline{(a,b)}$, seu inverso aditivo, que denotamos por $-\overline{(a,b)}$, é uma classe $\overline{(x,y)}$ tal que $\overline{(a,b)} + \overline{(x,y)} = \overline{(0,0)}$, que é o nosso elemento identidade.

$$\overline{(a+x,b+y)} = \overline{(0,0)} \implies (a+x)+0 = (b+y)+0 \implies a+x = b+y$$

A escolha mais simples para x e y que satisfaz esta condição é $x = b$ e $y = a$. Portanto, o inverso de $\overline{(a,b)}$ é a classe $\overline{(b,a)}$.

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

Por exemplo, o inverso de $\overline{(3,0)}$ é $\overline{(0,3)}$.

Proposição 2.4.2. Todo elemento $z \in \mathbb{Z}$ possui um único elemento inverso aditivo em $\mathbb{Z}$.

Demonstração. A demonstração se divide em duas partes: provar a existência do elemento inverso e, em seguida, provar que ele é único. Como a existência é garantida pela definição de inverso aditivo, resta provar que para cada $z \in \mathbb{Z}$ ele é único.

Unicidade

Para provar que o inverso aditivo é único, vamos supor que um elemento $z = \overline{(a,b)}$ possua dois inversos aditivos distintos, z' e z''. Por definição de inverso, eles devem satisfazer:

1. $z + z' = \overline{(0,0)}$
2. $z + z'' = \overline{(0,0)}$

Nosso objetivo é mostrar que, necessariamente, $z' = z''$.

$$\begin{aligned}
z' &= z' + \overline{(0,0)} && \text{(Propriedade do elemento identidade)}\\
&= z' + (z + z'') && \text{(Substituindo pela hipótese 2)}\\
&= (z' + z) + z'' && \text{(Associatividade da adição em } \mathbb{Z})\\
&= (z + z') + z'' && \text{(Comutatividade da adição em } \mathbb{Z})\\
&= \overline{(0,0)} + z'' && \text{(Substituindo pela hipótese 1)}\\
&= z'' && \text{(Propriedade do elemento identidade)}
\end{aligned}$$

A sequência de igualdades nos força a concluir que $z' = z''$. Nossa suposição inicial de que poderiam existir dois inversos distintos nos levou à conclusão de que eles são, na verdade, o mesmo elemento. Portanto, o inverso aditivo de qualquer inteiro é único. □

Com base no que foi estabelecido, podemos agora completar nossa notação. Já identificamos o natural m com a classe $\overline{(m,0)}$. A definição de elemento inverso nos mostra que o inverso de $\overline{(m,0)}$ é a classe $\overline{(0,m)}$. Portanto, é natural denotar a classe $\overline{(0,m)}$ como $-\mathbf{m}$, o oposto aditivo de m.

2.4.1 Subtração em $\mathbb{Z}$

Definição 2.4.2 (Subtração de Inteiros)**.** A subtração de dois inteiros é definida como a soma do primeiro com o inverso aditivo do segundo.

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

Usando a definição de inverso, isso se torna:

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

Com a notação usual: Sejam $p, q \in \mathbb{N}$. A operação $p - q$ em $\mathbb{Z}$ corresponde à soma do inteiro p com o inteiro $-q$:

$$p - q = p + (-q) = \overline{(p,0)} + \overline{(0,q)} = \overline{(p+0, 0+q)} = \overline{(p,q)}$$

A classe $\overline{(p,q)}$ é o resultado formal da operação.

Proposição 2.4.3. Para todo $n \in \mathbb{N}$, temos que $-n = (-1) \cdot n$.

Demonstração. Para provar esta igualdade no conjunto dos inteiros $\mathbb{Z}$, devemos mostrar que a classe de equivalência que representa $-n$ é a mesma que a classe resultante do produto das classes que representam -1 e n.

Primeiro, vamos identificar cada termo como uma classe de equivalência, com base nas definições já estabelecidas:

- O número natural n é representado pela classe $\overline{(n,0)}$.
- O inteiro $-n$ é o inverso aditivo de n, representado pela classe $\overline{(0,n)}$.
- O inteiro 1 é representado por $\overline{(1,0)}$. Seu inverso aditivo, -1, é, portanto, a classe $\overline{(0,1)}$.

O lado esquerdo da nossa proposição, $-n$, corresponde à classe $\overline{(0,n)}$.

Agora, vamos calcular o lado direito, $(-1) \cdot n$, usando a definição de multiplicação em $\mathbb{Z}$:

$$(-1) \cdot n = \overline{(0,1)} \cdot \overline{(n,0)}$$

A definição de multiplicação é $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$. Para o nosso caso, temos $a = 0$, $b = 1$, $c = n$ e $d = 0$. Substituindo na fórmula:

$$\overline{(0,1)} \cdot \overline{(n,0)} = \overline{((0 \cdot n) + (1 \cdot 0)), ((0 \cdot 0) + (1 \cdot n))}$$

Avaliando os produtos e as somas dentro das coordenadas, utilizando as propriedades do 0 e do 1 nos naturais, obtemos:

$$\overline{(0+0, 0+n)} = \overline{(0,n)}$$

O resultado do produto $(-1) \cdot n$ é a classe $\overline{(0,n)}$.

Comparando os dois lados, vemos que o lado esquerdo, $-n$, e o lado direito, $(-1) \cdot n$, são ambos representados pela mesma classe de equivalência $\overline{(0,n)}$. Portanto, a igualdade $-n = (-1) \cdot n$ é verdadeira.

□

2.5 Relações de Ordem nos Inteiros

Tendo estabelecido a estrutura algébrica dos inteiros, o próximo passo é dotar o conjunto $\mathbb{Z}$ de uma relação de ordem. De forma análoga à construção dos naturais, nossa abordagem será fundamentar esta nova relação na ordem já conhecida de $\mathbb{N}$.

2.5.1 Definindo a Ordem a partir dos Naturais

Definição 2.5.1 (Ordem em $\mathbb{Z}$)**.** Sejam $x = \overline{(a,b)}$ e $y = \overline{(c,d)}$ dois números inteiros. Dizemos que x é **menor ou igual a** y, e escrevemos $x \leq y$, se e somente se a seguinte relação for válida no conjunto dos números naturais:

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

Para que esta definição seja válida, primeiro precisamos garantir que a relação não dependa dos representantes escolhidos para as classes.

Proposição 2.5.1. A relação de ordem $\leq$ em $\mathbb{Z}$ é bem-definida.

Demonstração. Suponha que $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$. Isso nos fornece como hipóteses as igualdades em $\mathbb{N}$:

1. $a + b' = b + a'$

2. $d + c' = c + d'$

Devemos mostrar que $a+d \leq b+c \iff a'+d' \leq b'+c'$. Vamos provar a implicação ($\Rightarrow$). Assumimos que $a + d \leq b + c$. Pela definição de ordem em $\mathbb{N}$, existe um $k \in \mathbb{N}$ tal que $(a+d)+k = b+c$. Somando as duas equações das hipóteses, obtemos $(a+b')+(d+c') = (b + a') + (c + d')$. Pela associatividade e comutatividade, podemos reorganizar para:

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

Agora, substituímos $b + c$ pela nossa primeira expressão:

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

Pela lei do cancelamento da adição em $\mathbb{N}$ (cancelando o termo $a + d$), obtemos:

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

Rearranjando, temos $(a' + d') + k = b' + c'$. Como $k \in \mathbb{N}$, esta equação é a definição de $a' + d' \leq b' + c'$. A implicação ($\Leftarrow$) é análoga. Portanto, a relação está bem-definida. □

Exemplo 2.5.1. Para ilustrar como a definição formal se conecta à nossa intuição sobre a ordem dos inteiros, vejamos alguns casos:

- **Vamos verificar que $3 \leq 7$:**
  - Identificamos os inteiros: $x = 3 = \overline{(3, 0)}$ e $y = 7 = \overline{(7, 0)}$.
  - Temos $a = 3, b = 0$ e $c = 7, d = 0$.
  - A condição a ser verificada em $\mathbb{N}$ é $a + d \leq b + c$.
  - Substituindo: $3 + 0 \leq 0 + 7 \implies 3 \leq 7$. Como a afirmação é verdadeira nos naturais, a relação $3 \leq 7$ é válida nos inteiros.
- **Vamos verificar que $-4 \leq 2$:**
  - Identificamos os inteiros: $x = -4 = \overline{(0, 4)}$ e $y = 2 = \overline{(2, 0)}$.
  - Temos $a = 0, b = 4$ e $c = 2, d = 0$.
  - A condição a ser verificada em $\mathbb{N}$ é $a + d \leq b + c$.
  - Substituindo: $0 + 0 \leq 4 + 2 \implies 0 \leq 6$. Como a afirmação é verdadeira nos naturais, a relação $-4 \leq 2$ é válida nos inteiros.
- **Vamos verificar que $-5 \leq -2$:**
  - Identificamos os inteiros: $x = -5 = \overline{(0, 5)}$ e $y = -2 = \overline{(0, 2)}$.

- Temos $a = 0, b = 5$ e $c = 0, d = 2$.
- A condição a ser verificada em $\mathbb{N}$ é $a + d \leq b + c$.
- Substituindo: $0 + 2 \leq 5 + 0 \implies 2 \leq 5$. Como a afirmação é verdadeira nos naturais, a relação $-5 \leq -2$ é válida nos inteiros.

2.5.2 Ordem e a Operação de Subtração

Agora que definimos a ordem em $\mathbb{Z}$ de maneira formal, podemos conectá-la a uma noção mais intuitiva, utilizando a operação de subtração que já estabelecemos. Veremos que a nossa definição abstrata é perfeitamente equivalente à ideia de que um número é menor que outro se a diferença entre eles for não-negativa.

Proposição 2.5.2. Para quaisquer inteiros $x, y \in \mathbb{Z}$, a relação $x \leq y$ é equivalente a afirmar que o resultado da subtração $y - x$ é um inteiro não-negativo.

Demonstração. Sejam $x = \overline{(a, b)}$ e $y = \overline{(c, d)}$ dois inteiros.

A nossa definição de ordem estabelece que:

$$x \leq y \iff a + d \leq b + c \quad (\text{em } \mathbb{N})$$

Agora, vamos calcular a subtração $y - x$ utilizando a definição formal:

$$\begin{aligned} y - x &= \overline{(c, d)} - \overline{(a, b)} \\ &= \overline{(c, d)} + (-\overline{(a, b)}) && \text{(Definição de subtração)} \\ &= \overline{(c, d)} + \overline{(b, a)} && \text{(Definição de inverso aditivo)} \\ &= \overline{(c + b, d + a)} && \text{(Definição de adição em } \mathbb{Z}) \end{aligned}$$

O resultado da subtração é a classe de equivalência $\overline{(c + b, d + a)}$. Para que este inteiro seja **não-negativo**, por definição, a sua primeira componente deve ser maior ou igual à segunda, quando vistas como números naturais. Ou seja:

$$y - x \text{ é não-negativo} \iff c + b \geq d + a \quad (\text{em } \mathbb{N})$$

Pela comutatividade da adição em $\mathbb{N}$, a condição $c + b \geq d + a$ é a mesma que $b + c \geq a + d$. Esta, por sua vez, é a mesma condição que a nossa definição original de ordem, $a + d \leq b + c$.

Portanto, demonstramos a seguinte cadeia de equivalências:

$$x \leq y \iff a + d \leq b + c \iff c + b \geq d + a \iff y - x \text{ é um inteiro não-negativo}$$

Isso conclui a prova. A partir desta proposição, podemos usar a notação mais familiar: $x \leq y \iff y - x \geq 0$.

Adicionalmente, podemos definir a ordem estrita da seguinte forma:

$$x < y \iff x \leq y \wedge x \neq y \iff y - x \text{ é um inteiro positivo (maior que zero)}$$

□

Observação: Afirmar que o inteiro $y - x$ é não-negativo é equivalente a dizer que $y - x$ corresponde a um número natural $k \in \mathbb{N}$ (através do isomorfismo que identifica $\mathbb{N}$ com o subconjunto de inteiros não-negativos $\mathbb{Z}_{\geq 0}$). Portanto, a condição $x \leq y$ em $\mathbb{Z}$ é equivalente a:

$$y - x = k, \quad \text{para algum } k \in \mathbb{N}$$

$$y = x + k, \quad \text{para algum } k \in \mathbb{N}$$

Esta formulação ($y = x + k$ com $k \in \mathbb{N}$) é precisamente a forma como a ordem foi definida originalmente no conjunto dos números naturais. Isso demonstra que a ordem que definimos em $\mathbb{Z}$ é uma extensão consistente da ordem natural, preservando a estrutura de $(\mathbb{N}, \leq)$ dentro de $(\mathbb{Z}, \leq)$.

2.5.3 Propriedades da Relação de Ordem

Proposição 2.5.3. A relação $\leq$ definida sobre o conjunto dos números inteiros, $\mathbb{Z}$, é uma **relação de ordem total**.

Demonstração. Devemos provar que a relação é reflexiva, antissimétrica, transitiva e total.

1. Reflexividade ($x \leq x$)

Seja $x = \overline{(a, b)}$. Devemos mostrar que $\overline{(a, b)} \leq \overline{(a, b)}$. Pela definição, isso requer que $a + b \leq b + a$. Como a adição em $\mathbb{N}$ é comutativa, temos $a + b = b + a$, o que satisfaz a condição. A relação é reflexiva.

2. Antissimetria ($x \leq y \wedge y \leq x \implies x = y$)

Suponha que $x = \overline{(a, b)} \leq y = \overline{(c, d)}$ e $y = \overline{(c, d)} \leq x = \overline{(a, b)}$. Pela definição, temos duas condições em $\mathbb{N}$:

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

Como a relação $\leq$ é antissimétrica em $\mathbb{N}$, estas duas condições implicam que $a + d = b + c$. Esta é precisamente a definição da relação de equivalência $\overline{(a, b)} \sim \overline{(c, d)}$. Portanto, $x = y$. A relação é antissimétrica.

3. Transitividade ($x \leq y \wedge y \leq z \implies x \leq z$)

Sejam $x = \overline{(a, b)}$, $y = \overline{(c, d)}$ e $z = \overline{(e, f)}$. Suponha que $x \leq y$ e $y \leq z$. Temos então:

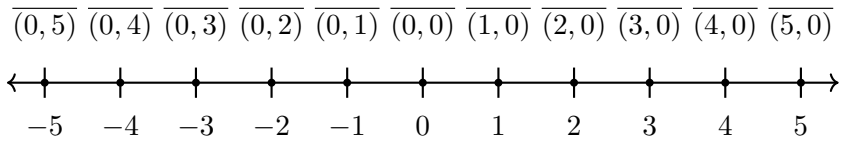
- $a + d \leq b + c \implies \exists k_1 \in \mathbb{N}, (a + d) + k_1 = b + c$
- $c + f \leq d + e \implies \exists k_2 \in \mathbb{N}, (c + f) + k_2 = d + e$

Somando as duas equações: $(a+d)+k_1+(c+f)+k_2 = (b+c)+(d+e)$. Reorganizando: $(a + f) + (c + d) + (k_1 + k_2) = (b + e) + (c + d)$. Pela lei do cancelamento da adição em $\mathbb{N}$, cancelamos $(c + d)$, resultando em $(a + f) + (k_1 + k_2) = b + e$. Como $k_1 + k_2 \in \mathbb{N}$, esta equação significa que $a + f \leq b + e$, o que por sua vez significa que $x \leq z$. A relação é transitiva.

4. Totalidade

Para quaisquer dois inteiros $x = \overline{(a, b)}$ e $y = \overline{(c, d)}$, devemos mostrar que $x \leq y$ ou $y \leq x$. Isso equivale a mostrar que, em $\mathbb{N}$, ou $a + d \leq b + c$ ou $b + c \leq a + d$. Como a, b, c, d são números naturais, as somas $a + d$ e $b + c$ também o são. Como já provado, a relação $\leq$ é uma ordem total em $\mathbb{N}$, portanto, quaisquer dois naturais são comparáveis. Assim, a condição é sempre satisfeita. □

Por ser um conjunto totalmente ordenado, podemos organizar os Inteiros em uma reta numérica, seguindo a relação de ordem que definimos:



Uma diferença fundamental entre a estrutura de ordem de $\mathbb{N}$ e a de $\mathbb{Z}$ é a perda do Princípio da Boa Ordem. Enquanto todo subconjunto não-vazio de números naturais possui um menor elemento, o mesmo não é verdade para os inteiros. Para demonstrar isso, basta encontrar um único subconjunto de $\mathbb{Z}$ que seja não-vazio mas que não contenha um elemento mínimo. O próprio conjunto dos inteiros, $\mathbb{Z}$, serve como contraexemplo. Ele é evidentemente não-vazio, mas não possui um menor elemento, pois para qualquer inteiro z que possamos escolher, o inteiro $z - 1$ também pertence a $\mathbb{Z}$ e é estritamente menor que z. Como é sempre possível encontrar um elemento menor, nenhum elemento pode ser o mínimo. Portanto $(\mathbb{Z}, \leq)$ não é um conjunto bem-ordenado.

2.5.4 Compatibilidade com as Operações Algébricas

Proposição 2.5.4. A relação de ordem em $\mathbb{Z}$ é compatível com a adição. Para quaisquer $x, y, z \in \mathbb{Z}$:

$$x \leq y \implies x + z \leq y + z$$

Demonstração. Sejam $x = \overline{(a, b)}$, $y = \overline{(c, d)}$ e $z = \overline{(e, f)}$. A hipótese $x \leq y$ significa que $a + d \leq b + c$. Queremos provar que $x + z \leq y + z$.

$$x + z = \overline{(a + e, b + f)} \quad \text{e} \quad y + z = \overline{(c + e, d + f)}$$

Pela definição de ordem em $\mathbb{Z}$, a desigualdade $x + z \leq y + z$ é verdadeira se:

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

Partindo da desigualdade que sabemos ser verdadeira:

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

Adicionando $(e + f)$ em ambos os lados:

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

Reorganizando os termos pela comutatividade e associatividade em $\mathbb{N}$:

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

Chegamos exatamente na condição que garante que a desigualdade $x + z \leq y + z$ é verdadeira.

□

Proposição 2.5.5 (Compatibilidade da Ordem com a Multiplicação)**.** Sejam $x, y, z \in \mathbb{Z}$. A relação de ordem se comporta da seguinte maneira em relação à multiplicação:

1. Se $x \leq y$ e $z > 0$, então $x \cdot z \leq y \cdot z$ (a desigualdade é preservada).
2. Se $x \leq y$ e $z < 0$, então $x \cdot z \geq y \cdot z$ (a desigualdade é invertida).
3. Se $z = 0$, então $x \cdot z = y \cdot z = 0$.

Demonstração. A forma mais clara de demonstrar esta proposição é utilizar a equivalência $x \leq y \iff y - x \geq 0$. Seja $w = y - x$. A nossa hipótese inicial, $x \leq y$, significa que o inteiro w é não-negativo ($w \geq 0$).

Para determinar a relação entre $x \cdot z$ e $y \cdot z$, analisaremos o sinal da diferença $(y \cdot z) - (x \cdot z)$. Assumindo a distributividade da multiplicação sobre a adição (uma propriedade que se herda da estrutura dos naturais), colocando o z em evidência, temos:

$$(y \cdot z) - (x \cdot z) = (y - x) \cdot z = w \cdot z$$

A prova se resume, então, a determinar o sinal do produto $w \cdot z$, sabendo que $w \geq 0$.

- **Caso 1:** $z > 0$ **(Multiplicador positivo)**
  Temos $w \geq 0$ e $z > 0$. Como w é não-negativo, ele pode ser representado pela classe $\overline{(k, 0)}$ para algum $k \in \mathbb{N}$. Como z é positivo, ele pode ser representado por $\overline{(s, 0)}$

para algum $s \in \mathbb{N}^*$. Calculando o produto:

$$w \cdot z = \overline{(k,0)} \cdot \overline{(s,0)} = \overline{(k \cdot s + 0 \cdot 0, k \cdot 0 + 0 \cdot s)} = \overline{(k \cdot s, 0)}$$

Como $k \in \mathbb{N}$ e $s \in \mathbb{N}^*$, o produto $k \cdot s$ é um número natural ($k \cdot s \geq 0$). A classe $\overline{(k \cdot s, 0)}$ representa, portanto, um inteiro não-negativo. Se $w \cdot z \geq 0$, então $(y \cdot z) - (x \cdot z) \geq 0$, o que implica $x \cdot z \leq y \cdot z$. A desigualdade é preservada.

- **Caso 2:** $z < 0$ **(Multiplicador negativo)**
  Temos $w \geq 0$ e $z < 0$. Novamente, $w = \overline{(k,0)}$ para $k \in \mathbb{N}$. Como z é negativo, ele pode ser representado pela classe $\overline{(0,s)}$ para algum $s \in \mathbb{N}^*$. Calculando o produto:

$$w \cdot z = \overline{(k,0)} \cdot \overline{(0,s)} = \overline{(k \cdot 0 + 0 \cdot s, k \cdot s + 0 \cdot 0)} = \overline{(0, k \cdot s)}$$

  Como $k \cdot s$ é um número natural, a classe $\overline{(0, k \cdot s)}$ representa um inteiro não-positivo. Se $w \cdot z \leq 0$, então $(y \cdot z) - (x \cdot z) \leq 0$, o que implica $x \cdot z \geq y \cdot z$. A desigualdade é invertida.

- **Caso 3:** $z = 0$
  Se $z = 0$, então o produto de qualquer inteiro por z é zero. Logo, $x \cdot z = 0$ e $y \cdot z = 0$.

□

2.6 Congruência Módulo m

No capítulo anterior, ao estudarmos as relações de equivalência, vimos um exemplo prático com a noção de paridade. A relação de paridade divide o conjunto dos números naturais (e, por extensão, o dos inteiros) em duas classes: os pares e os ímpares. Esta seção generaliza essa ideia. Em vez de apenas classificar os números com base em sua relação com o número 2, a congruência modular nos permite classificá-los com base em sua relação com um inteiro arbitrário m. Mas antes, precisamos compreender alguns conceitos importantes:

Definição 2.6.1 (Módulo ou Valor Absoluto de um Inteiro)**.** Seja $z \in \mathbb{Z}$. O **módulo** ou **valor absoluto** de z, denotado por $|z|$, é o número natural definido da seguinte forma:

$$|z| = \begin{cases} z, & \text{se } z \geq 0 \\ -z, & \text{se } z < 0 \end{cases}$$

Exemplo 2.6.1.

- $|5|$**:** Como $5 \geq 0$, $|5| = 5$.

- $|-8|$**:** Como $-8 < 0$, $|-8| = -(-8) = 8$.
- $|0|$**:** Como $0 \geq 0$, $|0| = 0$.

Definição 2.6.2 (Divisibilidade em $\mathbb{Z}$)**.** Sejam $d, z \in \mathbb{Z}$, com $d \neq 0$. Dizemos que d **divide** z, e escrevemos $d \mid z$, se existe um inteiro $k \in \mathbb{Z}$ tal que:

$$z = d \cdot k$$

Se não existe tal inteiro k, dizemos que d **não divide** z, e escrevemos $d \nmid z$. A principal diferença em relação à divisibilidade em $\mathbb{N}$ é que os divisores de um inteiro sempre aparecem em pares. Se d é um divisor de z, então $-d$ também é.

Exemplo 2.6.2.

- $4 \mid 12$, pois $12 = 4 \cdot 3$.
- $-5 \mid 30$, pois $30 = (-5) \cdot (-6)$.
- $-8 \mid -40$, pois $-40 = (-8) \cdot 5$.
- $3 \nmid 10$, pois não existe um inteiro k tal que $10 = 3 \cdot k$.
- Para qualquer $d \in \mathbb{Z}$ com $d \neq 0$, temos que $d \mid 0$, pois $0 = d \cdot 0$.

Definição 2.6.3 (Máximo Divisor Comum em $\mathbb{Z}$)**.** Sejam $a, b \in \mathbb{Z}$, não ambos nulos. O **Máximo Divisor Comum** de a e b, denotado por $\text{mdc}(a, b)$, é o maior inteiro positivo d que satisfaz as seguintes condições:

- $d \mid a$ e $d \mid b$ (d é um divisor comum).
- Se $c \in \mathbb{Z}$ é qualquer outro divisor comum (i.e., $c \mid a$ e $c \mid b$), então $c \mid d$.

A condição de que $c \mid d$ é equivalente à ideia intuitiva de que d é o maior divisor comum. Como d é um inteiro positivo e c é um divisor (seja c positivo ou negativo), a relação $c \mid d$ implica $|c| \leq d$. Assim, d é, de fato, o maior divisor comum.

Teorema 2.6.1 (Identidade de Bèzout)**.** Sejam $a, b \in \mathbb{Z}$, não nulos ao mesmo tempo (i.e. $a = 0 \implies b \neq 0$ e $b = 0 \implies a \neq 0$) e seja $d = \text{mdc}(a, b)$. Então, existem inteiros $x, y \in \mathbb{Z}$ tais que:

$$ax + by = d$$

Demonstração. A prova se baseia no Princípio da Boa Ordem e no Algoritmo da Divisão. Consideremos o conjunto S de todas as combinações inteiras de a e b que resultam em um número positivo:

$$S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$$

S **é não-vazio**

Como a e b não são ambos nulos, suponha $a \neq 0$. O conjunto S contém $a \cdot 1 + b \cdot 0 = a$ ou $a \cdot (-1) + b \cdot 0 = -a$. Como $a \neq 0$, seu módulo $|a|$ é positivo, e $|a|$ é igual a a ou $-a$. Portanto, $|a| \in S$, e S é não-vazio. (Um argumento análogo vale se $b \neq 0$).

S **possui um menor elemento**

Como S é um subconjunto não-vazio de inteiros positivos (logo, um subconjunto não-vazio de $\mathbb{N}$), pelo Princípio da Boa Ordem, S deve possuir um menor elemento. Seja d este menor elemento. Por pertencer a S, d deve ter a forma $d = ax + by$ para alguns $x, y \in \mathbb{Z}$.

$d =$ **mdc**(a, b)

Devemos provar que d satisfaz as duas condições da definição de Máximo Divisor Comum (MDC).

- d **é um divisor comum:** Pelo Algoritmo da Divisão, podemos dividir a por d:

$$a = dq + r, \quad \text{com } 0 \leq r < d$$

  Agora, isolamos o resto r e substituímos a expressão de d:

$$r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq)$$

  Esta equação mostra que r também é uma combinação de a e b. Se $r > 0$, então r pertenceria a S. Mas como $r < d$, isso contradiria a definição de d como o *menor* elemento de S. Portanto, a única possibilidade é que $r = 0$. Se $r = 0$, então $a = dq$, o que significa que $d \mid a$. Um argumento idêntico, dividindo b por d, mostra que $d \mid b$. Logo, d é um divisor comum de a e b.

- **Qualquer divisor comum de a e b, também é divisor de d:** Seja c qualquer outro divisor comum de a e b. Então $c \mid a$ e $c \mid b$. Por definição, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = ck_1$ e $b = ck_2$. Substituindo na equação de d:

$$d = ax + by = (ck_1)x + (ck_2)y = c(k_1x + k_2y)$$

  Como $k_1x + k_2y$ é um inteiro, esta equação mostra que $c \mid d$. Como c divide d, e ambos são positivos, devemos ter $c \leq d$.

Provamos que d é um divisor comum maior ou igual a qualquer outro divisor comum. Portanto, $d = \text{mdc}(a, b)$, e como $d \in S$, ele pode ser escrito como $ax + by$. □

Corolário 2.6.1.1. Se $a, b \in \mathbb{Z}$ são primos entre si (i.e., $\text{mdc}(a, b) = 1$), então existem

inteiros $x, y \in \mathbb{Z}$ tais que:

$$ax + by = 1$$

Teorema 2.6.2 (Algoritmo da Divisão nos Inteiros)**.** Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = bq + r \quad \text{com} \quad 0 \leq r < |b|.$$

Demonstração. A prova é dividida em duas partes:

Existência

Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Vamos considerar o conjunto S de todos os inteiros não-negativos da forma $a - bk$:

$$S = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\}.$$

Primeiro, devemos mostrar que S não é vazio. Se $b > 0$, podemos tomar $k = -|a|$. Então $a - b(-|a|) = a + b|a|$. Como $b \geq 1$, este valor é sempre não-negativo. Se $b < 0$, podemos tomar $k = |a|$, de onde segue que $a - b|a|$. Como $b < 0$, o termo $-b|a|$ é positivo, garantindo que a soma seja não-negativa para um k suficientemente grande. Portanto, $S \neq \emptyset$.

Pelo Princípio da Boa Ordem, como S é um subconjunto não-vazio de números naturais (inteiros não-negativos), ele deve possuir um menor elemento. Vamos chamar esse elemento de r. Por pertencer a S, r satisfaz duas condições:

1. $r \geq 0$.
2. Existe um inteiro q tal que $r = a - bq$. Esta equação pode ser reescrita como $a = bq + r$.

Com isso, já temos q e r. Resta apenas mostrar que r satisfaz a condição $r < |b|$.

Faremos isso por contradição. Suponha que $r \geq |b|$. Se $r \geq |b|$, então a diferença $r - |b|$ é um número não-negativo:

$$r - |b| \geq 0.$$

Vamos chamar este novo número de r'. Precisamos mostrar que r' também pertence a S. Para isso, ele deve ter a forma $a - bk$ para algum inteiro k. Analisemos os dois casos para b:

- **Caso 1:** $b > 0$. Temos $|b| = b$.

$$r' = r - |b| = (a - bq) - b = a - b(q + 1)$$

O número r' tem a forma $a - bk$ (com $k = q + 1$) e $r' \geq 0$, logo $r' \in S$.

- **Caso 2:** $b < 0$. Temos $|b| = -b$.

$$r' = r - |b| = (a - bq) - (-b) = a - bq + b = a - b(q - 1)$$

O número r' tem a forma $a - bk$ (com $k = q - 1$) e $r' \geq 0$, logo $r' \in S$.

Em ambos os casos, mostramos que, se $r \geq |b|$, então existe um elemento $r' \in S$. Agora, vamos comparar r' e r. Por definição, $r' = r - |b|$. Como $b \neq 0$, sabemos que $|b| > 0$. Portanto,

$$r' = r - |b| < r.$$

Isso nos leva a uma contradição: encontramos um elemento $r' \in S$ que é estritamente menor que r, mas r era, por definição, o menor elemento de S.

A contradição surgiu da nossa suposição de que $r \geq |b|$. Portanto, a suposição deve ser falsa, e a única possibilidade restante é que $r < |b|$. Isso garante a existência de q e r que satisfazem todas as condições do teorema.

Unicidade

Para provar que o quociente q e o resto r são únicos, suponha que existam duas representações para o mesmo inteiro a:

$$a = bq + r, \quad \text{com } 0 \leq r < |b|$$
$$a = bq' + r', \quad \text{com } 0 \leq r' < |b|$$

onde q, r, q', r' são inteiros.

Igualando as duas expressões para a, obtemos:

$$bq + r = bq' + r'$$

Rearranjando a equação para isolar os termos com b e os restos, temos:

$$bq - bq' = r' - r \implies b(q - q') = r' - r$$

A partir desta igualdade, a definição de divisibilidade nos diz que b divide a diferença dos restos, ou seja, $b \mid (r' - r)$.

Agora, vamos analisar o intervalo em que a diferença $r' - r$ pode estar. Das condições do teorema, sabemos que:

- $0 \leq r' < |b|$
- $0 \leq r < |b|$, o que implica $-|b| < -r \leq 0$.

Somando essas duas desigualdades, obtemos os limites para a diferença $r' - r$:

$$0 - |b| < r' - r < |b| + 0 \implies -|b| < r' - r < |b|$$

Temos então duas condições sobre o número inteiro $r' - r$:

1. Ele é um múltiplo de b.
2. O seu valor absoluto é estritamente menor que $|b|$, ou seja, $|r' - r| < |b|$.

O único múltiplo de um número não-nulo b que satisfaz a condição $|r' - r| < |b|$ é o zero. Todos os outros múltiplos de b (como $b, -b, 2b, -2b, \dots$) têm um valor absoluto igual ou maior que $|b|$.

Dessa forma, a única possibilidade é que a diferença seja zero:

$$r' - r = 0 \implies r' = r$$

Com a igualdade dos restos estabelecida, podemos substituir este resultado na equação $b(q - q') = r' - r$:

$$b(q - q') = 0$$

Como, por hipótese, o divisor b não é nulo ($b \neq 0$), a única forma de este produto ser zero é se o outro fator for zero. Logo:

$$q - q' = 0 \implies q' = q$$

Como demonstramos que $r = r'$ e $q = q'$, provamos que o quociente e o resto são únicos. □

Definição 2.6.4 (Congruência Módulo m)**.** Sejam $a, b, m \in \mathbb{Z}$, com $m > 0$. Dizemos que a é **congruente** a b **módulo** m, e escrevemos:

$$a \equiv b \pmod{m}$$

se, e somente se, m divide a diferença entre a e b. Ou seja:

$$a \equiv b \pmod{m} \iff m|(a - b)$$

Quando a relação $a \equiv b \pmod{m}$ é verdadeira, dizemos que a e b são congruentes módulo m. Se m não divide $a - b$, dizemos que a é incongruente a b módulo m, e escrevemos $a \not\equiv b \pmod{m}$.

Exemplo 2.6.3.

- $17 \equiv 2 \pmod 5$ é uma afirmação verdadeira, pois a diferença $17-2 = 15$, e sabemos que 5 divide 15 (pois $15 = 5 \cdot 3$).
- $-8 \equiv 2 \pmod 5$ também é uma afirmação verdadeira, pois a diferença $-8 - 2 = -10$, e 5 divide -10 (pois $-10 = 5 \cdot (-2)$).
- $10 \not\equiv 2 \pmod 3$ é uma afirmação verdadeira. A diferença é $10 - 2 = 8$, e como não existe um inteiro k tal que $3 \cdot k = 8$, 3 não divide 8.
- A relação de paridade é um caso de congruência módulo 2. Um número n é par se $n \equiv 0 \pmod 2$ e é ímpar se $n \equiv 1 \pmod 2$.

Proposição 2.6.1. A relação de congruência módulo m é uma relação de equivalência sobre o conjunto dos números inteiros $\mathbb{Z}$.

Demonstração. Para demonstrar esta proposição, devemos verificar as três propriedades de uma relação de equivalência: reflexividade, simetria e transitividade.

Reflexividade ($a \equiv a \pmod m$)

Para qualquer inteiro a, a diferença $a - a = 0$. Sabemos que todo inteiro não nulo m divide 0, pois existe o inteiro 0 tal que $m \cdot 0 = 0$. Portanto, $m|(a - a)$, o que significa que $a \equiv a \pmod m$. A relação é reflexiva.

Simetria ($a \equiv b \pmod m \implies b \equiv a \pmod m$)

Suponha que $a \equiv b \pmod m$. Pela definição, isso significa que $m|(a - b)$. Se m divide $a - b$, então existe um inteiro k tal que $a - b = m \cdot k$. Multiplicando a equação por -1, obtemos:

$$-(a - b) = -(m \cdot k) \implies b - a = m \cdot (-k)$$

Como k é um inteiro, $-k$ também é um inteiro. A existência de um inteiro $-k$ que satisfaz a equação acima significa, por definição, que $m|(b-a)$. Portanto, $b \equiv a \pmod m$. A relação é simétrica.

Transitividade ($a \equiv b \pmod m \wedge b \equiv c \pmod m \implies a \equiv c \pmod m$)

Suponha que $a \equiv b \pmod m$ e $b \equiv c \pmod m$. Isso nos fornece duas condições:

1. $m|(a - b)$, o que implica que existe um inteiro k_1 tal que $a - b = m \cdot k_1$.
2. $m|(b - c)$, o que implica que existe um inteiro k_2 tal que $b - c = m \cdot k_2$.

Somando as duas equações, obtemos:

$$(a - b) + (b - c) = (m \cdot k_1) + (m \cdot k_2)$$

Simplificando o lado esquerdo e fatorando m no lado direito:

$$a - c = m \cdot (k_1 + k_2)$$

Como k_1 e k_2 são inteiros, sua soma $k_1 + k_2$ também é um inteiro. A existência deste inteiro significa que $m|(a - c)$. Portanto, $a \equiv c \pmod{m}$. A relação é transitiva.

Como a congruência módulo m é reflexiva, simétrica e transitiva, ela é uma relação de equivalência. □

2.6.1 Classes de Congruência e o Conjunto $\mathbb{Z}_m$

Como a congruência módulo m é uma relação de equivalência, ela particiona o conjunto dos inteiros $\mathbb{Z}$ em subconjuntos disjuntos, que são as suas classes de equivalência. Neste contexto, estas são chamadas de **classes de congruência módulo** m. A classe de um inteiro a é o conjunto de todos os inteiros que são congruentes a ele:

$$[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

O conjunto de todas as classes de congruência módulo m é denotado por $\mathbb{Z}_m$ (lê-se "Z módulo m"ou "Z m").

Proposição 2.6.2 (Caracterização das Classes por Restos)**.** Dois inteiros a e b são congruentes módulo m se, e somente se, eles deixam o mesmo resto quando divididos por m.

Demonstração. Pelo Algoritmo da Divisão para inteiros, podemos escrever a e b de forma única como: $a = m \cdot q_1 + r_1$ e $b = m \cdot q_2 + r_2$, onde q_1, q_2 são os quocientes e $0 \leq r_1, r_2 < m$ são os restos.

($\Rightarrow$) Suponha que $a \equiv b \pmod{m}$. Isso significa que $m \mid (a - b)$, então $a - b = m \cdot k$ para algum $k \in \mathbb{Z}$. Substituindo as expressões acima:

$$(m \cdot q_1 + r_1) - (m \cdot q_2 + r_2) = m \cdot k$$

$$m(q_1 - q_2) + (r_1 - r_2) = m \cdot k$$

$$r_1 - r_2 = m \cdot k - m(q_1 - q_2) = m \cdot (k - q_1 + q_2)$$

Isso mostra que $m \mid (r_1 - r_2)$. Como os restos r_1 e r_2 satisfazem $0 \leq r_1 < m$ e $0 \leq r_2 < m$, a diferença entre eles satisfaz $-m < r_1 - r_2 < m$. O único múltiplo de m neste intervalo é o zero. Portanto, $r_1 - r_2 = 0$, o que implica $r_1 = r_2$.

($\Leftarrow$) Suponha que a e b têm o mesmo resto r. Então $a = m \cdot q_1 + r$ e $b = m \cdot q_2 + r$. A diferença é $a - b = (m \cdot q_1 + r) - (m \cdot q_2 + r) = m(q_1 - q_2)$. Isso mostra que $m \mid (a - b)$, e

portanto, $a \equiv b \pmod{m}$. □

Esta proposição é extremamente útil. Ela nos diz que todos os elementos em uma classe de congruência compartilham o mesmo resto na divisão por m. Como os únicos restos possíveis na divisão por m são $0, 1, 2, \ldots, m-1$, existem exatamente m classes de congruência distintas.

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}$$

2.6.2 Operações em $\mathbb{Z}_m$

Podemos definir operações de adição e multiplicação diretamente sobre as classes de congruência.

Definição 2.6.5 (Operações em $\mathbb{Z}_m$)**.** Sejam $[a]_m, [b]_m \in \mathbb{Z}_m$. Definimos:

- **Adição:** $[a]_m + [b]_m := [a+b]_m$
- **Multiplicação:** $[a]_m \cdot [b]_m := [a \cdot b]_m$

Em outras palavras, para somar ou multiplicar duas classes, somamos ou multiplicamos seus representantes (quaisquer elementos das classes) e encontramos a classe do resultado. Para que esta definição seja válida, precisamos provar que o resultado não depende dos representantes escolhidos.

Proposição 2.6.3. As operações de adição e multiplicação em $\mathbb{Z}_m$ são bem-definidas.

Demonstração. Seja $[a]_m = [a']_m$ e $[b]_m = [b']_m$. Isso significa que $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$. Logo, existem inteiros k_1, k_2 tais que $a - a' = m \cdot k_1$ e $b - b' = m \cdot k_2$.

Adição: Devemos mostrar que $[a+b]_m = [a'+b']_m$. A diferença $(a+b) - (a'+b') = (a-a') + (b-b') = m \cdot k_1 + m \cdot k_2 = m(k_1 + k_2)$. Como $m \mid ((a+b) - (a'+b'))$, temos que $a + b \equiv a' + b' \pmod{m}$, e a adição é bem-definida.

Multiplicação: Devemos mostrar que $[a \cdot b]_m = [a' \cdot b']_m$. A diferença $a \cdot b - a' \cdot b'$ pode ser reescrita como:

$$a \cdot b - a \cdot b' + a \cdot b' - a' \cdot b' = a(b - b') + b'(a - a')$$

Substituindo as expressões da hipótese:

$$a(m \cdot k_2) + b'(m \cdot k_1) = m \cdot (a \cdot k_2 + b' \cdot k_1)$$

Como $m \mid (a \cdot b - a' \cdot b')$, temos que $a \cdot b \equiv a' \cdot b' \pmod{m}$, e a multiplicação é bem-definida.

□

2.7 A Estrutura de Grupo em $\mathbb{Z}$

De forma análoga à análise feita para os números naturais, podemos agora examinar as estruturas algébricas formadas pelo conjunto dos inteiros $\mathbb{Z}$ com as operações de adição e multiplicação. Como já foi demonstrado, a adição e a multiplicação em $\mathbb{Z}$ são associativas e ambas possuem um elemento identidade (o 0 para a adição e o 1 para a multiplicação). Portanto, tanto $(\mathbb{Z}, +, 0)$ quanto $(\mathbb{Z}, \cdot, 1)$ são monoides. A questão que surge naturalmente é se com as novas propriedades dos inteiros conseguimos construir novas estruturas que eram inviáveis com os naturais.

Definição 2.7.1 (Grupo)**.** Um **grupo** é um monoide $(G, *)$ no qual todo elemento possui um inverso (ou elemento simétrico). Mais formalmente, $(G, *)$ é um grupo se satisfaz os seguintes axiomas:

1. **Associatividade:** A operação $*$ é associativa.

$$\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$$

2. **Elemento Identidade:** Existe um elemento identidade $e \in G$ tal que:

$$\forall a \in G, \quad a * e = e * a = a$$

3. **Elemento Inverso (ou simétrico):** Para cada elemento $a \in G$, existe um elemento $a' \in G$, chamado de inverso de a, tal que:

$$a * a' = e$$

Adicionalmente, se um grupo também satisfaz a propriedade comutativa ($a * b = b * a$), ele é chamado de **Grupo Comutativo ou Abeliano**.

A estrutura dos números inteiros com a adição, $(\mathbb{Z}, +)$, é um **grupo abeliano**. As propriedades necessárias para esta classificação já foram demonstradas: a operação é associativa e comutativa, o número 0 atua como elemento identidade e, fundamentalmente, foi provado que para cada inteiro x existe um elemento inverso aditivo, $-x$. Como todos os axiomas são satisfeitos, $(\mathbb{Z}, +, 0)$ é um grupo abeliano.

O monoide da multiplicação de inteiros, $(\mathbb{Z}, \cdot)$, **não é** um grupo. A estrutura falha no axioma do elemento inverso. Por exemplo, para o inteiro 2, não existe um inteiro k tal que $2 \cdot k = 1$. A ausência de inversos multiplicativos para a maioria dos elementos impede que $(\mathbb{Z}, \cdot)$ seja um grupo.

Exemplo 2.7.1. O conjunto $\mathbb{Z} \times \mathbb{Z}$, formado por todos os pares ordenados de inteiros (a, b), com a operação de adição definida componente a componente, forma um **grupo**

abeliano. A operação é definida como:

$$\forall (a,b),(c,d) \in \mathbb{Z} \times \mathbb{Z}, \quad (a,b) + (c,d) := (a+c, b+d)$$

A verificação das propriedades se baseia nas propriedades já conhecidas do grupo $(\mathbb{Z}, +)$:

1. **Associatividade:** A operação é associativa, pois a adição em $\mathbb{Z}$ o é. $((a+c)+e, (b+d)+f) = (a+(c+e), b+(d+f))$.
2. **Elemento Identidade:** O par $(0,0)$ é o elemento identidade, pois $(a,b)+(0,0) = (a+0, b+0) = (a,b)$.
3. **Elemento Inverso:** Para cada elemento (a,b), existe um inverso $(-a,-b) \in \mathbb{Z} \times \mathbb{Z}$, pois $(a,b)+(-a,-b) = (a-a, b-b) = (0,0)$.
4. **Comutatividade:** A operação é comutativa, pois a adição em $\mathbb{Z}$ o é. $(a+c, b+d) = (c+a, d+b)$.

Proposição 2.7.1 (Unicidade do Elemento Inverso)**.** Seja $(G, *)$ um grupo. Para cada elemento $a \in G$, seu elemento inverso é único.

Demonstração. Para provar a unicidade, seja a um elemento arbitrário de G. Suponha que a' e a'' sejam ambos elementos inversos de a. Por definição de inverso, eles devem satisfazer:

1. $a * a' = a' * a = e$
2. $a * a'' = a'' * a = e$

Nosso objetivo é mostrar que, necessariamente, $a' = a''$. Vamos começar com a' e usar as propriedades de grupo (identidade, associatividade e as hipóteses acima):

$$\begin{aligned}
a' &= a' * e && \text{(Propriedade do elemento identidade } e\text{)} \\
&= a' * (a * a'') && \text{(Substituindo } e \text{ pela hipótese 2)} \\
&= (a' * a) * a'' && \text{(Associatividade da operação } *\text{)} \\
&= e * a'' && \text{(Substituindo pela hipótese 1)} \\
&= a'' && \text{(Propriedade do elemento identidade } e\text{)}
\end{aligned}$$

A cadeia de igualdades $a' = a''$ nos força a concluir que os dois supostos inversos são, na verdade, o mesmo elemento.

Portanto, o inverso de qualquer elemento $a \in G$ é único.

□

Note que esta demonstração é, em essência, a mesma utilizada para provar a unicidade do inverso aditivo em $(\mathbb{Z}, +)$, o que ilustra como os axiomas de grupo generalizam as propriedades observadas nos inteiros.

Proposição 2.7.2 (Inverso do Inverso)**.** Seja $(G, *)$ um grupo com elemento identidade e. Para qualquer elemento $a \in G$, o inverso do inverso de a é o próprio a. Denotando o inverso de a por a', temos:

$$(a')' = a$$

Demonstração. Seja $a \in G$. Por definição de grupo, existe um $a' \in G$ tal que:

$$a * a' = e \quad \text{e} \quad a' * a = e$$

Agora, considere o elemento a'. Como a' também pertence a G, ele também deve possuir um inverso, que denotamos por $(a')'$. Por definição, este inverso $(a')'$ satisfaz:

$$a' * (a')' = e \quad \text{e} \quad (a')' * a' = e$$

Nosso objetivo é mostrar que $(a')' = a$.

Considere a equação da definição do inverso de a:

$$a' * a = e$$

Agora, considere a equação da definição do inverso de a':

$$a' * (a')' = e$$

Juntando as duas expressões:

$$a' * a = a' * (a')'$$

Operando à esquerda em ambos os lados da equação com a:

$$a * (a' * a) = a * (a' * (a')')$$

Pela associatividade:

$$(a * a') * a = (a * a') * (a')'$$

Usando $a * a' = e$:

$$e * a = e * (a')'$$

Pela propriedade da identidade:

$$a = (a')'$$

Isso prova que o inverso do inverso de a é o próprio a. □

Definição 2.7.2 (Subgrupo)**.** Seja $(G, *)$ um grupo e seja H um subconjunto não vazio de G ($H \subseteq G, H \neq \emptyset$). Dizemos que H é um **subgrupo** de G se H, munido da mesma operação $*$ restrita a seus elementos, também forma um grupo.

Verificar todos os axiomas de grupo para cada subconjunto pode ser trabalhoso. Felizmente, existe um critério mais simples. Como a associatividade é uma propriedade da operação em G, ela será automaticamente herdada por qualquer subconjunto de G. Portanto, precisamos apenas garantir o fechamento da operação, a existência do elemento identidade dentro do subconjunto e a presença do inverso de cada elemento.

Proposição 2.7.3. Um subconjunto não vazio H de um grupo $(G, *)$ é um subgrupo de G se, e somente se, as duas seguintes condições são satisfeitas:

1. **Fechamento sob a operação:** Para quaisquer $a, b \in H$, o resultado $a * b$ também pertence a H.
$$\forall a, b \in H, \quad a * b \in H$$

2. **Fechamento sob inversos:** Para todo elemento $a \in H$, seu inverso a' também pertence a H.
$$\forall a \in H, \quad a' \in H$$

Demonstração. A demonstração exige provar a implicação em ambos os sentidos.

($\Rightarrow$) Suponha que H é um subgrupo de G. Por definição, $(H, *)$ é um grupo. A definição de grupo exige que $*$ seja uma operação binária em H, o que implica diretamente que a operação é fechada (condição 1). A definição de grupo também exige que todo elemento em H possua um inverso que também esteja em H (condição 2). Portanto, se H é um subgrupo, as duas condições são necessariamente satisfeitas.

($\Leftarrow$) Agora, suponha que H é um subconjunto não vazio de G que satisfaz as duas condições. Devemos provar que $(H, *)$ é um grupo, verificando os três axiomas de grupo.

- **Associatividade:** A operação $*$ é associativa para todos os elementos de G. Como H é um subconjunto de G, a operação continua sendo associativa para todos os elementos de H. A propriedade é herdada diretamente.

- **Elemento Inverso:** A existência do inverso para cada elemento de H que também pertence a H é garantida diretamente pela nossa segunda hipótese.

- **Elemento Identidade:** Devemos provar que o elemento identidade e de G pertence a H.

  - Como H é não vazio, podemos tomar um elemento qualquer $a \in H$.
  - Pela nossa segunda hipótese (fechamento sob inversos), se $a \in H$, então seu inverso a' também deve estar em H.

- Agora temos dois elementos em H: a e a'. Pela nossa primeira hipótese (fechamento sob a operação), o resultado de $a * a'$ deve pertencer a H.
- Como G é um grupo, sabemos que $a * a' = e$.
- Portanto, concluímos que o elemento identidade e de G está em H.

Como a operação é associativa em H, H contém o elemento identidade e todo elemento de H tem um inverso em H, e, pela hipótese 1, a operação é fechada, concluímos que $(H, *)$ satisfaz todos os requisitos para ser um grupo. Logo, H é um subgrupo de G. □

Proposição 2.7.4 (Critério para Subgrupo em Um Único Passo)**.** Seja $(G, *)$ um grupo e H um subconjunto não vazio de G. Então, H é um subgrupo de G se, e somente se, para quaisquer $a, b \in H$, o elemento $a * b'$ (onde b' é o inverso de b) também pertence a H.

$$\forall a, b \in H, \quad a * b' \in H$$

Para grupos cuja operação é a adição, como $(\mathbb{Z}, +)$, o inverso de b é $-b$. Assim, a condição se torna: para quaisquer $a, b \in H$, a diferença $a - b$ também pertence a H.

Demonstração. Novamente, a prova exige a demonstração da equivalência, analisando os dois sentidos da implicação.

(⇒) Suponha que H seja um subgrupo de G. Devemos mostrar que a condição é satisfeita. Sejam a e b dois elementos quaisquer de H. Como H é um grupo, ele é fechado sob a tomada de inversos. Portanto, se $b \in H$, seu inverso b' também deve pertencer a H. Agora, temos dois elementos em H: o elemento a e o elemento b'. Como H é um grupo, ele também é fechado sob a operação $*$. Logo, o resultado da operação $a * b'$ deve, necessariamente, pertencer a H. Assim, a condição é satisfeita.

(⇐) Suponha que H é um subconjunto não vazio de G que satisfaz a condição de que $\forall a, b \in H, \quad a * b' \in H$. Para provar que H é um subgrupo, podemos demonstrar que esta única condição implica as duas condições do critério anterior (fechamento sob a operação e fechamento sob inversos).

1. **Existência do Elemento Identidade em H:** Como H é não vazio, existe pelo menos um elemento $x \in H$. Podemos aplicar a nossa hipótese usando este elemento para ambos a e b. Ou seja, façamos $a = x$ e $b = x$. A condição nos diz que $a * b' \in H$, o que se torna $x * x' \in H$. Pela definição de grupo, sabemos que $x * x'$ é o elemento identidade, e. Portanto, $e \in H$.

2. **Fechamento sob Inversos:** Agora que sabemos que $e \in H$, podemos usar este fato. Seja b um elemento qualquer de H. Queremos mostrar que seu inverso, b', também está em H. Podemos aplicar a nossa hipótese usando $a = e$ e o elemento b. A condição nos diz que $a * b' \in H$, o que se torna $e * b' \in H$. Pela propriedade do

elemento identidade, sabemos que $e * b' = b'$. Portanto, $b' \in H$. Isso prova que H é fechado sob a tomada de inversos.

3. **Fechamento sob a Operação:** Sejam a e b dois elementos quaisquer de H. Queremos mostrar que $a * b \in H$. Já provamos que se $b \in H$, então seu inverso b' também está em H. A nossa hipótese pode ser aplicada a quaisquer dois elementos de H. Vamos aplicá-la aos elementos a e b'. A condição nos diz que $a * (b')' \in H$. Como o inverso do inverso de um elemento é o próprio elemento, $(b')' = b$. Substituindo, temos que $a * b \in H$. Isso prova que H é fechado sob a operação $*$.

Como a condição única $\forall a, b \in H, a * b' \in H$ implica que H contém a identidade, é fechado sob inversos e é fechado sob a operação, e como a associatividade é herdada de G, concluímos que H é um subgrupo de G. □

Exemplo 2.7.2. Para qualquer inteiro $n > 1$, o conjunto dos múltiplos de n, denotado por $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, é um subgrupo do grupo dos inteiros com a adição, $(\mathbb{Z}, +)$. Por exemplo, o conjunto dos números pares $2\mathbb{Z} = \{..., -4, -2, 0, 2, 4, ...\}$ é um subgrupo de $\mathbb{Z}$.

Demonstração. Para provar que $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$ para qualquer inteiro $n > 1$, devemos verificar que $n\mathbb{Z}$ é um subconjunto não vazio de $\mathbb{Z}$ e que satisfaz as duas condições de fechamento (para a operação e para os inversos).

Primeiro, notamos que $n\mathbb{Z}$ não é vazio, pois o elemento identidade da adição, 0, pertence a $n\mathbb{Z}$, uma vez que pode ser escrito como $0 = n \cdot 0$.

Fechamento sob a Adição:

Devemos mostrar que, para quaisquer dois elementos em $n\mathbb{Z}$, a sua soma também está em $n\mathbb{Z}$. Sejam a e b dois elementos arbitrários de $n\mathbb{Z}$. Pela definição de $n\mathbb{Z}$, existem inteiros k_1 e k_2 tais que:

$$a = n \cdot k_1 \quad \text{e} \quad b = n \cdot k_2$$

A soma deles é:

$$a + b = (n \cdot k_1) + (n \cdot k_2)$$

Usando a propriedade distributiva da multiplicação sobre a adição, que é válida em $\mathbb{Z}$:

$$a + b = n \cdot (k_1 + k_2)$$

Seja $k_3 = k_1 + k_2$. Como k_1 e k_2 são inteiros, a sua soma k_3 também é um inteiro. A expressão $n \cdot k_3$ tem a forma de um múltiplo de n, o que, por definição, significa que o resultado $a + b$ pertence a $n\mathbb{Z}$. Portanto, $n\mathbb{Z}$ é fechado sob a adição.

Fechamento sob Inversos Aditivos:
Devemos mostrar que, para todo elemento em $n\mathbb{Z}$, seu inverso aditivo também está em $n\mathbb{Z}$. Seja a um elemento arbitrário de $n\mathbb{Z}$. Logo, existe um inteiro k tal que:

$$a = n \cdot k$$

O inverso aditivo de a é $-a$. Podemos escrevê-lo como:

$$-a = -(n \cdot k) = n \cdot (-k)$$

Seja $k' = -k$. Como k é um inteiro, k' também é um inteiro. A expressão $n \cdot k'$ tem a forma de um múltiplo de n, o que significa que $-a$ pertence a $n\mathbb{Z}$. Portanto, $n\mathbb{Z}$ é fechado sob inversos aditivos.

Como $n\mathbb{Z}$ é um subconjunto não vazio de $\mathbb{Z}$ e ambas as condições foram satisfeitas, concluímos que $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$. □

Proposição 2.7.5. Todo subgrupo H do grupo aditivo dos inteiros $(\mathbb{Z}, +)$ é da forma $n\mathbb{Z}$ para algum inteiro não-negativo $n \in \mathbb{N}$.

Demonstração. Seja H um subgrupo qualquer de $(\mathbb{Z}, +)$. Temos dois casos a considerar:

Caso 1: $H = \{0\}$. Neste caso, o subgrupo contém apenas o elemento identidade. Escolhendo $n = 0$, temos $0\mathbb{Z} = \{0 \cdot k \mid k \in \mathbb{Z}\} = \{0\}$. Portanto, $H = 0\mathbb{Z}$, que é da forma $n\mathbb{Z}$ com $n = 0$.

Caso 2: H **contém elementos não nulos**. Se $H \neq \{0\}$, então existe pelo menos um elemento $h \in H$ tal que $h \neq 0$. Como H é um subgrupo, ele é fechado sob inversos, então $-h$ também pertence a H. Um dos dois, h ou $-h$, deve ser positivo. Portanto, o conjunto $H^+ = H \cap \mathbb{N}^* = \{x \in H \mid x > 0\}$ é não vazio.

Pelo Princípio da Boa Ordem, como H^+ é um subconjunto não vazio de $\mathbb{N}^*$, ele deve possuir um menor elemento. Seja n este menor elemento positivo pertencente a H.

Agora, devemos provar que H é precisamente o conjunto de todos os múltiplos de n, ou seja, $H = n\mathbb{Z}$. Faremos isso provando as duas inclusões:

- **Prova de que** $n\mathbb{Z} \subseteq H$**:** Como $n \in H$ e H é um subgrupo (portanto fechado sob a adição e inversos):
  - O elemento identidade $0 = n \cdot 0$ está em H.
  - Para qualquer $k \in \mathbb{N}^*$, o elemento $n \cdot k = \underbrace{n + n + \cdots + n}_{k \text{ vezes}}$ deve estar em H pelo fechamento da adição.
  - O inverso de n, que é $-n$, deve estar em H.
  - Para qualquer $k \in \mathbb{N}^*$, o inverso de $n \cdot k$, que é $n \cdot (-k) = \underbrace{(-n) + (-n) + \cdots + (-n)}_{k \text{ vezes}}$, também deve estar em H.

Portanto, todos os múltiplos inteiros de n, $\{nk \mid k \in \mathbb{Z}\}$, pertencem a H. Logo, $n\mathbb{Z} \subseteq H$.

- **Prova de que $H \subseteq n\mathbb{Z}$:** Seja h um elemento arbitrário de H. Podemos aplicar o Algoritmo da Divisão Euclidiana para dividir h por n:

$$h = n \cdot q + r$$

onde $q, r \in \mathbb{Z}$ e $0 \leq r < n$.

Nosso objetivo é mostrar que r deve ser obrigatoriamente 0. Podemos reescrever a equação como $r = h - n \cdot q$.

  - Sabemos que $h \in H$ (por hipótese).
  - Sabemos que $n \in H$. Como H é um subgrupo, $n \cdot q$ (que é uma soma repetida de n ou $-n$) também pertence a H.
  - Como H é fechado sob a operação (adição) e inversos, ele também é fechado sob a subtração (pois $a - b = a + (-b)$). Portanto, $r = h - (n \cdot q)$ deve pertencer a H.

Assim, temos que $r \in H$ e, pela condição do algoritmo da divisão, $0 \leq r < n$.

Lembre-se que n foi definido como o *menor elemento positivo* em H. Como $r \in H$ e $r < n$, a única possibilidade para r não contradizer a minimalidade de n é se r não for positivo. A única opção não-negativa restante é $r = 0$.

Se $r = 0$, a equação da divisão se torna $h = n \cdot q + 0 = n \cdot q$. Isso significa que h é um múltiplo de n, ou seja, $h \in n\mathbb{Z}$. Como h foi escolhido como um elemento arbitrário de H, concluímos que todo elemento de H é um múltiplo de n. Logo, $H \subseteq n\mathbb{Z}$.

Como provamos que $n\mathbb{Z} \subseteq H$ e $H \subseteq n\mathbb{Z}$, concluímos que $H = n\mathbb{Z}$.
Portanto, todo subgrupo de $(\mathbb{Z}, +)$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{N}$. □

2.7.1 Grupos Cíclicos e Geradores

Uma das classes mais importantes e fundamentais de grupos é aquela em que toda a estrutura pode ser construída a partir de um único elemento. Esses são os grupos cíclicos, e o grupo dos inteiros, $(\mathbb{Z}, +)$, é o principal representante dessas estruturas.

Definição 2.7.3 (Subgrupo Gerado por um Elemento)**.** Seja $(G, *)$ um grupo e seja a um elemento de G. O conjunto de todas as potências inteiras de a, denotado por $\langle a \rangle$, é definido como:

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$$

Onde a notação de potência significa:

- Se $k > 0$, $a^k = \underbrace{a * a * \cdots * a}_{k \text{ vezes}}$.
- Se $k = 0$, $a^0 = e$ (o elemento identidade).
- Se $k < 0$, $a^k = (a')^{-k}$, onde a' é o inverso de a.

Este conjunto $\langle a \rangle$ forma um subgrupo de G, conhecido como o **subgrupo cíclico gerado por** a.

Proposição 2.7.6. Seja $(G, *)$ um grupo, $a \in G$ e a' o inverso de a. Para qualquer inteiro $m \in \mathbb{Z}$, a potência m do inverso de a é igual à potência $-m$ de a.

$$(a')^m = a^{-m}$$

Demonstração. Analisamos os casos para o inteiro m:

1. **Caso 1:** $m > 0$**.** Por definição da potência $-m$ (que é negativa), $a^{-m} = (a')^{-(-m)} = (a')^m$. A igualdade é direta da definição.
2. **Caso 2:** $m = 0$**.** $(a')^0 = e$ (identidade). $a^{-0} = a^0 = e$. Portanto, $(a')^0 = a^{-0}$.
3. **Caso 3:** $m < 0$**.** Seja $m = -p$, onde $p = -m > 0$, vamos analisar o que ocorre com $(a')^m = a^{-m}$
   O lado esquerdo é $(a')^m = (a')^{-p}$. Pela definição de potência negativa, $(a')^{-p} = ((a')')^{-(-p)} = ((a')')^p$. Como $(a')' = a$ (inverso do inverso), temos $(a')^m = a^p$.
   O lado direito é $a^{-m} = a^{-(-p)} = a^p$.

   Como ambos os lados são iguais a a^p, a igualdade é válida.

Em todos os casos, a igualdade $(a')^m = a^{-m}$ se verifica. □

Proposição 2.7.7. Seja $(G, *)$ um grupo e $a \in G$. O subgrupo cíclico $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ é o menor subgrupo de G que contém o elemento a.

Demonstração. A demonstração consiste em duas partes: primeiro, provar que $\langle a \rangle$ é de fato um subgrupo de G, e segundo, provar que ele está contido em qualquer outro subgrupo que contenha a.

Parte 1: $\langle a \rangle$ **é um subgrupo de** G**.** Devemos verificar duas condições: que $\langle a \rangle$ é não vazio e que, para quaisquer $x, y \in \langle a \rangle$, o elemento $x * y'$ (onde y' é o inverso de y) também pertence a $\langle a \rangle$.

- **Não Vazio:** Considerando $k = 0$ na definição de $\langle a \rangle$, temos $a^0 = e$, onde e é o elemento identidade de G. Como $e \in \langle a \rangle$, o conjunto não é vazio.

- **Verificação da Condição $x * y' \in \langle a \rangle$:** Sejam x, y dois elementos quaisquer de $\langle a \rangle$. Por definição de $\langle a \rangle$, existem inteiros $k, m \in \mathbb{Z}$ tais que $x = a^k$ e $y = a^m$.

  O inverso de $y = a^m$ é $y' = (a^m)' = a^{-m}$. Como $m \in \mathbb{Z}$, $-m$ também é um inteiro, então y' pertence a $\langle a \rangle$.

  Agora, devemos calcular $x * y'$ e verificar se pertence a $\langle a \rangle$:

  $$x * y' = a^k * a^{-m} = a^{k+(-m)} = a^{k-m}$$

  Como $k \in \mathbb{Z}$ e $m \in \mathbb{Z}$, a diferença $k-m$ também é um inteiro. Portanto, $x * y' \in \langle a \rangle$.

Como $\langle a \rangle$ é um subconjunto não vazio de G que satisfaz a condição $\forall x, y \in \langle a \rangle, x * y' \in \langle a \rangle$, concluímos que $\langle a \rangle$ é um subgrupo de G.

Parte 2: $\langle a \rangle$ é o menor subgrupo contendo a. Seja H um subgrupo qualquer de G tal que $a \in H$. Devemos mostrar que $\langle a \rangle \subseteq H$. Seja x um elemento arbitrário de $\langle a \rangle$. Por definição, $x = a^k$ para algum $k \in \mathbb{Z}$. Analisamos os casos para k:

- **Caso 1: $k > 0$.** $x = a^k = \underbrace{a * a * \cdots * a}_{k \text{ vezes}}$. Como $a \in H$ e H é um subgrupo (portanto, fechado sob a operação $*$), a operação repetida de a consigo mesmo deve resultar em um elemento que também está em H. Logo, $x = a^k \in H$.

- **Caso 2: $k = 0$.** $x = a^0 = e$. Como H é um subgrupo, ele deve conter o elemento identidade e. Logo, $x = e \in H$.

- **Caso 3: $k < 0$.** Seja $k = -m$, onde $m = -k > 0$. Então $x = a^k = a^{-m}$. Por definição, $a^{-m} = (a')^m$, onde a' é o inverso de a. Como $a \in H$ e H é um subgrupo, o inverso a' também deve pertencer a H. Agora, temos $(a')^m = \underbrace{a' * a' * \cdots * a'}_{m \text{ vezes}}$. Pelo fechamento da operação em H, este resultado deve pertencer a H. Logo, $x = a^k \in H$.

Como um elemento arbitrário x de $\langle a \rangle$ demonstrou pertencer a H, concluímos que $\langle a \rangle \subseteq H$.

Visto que $\langle a \rangle$ é um subgrupo de G que contém a, e ele está contido em *qualquer* outro subgrupo H que contenha a, $\langle a \rangle$ é, por definição, o menor subgrupo de G que contém a. □

Notação Aditiva: No contexto de um grupo aditivo como $(\mathbb{Z}, +)$, a notação de potência a^k é substituída pela notação de múltiplo $k \cdot a$. Assim, o subgrupo gerado por a é $\langle a \rangle = \{k \cdot a \mid k \in \mathbb{Z}\}$.

Definição 2.7.4 (Grupo Cíclico e Gerador)**.** Um grupo $(G, *)$ é dito **cíclico** se existe um elemento $a \in G$ que gera o grupo inteiro. Ou seja, se $G = \langle a \rangle$. Tal elemento a é chamado de **gerador** do grupo.

Exemplo 2.7.3 (O Grupo dos Inteiros)**.** O grupo dos inteiros com a adição, $(\mathbb{Z}, +)$, é um grupo cíclico infinito.

- O elemento 1 é um gerador, pois $\langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$.
- O elemento -1 também é um gerador, pois $\langle -1 \rangle = \{k \cdot (-1) \mid k \in \mathbb{Z}\} = \{\ldots, 2, 1, 0, -1, -2, \ldots\} = \mathbb{Z}$.
- Nenhum outro inteiro é gerador de $\mathbb{Z}$. Por exemplo, o subgrupo gerado por 2 é $\langle 2 \rangle = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$, que é o subgrupo dos números pares, e não o conjunto $\mathbb{Z}$ inteiro. Note que o subconjunto dos números impares $(2\mathbb{Z} + 1)$ não é um subgrupo, já que não é fechado para a adição.

De fato, como já foi exemplificado, todo subgrupo de $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{N}$. Portanto, todo subgrupo de $\mathbb{Z}$ é cíclico, gerado por n (e por $-n$).

Exemplo 2.7.4 (Grupos de Inteiros Módulo n)**.** O grupo $(\mathbb{Z}_m, +)$ é um exemplo de grupo cíclico **finito**. Consideremos o grupo $(\mathbb{Z}_4, +) = \{[0], [1], [2], [3]\}$.

- A classe [1] é um gerador. Vejamos as potências (múltiplos) de [1]:

$$\begin{aligned} 1 \cdot [1] &= [1] \\ 2 \cdot [1] &= [1] + [1] = [2] \\ 3 \cdot [1] &= [1] + [1] + [1] = [3] \\ 4 \cdot [1] &= [1] + [1] + [1] + [1] = [4] = [0] \end{aligned}$$

  Como todos os elementos de $\mathbb{Z}_4$ foram gerados, $\langle [1] \rangle = \mathbb{Z}_4$. A classe [3] também é um gerador.

- A classe [2] **não** é um gerador. Seus múltiplos são:

$$\begin{aligned} 1 \cdot [2] &= [2] \\ 2 \cdot [2] &= [2] + [2] = [4] = [0] \\ 3 \cdot [2] &= [2] + [2] + [2] = [6] = [2] \end{aligned}$$

  O subgrupo gerado por [2] é $\langle [2] \rangle = \{[0], [2]\}$, que é um subgrupo próprio de $\mathbb{Z}_4$.

Exemplo 2.7.5 (Um Grupo Não Cíclico: $\mathbb{Z}\times\mathbb{Z}$)**.** Consideremos o grupo $G = \mathbb{Z}\times\mathbb{Z}$, onde os elementos são pares ordenados de inteiros (a, b), e a operação é a adição componente a componente:

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

Já foi demonstrado que $(G, +)$ é um grupo abeliano. O elemento identidade é $(0, 0)$ e o inverso de (a, b) é $(-a, -b)$.

Vamos provar que este grupo **não é cíclico**, ou seja, não existe nenhum elemento $g \in G$ tal que $\langle g\rangle = G$.

Seja $g = (a, b)$ um elemento arbitrário de $\mathbb{Z} \times \mathbb{Z}$. O subgrupo cíclico gerado por g é:

$$\langle g\rangle = \langle (a, b)\rangle = \{k \cdot (a, b) \mid k \in \mathbb{Z}\} = \{(ka, kb) \mid k \in \mathbb{Z}\}$$

Para que G fosse cíclico, deveríamos ter $\langle (a, b)\rangle = \mathbb{Z} \times \mathbb{Z}$ para algum par (a, b). Vamos mostrar que isso é impossível.

- **Caso 1:** $a = 0$ **e** $b = 0$**.** Neste caso, $g = (0, 0)$. O subgrupo gerado é $\langle (0, 0)\rangle = \{(k \cdot 0, k \cdot 0) \mid k \in \mathbb{Z}\} = \{(0, 0)\}$. Este é o subgrupo trivial, que claramente não é todo o $\mathbb{Z} \times \mathbb{Z}$.

- **Caso 2:** $a \neq 0$ **e** $b = 0$**.** O gerador é $g = (a, 0)$. O subgrupo gerado é $\langle (a, 0)\rangle = \{(ka, k \cdot 0) \mid k \in \mathbb{Z}\} = \{(ka, 0) \mid k \in \mathbb{Z}\}$. Este subgrupo contém apenas elementos cuja segunda componente é zero. Ele não contém elementos como $(0, 1)$, portanto não pode ser $\mathbb{Z} \times \mathbb{Z}$.

- **Caso 3:** $a = 0$ **e** $b \neq 0$**.** O gerador é $g = (0, b)$. O subgrupo gerado é $\langle (0, b)\rangle = \{(k \cdot 0, kb) \mid k \in \mathbb{Z}\} = \{(0, kb) \mid k \in \mathbb{Z}\}$. Este subgrupo contém apenas elementos cuja primeira componente é zero. Ele não contém elementos como $(1, 0)$, portanto não pode ser $\mathbb{Z} \times \mathbb{Z}$.

- **Caso 4:** $a \neq 0$ **e** $b \neq 0$**.** Seja $H = \langle (a, b)\rangle = \{(ka, kb) \mid k \in \mathbb{Z}\}$. Suponha, por contradição, que $H = \mathbb{Z} \times \mathbb{Z}$. Se H fosse todo o grupo, ele deveria conter todos os elementos de $\mathbb{Z} \times \mathbb{Z}$. Consideremos o elemento $(1, 0) \in \mathbb{Z} \times \mathbb{Z}$. Para que $(1, 0)$ pertencesse a H, deveria existir um inteiro k tal que:

  $$(ka, kb) = (1, 0)$$

  Isto nos forneceria duas equações em $\mathbb{Z}$:

  $$ka = 1$$
  $$kb = 0$$

Como estamos neste caso com $b \neq 0$, a segunda equação ($kb = 0$) implica que k deve ser 0. Mas se $k = 0$, a primeira equação se torna $0 \cdot a = 0$. Chegamos a uma contradição ($0 = 1$). Portanto, o elemento $(1, 0)$ não pode ser gerado por (a, b) se $a \neq 0$ e $b \neq 0$.

Como nenhum dos casos possíveis permite que um único elemento (a, b) gere todo o grupo $\mathbb{Z} \times \mathbb{Z}$, concluímos que $(\mathbb{Z} \times \mathbb{Z}, +)$ é um grupo abeliano que não é cíclico.

Exemplo 2.7.6 (Um Grupo Finito Não Cíclico: O Grupo de Klein)**.** Consideremos o grupo finito $K = \mathbb{Z}_2 \times \mathbb{Z}_2$, conhecido como o **Grupo de Klein**. Os elementos deste grupo são pares ordenados de classes de congruência módulo 2:

$$K = \{([0], [0]), ([1], [0]), ([0], [1]), ([1], [1])\}$$

A ordem do grupo é $|K| = 4$. Para que K fosse cíclico, deveria existir um elemento gerador $g \in K$ com ordem 4, ou seja, $\langle g \rangle = K$.

Vamos analisar o subgrupo gerado por um elemento arbitrário $g = (a, b) \in K$:

- Se $g = ([0], [0])$, o subgrupo gerado é o trivial $\{([0], [0])\}$, que tem ordem 1.
- Para qualquer outro elemento $g \neq ([0], [0])$, observamos o que acontece quando o operamos consigo mesmo:

  $$2 \cdot g = g + g = (a, b) + (a, b) = (a + a, b + b) = (2a, 2b)$$

  Como estamos em $\mathbb{Z}_2$, sabemos que $[2] = [0]$. Portanto:

  $$2 \cdot (a, b) = ([0], [0])$$

Isso demonstra que todo elemento não nulo de $\mathbb{Z}_2 \times \mathbb{Z}_2$ tem ordem 2. Consequentemente, o maior subgrupo cíclico que podemos formar possui apenas 2 elementos (a identidade e o próprio gerador), nunca alcançando os 4 elementos necessários para cobrir todo o grupo K.

Portanto, $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um exemplo clássico de grupo abeliano finito que não é cíclico.

2.7.2 Ordem de um Grupo e Ordem de um Elemento

Definição 2.7.5 (Ordem de um Grupo)**.** A **ordem** de um grupo $(G, *)$, denotada por $|G|$, é o número de elementos no conjunto G (ou seja, a cardinalidade de G).

- Se G possui um número finito de elementos, dizemos que G é um **grupo finito**.
- Se G possui um número infinito de elementos, dizemos que G é um **grupo infinito**.

Exemplo 2.7.7.

- O grupo dos inteiros, $(\mathbb{Z}, +)$, é um **grupo infinito**. Escrevemos $|\mathbb{Z}| = \infty$.
- O grupo dos inteiros módulo m, $(\mathbb{Z}_m, +)$, é um **grupo finito**. Como já estabelecido, ele possui exatamente m classes de equivalência distintas, portanto, sua ordem é $|\mathbb{Z}_m| = m$.

O conceito de ordem também pode ser aplicado a elementos individuais de um grupo. A ordem de um elemento não se refere ao seu valor, mas sim ao seu comportamento cíclico dentro do grupo.

Definição 2.7.6 (Ordem de um Elemento)**.** Seja $(G, *)$ um grupo com elemento identidade e, e seja $a \in G$.

- Dizemos que a tem **ordem finita** se existe um inteiro positivo n tal que $a^n = e$. O menor inteiro positivo n que satisfaz esta condição é chamado de **ordem** do elemento a, denotada por $\text{ord}(a)$.
- Se não existe nenhum inteiro positivo n tal que $a^n = e$, dizemos que a tem **ordem infinita**.

Para um grupo aditivo, a condição $a^n = e$ se traduz para $n \cdot a = 0$, onde 0 é o elemento identidade aditivo.

Proposição 2.7.8. Seja G um grupo e $a \in G$. A ordem do elemento a é igual à cardinalidade do subgrupo cíclico gerado por ele.

$$\text{ord}(a) = |\langle a \rangle|$$

Demonstração. A demonstração será dividida em dois casos, dependendo se a ordem de a é finita ou infinita.

Caso 1: a **tem ordem finita.** Seja $n = \text{ord}(a)$. Por definição, n é o menor inteiro positivo tal que $a^n = e$. Vamos provar que $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

- *Elementos distintos:* Suponha que $a^i = a^j$ para inteiros $0 \leq i < j < n$. Multiplicando ambos os lados por a^{-i}, obtemos $a^{j-i} = e$. Como $0 < j - i < n$, isso contradiz a minimalidade de n. Portanto, os n elementos listados são distintos.
- *Exaustão do subgrupo:* Seja a^k um elemento qualquer de $\langle a \rangle$, com $k \in \mathbb{Z}$. Pelo Algoritmo da Divisão, podemos escrever $k = qn + r$, onde $0 \leq r < n$. Assim:

$$a^k = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

Como $0 \leq r < n$, a^k pertence ao conjunto $\{e, a, \ldots, a^{n-1}\}$.

Concluímos que $\langle a \rangle$ tem exatamente n elementos.

Caso 2: a tem ordem infinita. Neste caso, não existe $n > 0$ tal que $a^n = e$. Suponha que $|\langle a \rangle|$ fosse finito. Então, existiriam inteiros distintos i, j tais que $a^i = a^j$. Supondo sem perda de generalidade que $i < j$, teríamos $a^{j-i} = e$ com $j - i > 0$. Isso implicaria que a tem ordem finita, o que é uma contradição. Portanto, todas as potências de a são distintas, e o subgrupo gerado tem cardinalidade infinita. □

Exemplo 2.7.8.

- **No grupo $(\mathbb{Z}, +)$:**
  - O elemento identidade, 0, tem ordem 1, pois $1 \cdot 0 = 0$ e 1 é o menor inteiro positivo para o qual isso ocorre.
  - Qualquer outro elemento não nulo, como 2, tem **ordem infinita**. Não existe um inteiro positivo n tal que $n \cdot 2 = 0$. O subgrupo gerado, $\langle 2 \rangle = 2\mathbb{Z}$, é infinito.
- **No grupo $(\mathbb{Z}_6, +)$:** O grupo é $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.
  - $\text{ord}([0]) = 1$. O subgrupo gerado é $\langle [0] \rangle = \{[0]\}$.
  - $\text{ord}([1]) = 6$, pois $6 \cdot [1] = [6] = [0]$ e nenhum múltiplo positivo menor resulta em $[0]$. O subgrupo gerado é $\langle [1] \rangle = \{[0], [1], [2], [3], [4], [5]\}$, que tem 6 elementos.
  - $\text{ord}([2]) = 3$, pois $3 \cdot [2] = [6] = [0]$ e nenhum múltiplo positivo menor resulta em $[0]$. O subgrupo gerado é $\langle [2] \rangle = \{[0], [2], [4]\}$, que tem 3 elementos.
  - $\text{ord}([3]) = 2$, pois $2 \cdot [3] = [6] = [0]$ e nenhum múltiplo positivo menor resulta em $[0]$. O subgrupo gerado é $\langle [3] \rangle = \{[0], [3]\}$, que tem 2 elementos.
  - $\text{ord}([4]) = 3$, pois $3 \cdot [4] = [12] = [0]$ e nenhum múltiplo positivo menor resulta em $[0]$. O subgrupo gerado é $\langle [4] \rangle = \{[0], [2], [4]\}$, que tem 3 elementos.
  - $\text{ord}([5]) = 6$, pois $6 \cdot [5] = [30] = [0]$ e nenhum múltiplo positivo menor resulta em $[0]$. O subgrupo gerado é $\langle [5] \rangle = \{[0], [1], [2], [3], [4], [5]\}$, que tem 6 elementos.

2.7.3 Grupos de Permutações

Até o momento, nossos exemplos de grupos se concentraram em conjuntos numéricos com operações de adição ou multiplicação. Contudo, uma vasta e importante classe de grupos surge não de números, mas do conceito de simetria e rearranjo de elementos de um conjunto. Estes são os grupos de permutações, que fornecem os primeiros exemplos concretos de estruturas de grupo **não-abelianas**.

Definição 2.7.7 (Permutação)**.** Uma **permutação** de um conjunto não vazio A é uma bijeção $\sigma : A \to A$. Em outras palavras, é uma regra que rearranja os elementos de A de

tal forma que cada elemento é mapeado para uma posição única, e todas as posições são preenchidas.

Definição 2.7.8 (Grupo Simétrico)**.** Seja S_n o conjunto de todas as permutações do conjunto $\{1, 2, \ldots, n\}$. O conjunto S_n, munido da operação de **composição de funções** ($\circ$), forma um grupo. Este grupo é chamado de **Grupo Simétrico de grau n**.

Para verificar que $(S_n, \circ)$ é de fato um grupo, observamos:

1. **Fechamento:** A composição de duas bijeções é sempre uma bijeção. Se $\sigma, \tau \in S_n$, então $\sigma \circ \tau$ também é uma permutação em S_n.
2. **Associatividade:** A composição de funções é inerentemente associativa.
3. **Elemento Identidade:** A função identidade, $e(x) = x$ para todo x, atua como o elemento identidade do grupo.
4. **Elemento Inverso:** Como toda permutação é uma bijeção, ela admite uma função inversa que também é uma bijeção, garantindo que todo elemento em S_n possui um inverso.

A ordem do grupo simétrico S_n é o total de rearranjos possíveis de n elementos, que é $n!$. Portanto, $|S_n| = n!$.

Exemplo 2.7.9 (O Grupo Simétrico S_3)**.** O grupo S_3 é o grupo de todas as permutações do conjunto $\{1, 2, 3\}$. Sua ordem é $|S_3| = 3! = 6$. Este grupo é pequeno o suficiente para ser analisado em detalhe, mas complexo o suficiente para ilustrar o comportamento não-abeliano. Seus 6 elementos são:

- $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ (a identidade)
- $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
- $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ (troca 2 e 3)
- $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ (troca 1 e 3)
- $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ (troca 1 e 2)

A notação de duas linhas acima é a forma mais explícita de representar uma permutação: a primeira linha lista os elementos do domínio e a segunda linha, suas respectivas imagens.

Composição de Permutações A operação em S_n é a composição de funções, que lemos da direita para a esquerda. Vamos calcular $\sigma_1 \circ \tau_1$:

$$\sigma_1 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Para encontrar o resultado, seguimos o caminho de cada elemento:

- $1 \xrightarrow{\tau_1} 1 \xrightarrow{\sigma_1} 2$
- $2 \xrightarrow{\tau_1} 3 \xrightarrow{\sigma_1} 1$
- $3 \xrightarrow{\tau_1} 2 \xrightarrow{\sigma_1} 3$

Portanto, $\sigma_1 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_3$.

Agora, vamos calcular na ordem inversa, $\tau_1 \circ \sigma_1$:

$$\tau_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

- $1 \xrightarrow{\sigma_1} 2 \xrightarrow{\tau_1} 3$
- $2 \xrightarrow{\sigma_1} 3 \xrightarrow{\tau_1} 2$
- $3 \xrightarrow{\sigma_1} 1 \xrightarrow{\tau_1} 1$

Portanto, $\tau_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_2$.

Como $\sigma_1 \circ \tau_1 = \tau_3$ e $\tau_1 \circ \sigma_1 = \tau_2$, vemos que $\sigma_1 \circ \tau_1 \neq \tau_1 \circ \sigma_1$. Isso demonstra que S_3, e em geral S_n para $n \geq 3$, é um grupo **não-abeliano**.

Notação de Ciclo e Decomposição

Notação de Ciclo: Uma notação mais compacta é a notação de ciclo. Um ciclo $(a_1, a_2, \ldots, a_k)$ representa a permutação que mapeia $a_1 \to a_2$, $a_2 \to a_3, \ldots, a_k \to a_1$, e deixa todos os outros elementos do conjunto fixos. O **comprimento** de um ciclo é o número de elementos que ele contém.

Exemplo 2.7.10. Em S_5, a permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$ pode ser analisada seguindo seus caminhos:

- Começando pelo 1: $1 \to 2 \to 5 \to 1$. Isso forma o ciclo $(1, 2, 5)$.
- Dos elementos restantes, começamos pelo 3: $3 \to 4 \to 3$. Isso forma o ciclo $(3, 4)$.

Podemos, então, escrever σ como o produto de seus ciclos: $\sigma = (1, 2, 5)(3, 4)$. Devemos interpretar cada ciclo como uma permutação distinta que age apenas nos elementos dentro do ciclo e como a identidade nos demais elementos do conjunto $A = \{1, 2, 3, 4, 5\}$.

Definimos duas permutações:

- Seja $\pi_1 = (1, 2, 5)$. Como função, $\pi_1 : A \to A$ é definida por: $\pi_1(1) = 2$, $\pi_1(2) = 5$, $\pi_1(5) = 1$, e $\pi_1(x) = x$ para $x \in \{3, 4\}$.
- Seja $\pi_2 = (3, 4)$. Como função, $\pi_2 : A \to A$ é definida por: $\pi_2(3) = 4$, $\pi_2(4) = 3$, e $\pi_2(x) = x$ para $x \in \{1, 2, 5\}$.

A notação $\sigma = (1, 2, 5)(3, 4)$ significa que a permutação σ é a **composição** (ou produto) destas duas permutações, $\sigma = \pi_1 \circ \pi_2$. Vamos verificar que esta composição resulta na permutação original (lembrando que a composição é lida da direita para a esquerda):

- $\sigma(1) = (\pi_1 \circ \pi_2)(1) = \pi_1(\pi_2(1)) = \pi_1(1) = 2$.
- $\sigma(2) = (\pi_1 \circ \pi_2)(2) = \pi_1(\pi_2(2)) = \pi_1(2) = 5$.
- $\sigma(3) = (\pi_1 \circ \pi_2)(3) = \pi_1(\pi_2(3)) = \pi_1(4) = 4$.
- $\sigma(4) = (\pi_1 \circ \pi_2)(4) = \pi_1(\pi_2(4)) = \pi_1(3) = 3$.
- $\sigma(5) = (\pi_1 \circ \pi_2)(5) = \pi_1(\pi_2(5)) = \pi_1(5) = 1$.

O resultado da composição $(\pi_1 \circ \pi_2)$ é $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$, que é exatamente a permutação σ da qual partimos.

Os elementos de S_3 na notação de ciclo são:

- $e = (1)$ (a identidade, frequentemente omitida)
- $\sigma_1 = (1, 2, 3)$
- $\sigma_2 = (1, 3, 2)$
- $\tau_1 = (2, 3)$
- $\tau_2 = (1, 3)$
- $\tau_3 = (1, 2)$

Proposição 2.7.9. Toda permutação em S_n pode ser escrita como um produto de ciclos disjuntos (ciclos que não compartilham elementos). Essa decomposição é única, a menos da ordem em que os ciclos são escritos.

Demonstração. A demonstração é dividida em duas partes: a prova da **existência** da fatoração e a prova de sua **unicidade**.

Prova da Existência

A prova é construtiva. Seja $\sigma \in S_n$ uma permutação qualquer. Construímos sua decomposição em ciclos disjuntos através do seguinte algoritmo:

1. Escolha um elemento qualquer $a_1 \in \{1, 2, \ldots, n\}$ que ainda não tenha sido incluído em um ciclo.

2. Construa a sequência de imagens sucessivas de a_1 sob σ:

$$a_1, \sigma(a_1), \sigma^2(a_1), \sigma^3(a_1), \ldots$$

   Como o conjunto $\{1, 2, \ldots, n\}$ é finito, esta sequência deve eventualmente se repetir. Seja k o primeiro inteiro positivo tal que $\sigma^k(a_1)$ é igual a um elemento anterior da sequência, $\sigma^j(a_1)$ com $j < k$. Se $j > 0$, poderíamos aplicar σ^{-1} a ambos os lados da igualdade $\sigma^k(a_1) = \sigma^j(a_1)$ para obter $\sigma^{k-1}(a_1) = \sigma^{j-1}(a_1)$, contradizendo a minimalidade de k. Portanto, a primeira repetição deve ser o próprio a_1, ou seja, $j = 0$ e $\sigma^k(a_1) = a_1$.

3. Isso nos fornece o primeiro ciclo, $C_1 = (a_1, \sigma(a_1), \ldots, \sigma^{k-1}(a_1))$.

4. Se todos os elementos de $\{1, 2, \ldots, n\}$ foram incluídos em C_1, o processo termina e $\sigma = C_1$.

5. Caso contrário, retorne ao passo 1, escolhendo um novo elemento b_1 que não pertence a C_1, e repita o processo para gerar um segundo ciclo, C_2.

Este processo garante que os ciclos gerados sejam disjuntos. Suponha que um ciclo C_2, gerado a partir de b_1, compartilhasse um elemento com um ciclo anterior C_1, gerado a partir de a_1. Isso significaria que, para alguns inteiros p e q, teríamos $\sigma^p(a_1) = \sigma^q(b_1)$. Aplicando σ^{-q} a ambos os lados, obteríamos $b_1 = \sigma^{p-q}(a_1)$, o que implicaria que b_1 pertence ao conjunto de elementos do ciclo C_1. Isso contradiz a forma como b_1 foi escolhido (como um elemento que *não* pertencia a nenhum ciclo anterior).

Como o conjunto $\{1, 2, \ldots, n\}$ é finito, este algoritmo deve terminar após um número finito de passos, resultando em uma decomposição de σ em um produto de ciclos disjuntos, $\sigma = C_1 C_2 \cdots C_r$.

Prova da Unicidade

Suponha que tenhamos duas decomposições de σ em produtos de ciclos disjuntos:

$$\sigma = C_1 C_2 \cdots C_r \quad \text{e} \quad \sigma = D_1 D_2 \cdots D_s$$

Nosso objetivo é mostrar que os conjuntos de ciclos $\{C_1, \ldots, C_r\}$ e $\{D_1, \ldots, D_s\}$ são idênticos.

Seja a um elemento qualquer de $\{1, 2, \ldots, n\}$. Na primeira decomposição, como os ciclos C_i são disjuntos, a deve pertencer a exatamente um ciclo, digamos C_k. Pela forma como os ciclos são construídos, o ciclo C_k é unicamente determinado por de a sob a ação de σ, ou seja, C_k é composto precisamente pelos elementos $\{\sigma^i(a) \mid i \in \mathbb{Z}\}$.

Da mesma forma, na segunda decomposição, a deve pertencer a exatamente um ciclo, digamos D_j. Este ciclo D_j também é determinado por a sob a ação de σ. Como tanto C_k quanto D_j são definidos pelo mesmo conjunto de elementos, eles devem ser o mesmo ciclo: $C_k = D_j$.

Como isso vale para qualquer elemento a, cada ciclo na primeira decomposição deve ser igual a um ciclo na segunda decomposição, e vice-versa. Portanto, os dois conjuntos de ciclos são os mesmos. A única liberdade que resta é a ordem em que os ciclos são escritos, pois, como mostraremos a seguir, ciclos disjuntos comutam. □

Proposição 2.7.10. Ciclos disjuntos comutam.

Demonstração. Sejam $\sigma = (a_1, a_2, \ldots, a_k)$ e $\tau = (b_1, b_2, \ldots, b_l)$ dois ciclos disjuntos. Seja $A = \{a_1, \ldots, a_k\}$ o conjunto de elementos movidos por σ, e $B = \{b_1, \ldots, b_l\}$ o conjunto de elementos movidos por τ. Por serem disjuntos, $A \cap B = \emptyset$.

Devemos mostrar que $(\sigma \circ \tau)(x) = (\tau \circ \sigma)(x)$ para qualquer elemento $x \in \{1, 2, \ldots, n\}$. Analisamos três casos:

1. **Caso 1:** $x \in A$.

   - $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. Como $x \notin B$, $\tau(x) = x$. Logo, o resultado é $\sigma(x)$.
   - $(\tau \circ \sigma)(x) = \tau(\sigma(x))$. Como $x \in A$, seu sucessor $\sigma(x)$ também está em A. Portanto, $\sigma(x) \notin B$, o que implica que τ fixa $\sigma(x)$. Logo, o resultado é $\sigma(x)$.

   Ambos os lados são iguais a $\sigma(x)$.

2. **Caso 2:** $x \in B$.

   - $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. Como $x \in B$, seu sucessor $\tau(x)$ também está em B. Portanto, $\tau(x) \notin A$, o que implica que σ fixa $\tau(x)$. Logo, o resultado é $\tau(x)$.
   - $(\tau \circ \sigma)(x) = \tau(\sigma(x))$. Como $x \notin A$, $\sigma(x) = x$. Logo, o resultado é $\tau(x)$.

   Ambos os lados são iguais a $\tau(x)$.

3. **Caso 3:** $x \notin A$ **e** $x \notin B$. Neste caso, x é fixado por ambos os ciclos.

   - $(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$.
   - $(\tau \circ \sigma)(x) = \tau(\sigma(x)) = \tau(x) = x$.

Ambos os lados são iguais a x.

Como a igualdade $(\sigma \circ \tau)(x) = (\tau \circ \sigma)(x)$ se verifica para todos os elementos x, concluímos que $\sigma \circ \tau = \tau \circ \sigma$. □

Ordem de uma Permutação

Proposição 2.7.11. A ordem de uma permutação $\sigma \in S_n$, escrita como um produto de ciclos disjuntos, é o **mínimo múltiplo comum (mmc)** dos comprimentos desses ciclos.

Demonstração. Seja $\sigma \in S_n$, podemos escrever σ de forma única (a menos da ordem dos fatores) como um produto de ciclos disjuntos:

$$\sigma = \pi_1 \pi_2 \dots \pi_m$$

onde cada π_i é um ciclo de comprimento $l_i \geq 1$. Se σ for a identidade, $m = 1$ e $l_1 = 1$.

A ordem de σ, denotada por $\text{ord}(\sigma)$, é o menor inteiro positivo k tal que $\sigma^k = e$, onde e é a permutação identidade.

A comutatividade entre ciclos disjuntos nos permite calcular as potências de σ da seguinte forma:

$$\sigma^k = (\pi_1 \pi_2 \dots \pi_m)^k = \pi_1^k \pi_2^k \dots \pi_m^k$$

Para que σ^k seja a permutação identidade e, a composição $\pi_1^k \pi_2^k \dots \pi_m^k$ deve mapear cada elemento $x \in \{1, 2, \dots, n\}$ para si mesmo.

Consideremos um elemento x que pertence a um dos ciclos, digamos π_i. Como os ciclos são disjuntos, x não é movido por nenhum outro ciclo π_j (onde $j \neq i$). Portanto, a ação de σ^k sobre x é a mesma que a ação de π_i^k sobre x:

$$\sigma^k(x) = (\pi_1^k \dots \pi_i^k \dots \pi_m^k)(x) = \pi_i^k(x)$$

Para que $\sigma^k(x) = x$ (a condição para ser a identidade), devemos ter $\pi_i^k(x) = x$. Isso deve valer para todos os elementos x pertencentes a π_i. A condição para que uma potência de um ciclo π_i mapeie todos os seus elementos para si mesmos é que essa potência seja a identidade.

Portanto, a condição $\sigma^k = e$ é equivalente a exigir que **cada** ciclo individual elevado à potência k resulte na identidade:

$$\sigma^k = e \iff \pi_i^k = e \quad \text{para todo } i = 1, 2, \dots, m$$

A ordem de um único ciclo π_i de comprimento l_i é precisamente l_i. Ou seja, $\pi_i^k = e$ se, e somente se, k é um múltiplo de l_i (ou seja, $l_i \mid k$).

Assim, para que $\sigma^k = e$, o inteiro k deve ser um múltiplo comum de todos os comprimentos dos ciclos disjuntos:

$$l_1 \mid k, \quad l_2 \mid k, \quad \ldots, \quad l_m \mid k$$

A ordem de σ é o *menor* inteiro *positivo* k que satisfaz esta condição. Por definição, o menor inteiro positivo que é um múltiplo comum de $l_1, l_2, \ldots, l_m$ é o **mínimo múltiplo comum** (mmc) desses números.

Se σ contiver pontos fixos, estes correspondem a ciclos de comprimento 1, que podem ser incluídos ou omitidos sem alterar a permutação. Ou seja, para o cálculo da ordem, podemos desconsiderar os ciclos de comprimento 1 sabendo que $\text{mmc}(l_1, \ldots, l_m, 1) = \text{mmc}(l_1, \ldots, l_m)$.

Portanto,

$$\text{ord}(\sigma) = \text{mmc}(l_1, l_2, \ldots, l_m)$$

□

Exemplo 2.7.11.

- A ordem de $\sigma = (1, 2, 5)(3, 4) \in S_5$ é $\text{mmc}(3, 2) = 6$. Isso significa que precisamos aplicar σ seis vezes para que todos os elementos voltem à sua posição original.
- A ordem de $\alpha = (1, 2, 3, 4)(5, 6) \in S_7$ é $\text{mmc}(4, 2) = 4$.

2.7.4 Classes Laterais

Já estabelecemos que um subgrupo é uma estrutura de grupo contida dentro de outra. Uma das consequências mais importantes da existência de um subgrupo é a sua capacidade de particionar o grupo maior em subconjuntos disjuntos e de mesmo tamanho. Essas partições são chamadas de classes laterais (ou cosets).

Definição 2.7.9 (Classes Laterais)**.** Sejam $(G, *)$ um grupo, H um subgrupo de G, e g um elemento qualquer de G.

- A **classe lateral à esquerda** de H determinada por g é o conjunto:

$$gH := \{g * h \mid h \in H\}$$

- A **classe lateral à direita** de H determinada por g é o conjunto:

$$Hg := \{h * g \mid h \in H\}$$

O elemento g é chamado de **representante** da classe. Para grupos comutativos (abelianos), como $(\mathbb{Z}, +)$, as classes laterais à esquerda e à direita são sempre idênticas,

pois $g * h = h * g$. Nesse caso, a notação aditiva é frequentemente usada: $g + H = \{g + h \mid h \in H\}$.

Exemplo 2.7.12 (Classes Laterais em $\mathbb{Z}$)**.** Consideremos o grupo $G = (\mathbb{Z}, +)$ e o subgrupo $H = 4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$. Vamos determinar suas classes laterais.

- **Classe do 0:** $0 + 4\mathbb{Z} = \{0 + h \mid h \in 4\mathbb{Z}\} = \{\dots, -4, 0, 4, 8, \dots\} = 4\mathbb{Z}$. Esta é a classe dos inteiros que deixam resto 0 na divisão por 4.
- **Classe do 1:** $1 + 4\mathbb{Z} = \{1 + h \mid h \in 4\mathbb{Z}\} = \{\dots, -3, 1, 5, 9, \dots\}$. Esta é a classe dos inteiros que deixam resto 1 na divisão por 4.
- **Classe do 2:** $2 + 4\mathbb{Z} = \{2 + h \mid h \in 4\mathbb{Z}\} = \{\dots, -2, 2, 6, 10, \dots\}$. Esta é a classe dos inteiros que deixam resto 2 na divisão por 4.
- **Classe do 3:** $3 + 4\mathbb{Z} = \{3 + h \mid h \in 4\mathbb{Z}\} = \{\dots, -1, 3, 7, 11, \dots\}$. Esta é a classe dos inteiros que deixam resto 3 na divisão por 4.
- **Classe do 4:** $4 + 4\mathbb{Z} = \{4 + h \mid h \in 4\mathbb{Z}\} = \{\dots, 0, 4, 8, 12, \dots\}$. Note que este é exatamente o mesmo conjunto que $0 + 4\mathbb{Z}$. Portanto, $4 + 4\mathbb{Z} = 0 + 4\mathbb{Z}$.

Percebemos que existem exatamente 4 classes laterais distintas, que são precisamente as classes de congruência módulo 4. De fato, para qualquer subgrupo $n\mathbb{Z}$ de $\mathbb{Z}$, as classes laterais são as classes de congruência que formam o conjunto $\mathbb{Z}_n$.

As classes laterais possuem propriedades fundamentais que justificam sua importância. A primeira é que todas elas possuem a mesma cardinalidade que o subgrupo original.

Proposição 2.7.12 (Equipotência das Classes Laterais)**.** Todas as classes laterais (à esquerda ou à direita) de um subgrupo H em um grupo G têm a mesma cardinalidade que o próprio H.

Demonstração. Para demonstrar que $|gH| = |H|$ para qualquer $g \in G$, construiremos uma bijeção $f : H \to gH$. Seja a função $f(h) = g * h$.

- **Injetividade:** Suponha que $f(h_1) = f(h_2)$ para $h_1, h_2 \in H$.

$$g * h_1 = g * h_2$$

Operando g' à esquerda em ambos os lados, podemos cancelar o elemento g:

$$g' * g * h_1 = g' * g * h_2 \implies h_1 = h_2$$

Como $f(h_1) = f(h_2)$ implica $h_1 = h_2$, a função é injetiva.

- **Sobrejetividade:** Seja y um elemento arbitrário da classe lateral gH. Por definição, y deve ter a forma $y = g * h$ para algum $h \in H$. Este elemento h pertence ao domínio H, e é precisamente o elemento tal que $f(h) = y$. Como para todo elemento do contradomínio existe um correspondente no domínio, a função é sobrejetiva.

Como existe uma bijeção entre H e gH, os dois conjuntos possuem a mesma cardinalidade. A demonstração para as classes à Direita (Hg) é análoga.

□

Proposição 2.7.13 (Partição de um Grupo por Classes Laterais)**.** O conjunto de todas as classes laterais à esquerda (ou à direita) de um subgrupo H em G forma uma partição de G. Isto é, duas classes laterais quaisquer são ou idênticas ou disjuntas.

Demonstração. Sejam aH e bH duas classes laterais à esquerda de H em G. Devemos provar que ou $aH = bH$ ou $aH \cap bH = \emptyset$.

Para isso, vamos assumir que a interseção delas **não** é vazia e provar que, neste caso, elas devem ser idênticas. Suponha que $aH \cap bH \neq \emptyset$. Isso significa que existe pelo menos um elemento x que pertence a ambas as classes.

$$x \in aH \quad \text{e} \quad x \in bH$$

Pela definição de classe lateral, existem elementos $h_1, h_2 \in H$ tais que:

$$x = a * h_1 \quad \text{e} \quad x = b * h_2$$

Igualando as duas expressões para x, temos $a * h_1 = b * h_2$. Isolando a, obtemos $a = (b * h_2) * h_1'$, onde h_1' é o inverso de h_1. Pela associatividade,

$$a = b * (h_2 * h_1')$$

Seja $h_3 = h_2 * h_1'$. Como H é um subgrupo, ele é fechado sob a operação e sob inversos, então h_3 também deve pertencer a H. Assim, podemos escrever $a = b * h_3$ para algum $h_3 \in H$.

Agora, vamos provar que $aH = bH$.

- **Prova de que $aH \subseteq bH$:** Seja y um elemento qualquer de aH. Então $y = a * h_4$ para algum $h_4 \in H$. Substituindo a expressão para a:

  $$y = (b * h_3) * h_4 = b * (h_3 * h_4)$$

  Como H é um subgrupo, o elemento $h_5 = h_3 * h_4$ também está em H. Logo, $y = b * h_5$, o que, por definição, significa que $y \in bH$.

- **Prova de que** $bH \subseteq aH$**:** A partir de $a = b * h_3$, podemos isolar b: $b = a * h_3'$. O argumento é simétrico ao anterior. Seja z um elemento qualquer de bH. Então $z = b * h_6$ para algum $h_6 \in H$. Substituindo b:

$$z = (a * h_3') * h_6 = a * (h_3' * h_6)$$

  O elemento $h_7 = h_3' * h_6$ está em H, logo $z \in aH$.

Como $aH \subseteq bH$ e $bH \subseteq aH$, concluímos que $aH = bH$. Portanto, se duas classes laterais têm qualquer elemento em comum, elas são idênticas. A única outra possibilidade é que elas não tenham nenhum elemento em comum, ou seja, sejam disjuntas.
A demonstração para as classes à Direita (Ha e Hb) é análoga. □

Uma maneira alternativa de compreender as classes laterais é através do conceito de relação de equivalência. Podemos definir uma relação específica sobre os elementos do grupo G que agrupa os elementos exatamente nas classes laterais de H.

Proposição 2.7.14 (Relação de Congruência Módulo um Subgrupo)**.** Seja H um subgrupo de um grupo G. A relação definida em G por:

$$a \sim_L b \iff a^{-1}b \in H$$

é uma relação de equivalência. Além disso, a classe de equivalência de qualquer elemento $a \in G$, denotada por $[a]$, é exatamente a classe lateral à esquerda aH.

Demonstração. Para provar que $\sim_L$ é uma relação de equivalência, verificamos as três propriedades fundamentais:

1. **Reflexividade:** Para todo $a \in G$, temos $a^{-1}a = e$. Como H é um subgrupo, o elemento identidade e pertence a H. Logo, $a \sim_L a$.

2. **Simetria:** Se $a \sim_L b$, então $a^{-1}b \in H$. Como H é um subgrupo, ele é fechado sob inversos. Portanto, o inverso de $a^{-1}b$, que é $(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$, também pertence a H. Isso implica que $b \sim_L a$.

3. **Transitividade:** Se $a \sim_L b$ e $b \sim_L c$, então $a^{-1}b \in H$ e $b^{-1}c \in H$. Como H é fechado sob a operação do grupo, o produto desses elementos também está em H:

$$(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}ec = a^{-1}c$$

   Como $a^{-1}c \in H$, concluímos que $a \sim_L c$.

Agora, vamos mostrar que a classe de equivalência $[a]$ é igual ao conjunto aH. Por definição, $[a] = \{x \in G \mid a \sim_L x\}$.

$$x \in [a] \iff a \sim_L x \iff a^{-1}x \in H$$

Seja $h = a^{-1}x$. Então $h \in H$ e podemos escrever $x = ah$. Isso mostra que x é um elemento da forma ah com $h \in H$, ou seja, $x \in aH$. Reciprocamente, se $x \in aH$, então $x = ah$ para algum $h \in H$, o que implica $a^{-1}x = h \in H$, logo $x \in [a]$. Portanto, $[a] = aH$. □

2.7.5 Teorema de Lagrange

A partição de um grupo por meio das classes laterais de um subgrupo é uma ferramenta especialmente importante no estudo de grupos finitos. Como todas as classes laterais de um subgrupo H possuem o mesmo tamanho de H, e como elas separam os elementos do grupo G sem sobreposição, podemos concluir uma relação entre o número de elementos de G e o de H. Essa conclusão é formalizada no Teorema de Lagrange.

Teorema 2.7.1 (Teorema de Lagrange)**.** Sejam G um grupo **finito** e H um subgrupo de G. Então, a ordem de H divide a ordem de G.

Demonstração. Seja G um grupo finito de ordem n e H um subgrupo de G de ordem m. Como já demonstrado, o conjunto de todas as classes laterais à esquerda de H em G forma uma partição de G. Sejam $g_1H, g_2H, \ldots, g_kH$ as k classes laterais à esquerda distintas de H.

Por formarem uma partição, duas propriedades são verdadeiras:

1. Elas são mutuamente disjuntas: $g_iH \cap g_jH = \emptyset$ para $i \neq j$.
2. Sua união reconstrói o grupo G por completo: $G = g_1H \cup g_2H \cup \cdots \cup g_kH$.

Como os conjuntos são disjuntos, a ordem da união é a soma das cardinalidades de cada subconjunto:

$$|G| = |g_1H| + |g_2H| + \cdots + |g_kH|$$

Também já demonstramos que todas as classes laterais têm a mesma cardinalidade que o subgrupo H. Portanto, para todo $i \in \{1, \ldots, k\}$, temos $|g_iH| = |H| = m$. Substituindo essa igualdade na soma, obtemos:

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{k \text{ vezes}}$$

Ou seja:

$$n = k \cdot m$$

Esta equação, por definição, significa que a ordem de H (m) divide a ordem de G (n). O quociente da divisão é exatamente k, que é o número de classes laterais distintas. Este número k é chamado de **índice** de H em G, denotado por $[G : H]$. Portanto, a relação pode ser escrita como $|G| = |H| \cdot [G : H]$. □

O Teorema de Lagrange é extremamente poderoso não apenas pelo que afirma, mas também pelo que restringe. Por exemplo, ele nos diz que um grupo de ordem 10 **não pode** ter um subgrupo de ordem 3.

Proposição 2.7.15 (Ordem de um Elemento divide a Ordem do Grupo)**.** Em um grupo finito G, a ordem de qualquer elemento $a \in G$ deve dividir a ordem de G.

Demonstração. Seja a um elemento de um grupo finito G. A ordem de a, denotada por $\text{ord}(a)$, é, por definição, a ordem do subgrupo cíclico gerado por a, $\langle a \rangle$. Como $\langle a \rangle$ é um subgrupo de G, pelo Teorema de Lagrange, sua ordem deve dividir a ordem de G. Logo, $\text{ord}(a) \mid |G|$. □

Proposição 2.7.16 (Grupos de Ordem Prima)**.** Todo grupo de ordem prima é cíclico.

Demonstração. Seja G um grupo de ordem $|G| = p$, onde p é um número primo. Como $p \geq 2$, o grupo deve conter pelo menos um elemento além da identidade, e. Seja a um elemento de G tal que $a \neq e$. Consideremos o subgrupo cíclico gerado por a, $\langle a \rangle$. Pelo Teorema de Lagrange, a ordem de $\langle a \rangle$ deve dividir a ordem de G, que é p. Os únicos divisores positivos de um número primo p são 1 e p. Como $a \neq e$, o subgrupo $\langle a \rangle$ contém mais do que apenas o elemento identidade, então sua ordem não pode ser 1. A única possibilidade restante é que $|\langle a \rangle| = p$. Como $\langle a \rangle$ é um subgrupo de G e tem a mesma ordem de G, ele deve ser o próprio grupo G. Portanto, $G = \langle a \rangle$, o que, por definição, significa que G é cíclico. □

Observação: Como o elemento $a \neq e$ foi escolhido arbitrariamente, o mesmo argumento se aplica a qualquer elemento de G que não seja a identidade. Ou seja, se $|G| = p$ (primo), então para **todo** $a \in G$ com $a \neq e$, temos que $\langle a \rangle = G$. Em outras palavras, em um grupo de ordem prima, todo elemento diferente da identidade é um gerador do grupo.

Exemplo 2.7.13. Vamos analisar o grupo $G = (\mathbb{Z}_{12}, +)$, cuja ordem é $|G| = 12$.

- O elemento $[3]$ gera o subgrupo $\langle [3] \rangle = \{[0], [3], [6], [9]\}$. A ordem deste subgrupo é 4, e 4 divide 12. A ordem do elemento $[3]$ é 4.
- O elemento $[8]$ gera o subgrupo $\langle [8] \rangle = \{[0], [4], [8]\}$. A ordem deste subgrupo é 3, e 3 divide 12. A ordem do elemento $[8]$ é 3.
- O Teorema de Lagrange nos garante que $\mathbb{Z}_{12}$ não pode ter subgrupos de ordem 5, 7, 8, 9, 10 ou 11.

Exemplo 2.7.14 (Grupos de Ordem Prima)**.** Vamos ilustrar a afirmação de que todo grupo de ordem prima é cíclico, usando o grupo $G = (\mathbb{Z}_7, +)$. A ordem deste grupo é $|G| = 7$, que é um número primo. A afirmação implica que qualquer elemento não nulo de $\mathbb{Z}_7$ deve ser um gerador do grupo. Vamos demonstrar que isso é verdade.

Para verificar isso na prática, podemos calcular o subgrupo gerado por alguns elementos não nulos:

- **Verificação para o gerador** $[2]$**:**

$$\begin{aligned}
1 \cdot [2] &= [2] \\
2 \cdot [2] &= [2] + [2] = [4] \\
3 \cdot [2] &= [2] + [2] + [2] = [6] \\
4 \cdot [2] &= [6] + [2] = [8] \equiv [1] \pmod 7 \\
5 \cdot [2] &= [1] + [2] = [3] \\
6 \cdot [2] &= [3] + [2] = [5] \\
7 \cdot [2] &= [5] + [2] = [7] \equiv [0] \pmod 7
\end{aligned}$$

  O conjunto gerado é $\{[0], [1], [2], [3], [4], [5], [6]\}$, que é o próprio $\mathbb{Z}_7$.

- **Verificação para o gerador** $[3]$**:**

$$\begin{aligned}
1 \cdot [3] &= [3] \\
2 \cdot [3] &= [3] + [3] = [6] \\
3 \cdot [3] &= [6] + [3] = [9] \equiv [2] \pmod 7 \\
4 \cdot [3] &= [2] + [3] = [5] \\
5 \cdot [3] &= [5] + [3] = [8] \equiv [1] \pmod 7 \\
6 \cdot [3] &= [1] + [3] = [4] \\
7 \cdot [3] &= [4] + [3] = [7] \equiv [0] \pmod 7
\end{aligned}$$

  O conjunto gerado é $\{[0], [1], [2], [3], [4], [5], [6]\}$, que novamente é o próprio $\mathbb{Z}_7$.

- **Verificação para o gerador** $[4]$**:**

$$\begin{aligned}
&1 \cdot [4] = [4] \\
&2 \cdot [4] = [4] + [4] = [8] \equiv [1] \pmod 7 \\
&3 \cdot [4] = [1] + [4] = [5] \\
&4 \cdot [4] = [5] + [4] = [9] \equiv [2] \pmod 7 \\
&5 \cdot [4] = [2] + [4] = [6] \\
&6 \cdot [4] = [6] + [4] = [10] \equiv [3] \pmod 7 \\
&7 \cdot [4] = [3] + [4] = [7] \equiv [0] \pmod 7
\end{aligned}$$

  O conjunto gerado é $\{[0], [1], [2], [3], [4], [5], [6]\}$, que é o próprio $\mathbb{Z}_7$.

- **Verificação para o gerador** $[5]$**:**

$$\begin{aligned}
&1 \cdot [5] = [5] \\
&2 \cdot [5] = [5] + [5] = [10] \equiv [3] \pmod 7 \\
&3 \cdot [5] = [3] + [5] = [8] \equiv [1] \pmod 7 \\
&4 \cdot [5] = [1] + [5] = [6] \\
&5 \cdot [5] = [6] + [5] = [11] \equiv [4] \pmod 7 \\
&6 \cdot [5] = [4] + [5] = [9] \equiv [2] \pmod 7 \\
&7 \cdot [5] = [2] + [5] = [7] \equiv [0] \pmod 7
\end{aligned}$$

  O conjunto gerado é $\{[0], [1], [2], [3], [4], [5], [6]\}$, que é o próprio $\mathbb{Z}_7$.

- **Verificação para o gerador** $[6]$**:**

$$\begin{aligned}
&1 \cdot [6] = [6] \\
&2 \cdot [6] = [6] + [6] = [12] \equiv [5] \pmod 7 \\
&3 \cdot [6] = [5] + [6] = [11] \equiv [4] \pmod 7 \\
&4 \cdot [6] = [4] + [6] = [10] \equiv [3] \pmod 7 \\
&5 \cdot [6] = [3] + [6] = [9] \equiv [2] \pmod 7 \\
&6 \cdot [6] = [2] + [6] = [8] \equiv [1] \pmod 7 \\
&7 \cdot [6] = [1] + [6] = [7] \equiv [0] \pmod 7
\end{aligned}$$

  O conjunto gerado é $\{[0], [1], [2], [3], [4], [5], [6]\}$, que é o próprio $\mathbb{Z}_7$.

Com isso, a verificação está completa, demonstrando que todos os 6 elementos não nulos de $\mathbb{Z}_7$ são, de fato, geradores do grupo.

2.7.6 Subgrupos Normais

Vimos que qualquer subgrupo H de um grupo G particiona G em classes laterais à esquerda (gH) e à direita (Hg). Em grupos abelianos, como $(\mathbb{Z}, +)$, a comutatividade da operação garante que $g + H = H + g$, ou seja, as classes laterais à esquerda e à direita são sempre idênticas. No entanto, em grupos não-abelianos, isso nem sempre é verdade. Os subgrupos que satisfazem essa condição são chamados de **Subgrupos Normais**.

Definição 2.7.10 (Subgrupo Normal)**.** Um subgrupo N de um grupo $(G, *)$ é chamado de **subgrupo normal** de G se suas classes laterais à esquerda e à direita coincidem para todos os elementos do grupo. Ou seja:

$$\forall g \in G, \quad gN = Ng$$

Para denotar que N é um subgrupo normal de G, utilizamos a notação $N \triangleleft G$.

Todo grupo G possui pelo menos dois subgrupos normais, chamados de **subgrupos normais triviais**: o subgrupo que contém apenas a identidade, $\{e\}$, e o próprio grupo G.

Proposição 2.7.17. Todo subgrupo de um grupo abeliano é normal.

Demonstração. Sejam G um grupo abeliano e H um subgrupo qualquer de G. Para provar que H é normal, devemos mostrar que $gH = Hg$ para todo $g \in G$.

Primeiro, vamos mostrar que $gH \subseteq Hg$. Seja x um elemento qualquer de gH. Por definição, $x = g * h$ para algum $h \in H$. Como G é abeliano, a operação é comutativa, então $g * h = h * g$. A expressão $h * g$ é, por definição, um elemento da classe lateral à direita Hg. Portanto, $x \in Hg$.

A prova de que $Hg \subseteq gH$ é análoga. Seja $y \in Hg$, então $y = h * g$ para algum $h \in H$. Pela comutatividade, $y = g * h$, o que implica que $y \in gH$.

Como provamos a inclusão em ambos os sentidos, concluímos que $gH = Hg$. Portanto, em um grupo abeliano, todo subgrupo é normal. □

Exemplo 2.7.15 (Subgrupos de $\mathbb{Z}$ e $\mathbb{Z}_m$)**.** Uma consequência direta da proposição anterior é que todos os subgrupos que estudamos até agora são normais.

- Como $(\mathbb{Z}, +)$ é um grupo abeliano, todo subgrupo da forma $n\mathbb{Z}$ é um subgrupo normal de $\mathbb{Z}$.
- Como $(\mathbb{Z}_m, +)$ é um grupo abeliano, todos os seus subgrupos são normais.

A definição $gN = Ng$ é intuitiva, mas para demonstrações, muitas vezes é mais prático usar uma condição equivalente que envolve a chamada conjugação.

Proposição 2.7.18 (Critério de Normalidade por Conjugação)**.** Seja N um subgrupo de G. As seguintes afirmações são equivalentes:

1. N é um subgrupo normal de G (i.e., $\forall g \in G, gN = Ng$).
2. $\forall g \in G, gNg^{-1} = N$, onde $gNg^{-1} := \{g * n * g^{-1} \mid n \in N\}$.

Demonstração. **($1 \implies 2$):** Suponha que N é normal, ou seja, $gN = Ng$ para todo $g \in G$. Vamos provar que $gNg^{-1} = N$.

- ($gNg^{-1} \subseteq N$) Seja $x \in gNg^{-1}$. Então $x = g * n * g^{-1}$ para algum $n \in N$. O termo $g * n$ é um elemento de gN. Como $gN = Ng$, este elemento também deve estar em Ng. Isso significa que $g * n = n_1 * g$ para algum $n_1 \in N$. Substituindo na expressão de x:

  $$x = (n_1 * g) * g^{-1} = n_1 * (g * g^{-1}) = n_1 * e = n_1$$

  Como $n_1 \in N$, concluímos que $x \in N$. Logo, $gNg^{-1} \subseteq N$.

- ($n \subseteq gNg^{-1}$) Seja n um elemento qualquer de N. Queremos mostrar que $n \in gNg^{-1}$. O termo $n * g$ é um elemento de Ng. Como $Ng = gN$, este elemento também deve estar em gN. Isso significa que $n * g = g * n_2$ para algum $n_2 \in N$. Multiplicando ambos os lados à direita por g^{-1}:

  $$(n * g) * g^{-1} = (g * n_2) * g^{-1} \implies n = g * n_2 * g^{-1}$$

  A expressão $g * n_2 * g^{-1}$ é, por definição, um elemento de gNg^{-1}. Logo, $n \in gNg^{-1}$.

Como as duas inclusões são verdadeiras, $gNg^{-1} = N$.

($2 \implies 1$): Suponha que $gNg^{-1} = N$ para todo $g \in G$. Queremos provar que $gN = Ng$.

- ($gN \subseteq Ng$) Seja $x \in gN$, então $x = g * n$ para algum $n \in N$. Da nossa hipótese, sabemos que $g * n * g^{-1}$ é um elemento de N. Vamos chamá-lo de n_1.

  $$g * n * g^{-1} = n_1 \implies g * n = n_1 * g$$

  Como $n_1 * g$ é um elemento de Ng, mostramos que $x \in Ng$.

- ($Ng \subseteq gN$) Seja $y \in Ng$, então $y = n * g$ para algum $n \in N$. Da nossa hipótese, sabemos que $N = gNg^{-1}$, o que implica que para qualquer $n \in N$, existem $n_2 \in N$ tal que $n = g * n_2 * g^{-1}$. Substituindo na expressão de y:

  $$y = (g * n_2 * g^{-1}) * g = g * n_2 * (g^{-1} * g) = g * n_2 * e = g * n_2$$

  Como $g * n_2$ é um elemento de gN, mostramos que $y \in gN$.

Como as duas inclusões são verdadeiras, $gN = Ng$, e N é normal. □

Exemplo 2.7.16 (Um Subgrupo Normal em um Grupo Não-Abeliano)**.** Como já estabelecido, o grupo simétrico S_3 é um grupo não-abeliano de ordem $3! = 6$. Vamos demonstrar que o subgrupo gerado pela permutação $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$ é um subgrupo normal de S_3.

Os elementos de S_3, em notação de duas linhas e ciclo, são:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3), \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2), \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3), \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$$

Seja N o subgrupo cíclico gerado por $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$. Seus elementos são as potências (composições) de σ_1:

- $\sigma_1^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$
- $\sigma_1^2 = \sigma_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$
- $\sigma_1^3 = \sigma_1^2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$

Portanto, o subgrupo é $N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} = \{e, (1,2,3), (1,3,2)\}$. Este subgrupo, conhecido como o **grupo alternado** A_3, tem ordem $|N| = 3$.

Para provar que N é um subgrupo normal de S_3 ($N \triangleleft S_3$), devemos mostrar que suas classes laterais à esquerda e à direita coincidem para todos os elementos do grupo, ou seja, $\forall g \in S_3, gN = Ng$. O número de classes laterais distintas (o índice de N em S_3) é $[S_3 : N] = |S_3|/|N| = 6/3 = 2$. Portanto, precisamos encontrar duas classes distintas.

Cálculo das Classes Laterais à Esquerda

- **Classe de e:** A primeira classe é o próprio subgrupo N, que pode ser representada por qualquer um de seus elementos, como e.

$$eN = N = \{e, \sigma_1, \sigma_2\}$$

Em notação de ciclo e de duas linhas, os elementos são:

$$N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} = \{e, (1,2,3), (1,3,2)\}$$

- **Classe de τ_1:** A segunda classe é obtida escolhendo um elemento $g \in S_3$ que não pertence a N, como $g = \tau_1 = (1,2)$. A classe é o conjunto $\tau_1 N = \{\tau_1 \circ n \mid n \in N\}$. Vamos calcular cada elemento:

$$\begin{aligned} \tau_1 \circ e &= (1,2) \circ e = (1,2) = \tau_1 \\ \tau_1 \circ \sigma_1 &= (1,2) \circ (1,2,3) = (2,3) = \tau_3 \\ \tau_1 \circ \sigma_2 &= (1,2) \circ (1,3,2) = (1,3) = \tau_2 \end{aligned}$$

  Portanto, a segunda classe lateral à esquerda é o conjunto das transposições:

$$\tau_1 N = \{\tau_1, \tau_3, \tau_2\}$$

  Em notação de ciclo e de duas linhas:

$$\tau_1 N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} = \{(1,2), (2,3), (1,3)\}$$

As duas classes laterais à esquerda, N e $\tau_1 N$, são disjuntas e sua união é S_3.

Cálculo das Classes Laterais à Direita

Agora, repetimos o processo para as classes laterais à direita.

- **Classe de e:** A primeira classe é, novamente, o próprio subgrupo N.

$$Ne = N = \{e, \sigma_1, \sigma_2\} = \{e, (1,2,3), (1,3,2)\}$$

- **Classe de τ_1:** Usando o mesmo representante $g = \tau_1 = (1,2)$, calculamos a classe $N\tau_1 = \{n \circ \tau_1 \mid n \in N\}$.

$$\begin{aligned} e \circ \tau_1 &= e \circ (1,2) = (1,2) = \tau_1 \\ \sigma_1 \circ \tau_1 &= (1,2,3) \circ (1,2) = (1,3) = \tau_2 \\ \sigma_2 \circ \tau_1 &= (1,3,2) \circ (1,2) = (2,3) = \tau_3 \end{aligned}$$

  A segunda classe lateral à direita é, portanto:

$$N\tau_1 = \{\tau_1, \tau_2, \tau_3\}$$

Em notação de ciclo e de duas linhas:

$$N\tau_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} = \{(1,2), (1,3), (2,3)\}$$

As duas classes laterais à direita, N e $N\tau_1$, também particionam S_3.

Como a partição de S_3 em classes laterais à esquerda é a mesma que a partição em classes laterais à direita, concluímos que $gN = Ng$ para todo $g \in S_3$. Portanto, $N = A_3$ é um subgrupo normal de S_3, fornecendo um exemplo concreto de um subgrupo normal não trivial em um grupo não-abeliano.

2.7.7 Grupo Quociente

A propriedade fundamental de um subgrupo normal $N \triangleleft G$ é que suas classes laterais à esquerda e à direita coincidem. Essa simetria nos permite dar um passo adiante: em vez de ver as classes laterais apenas como uma partição do grupo original, podemos tratá-las como os elementos de um novo grupo. A construção deste novo grupo, chamado de **grupo quociente**, é uma das ideias mais poderosas da teoria dos grupos.

Definição 2.7.11 (Grupo Quociente)**.** Sejam G um grupo e N um subgrupo normal de G. O **grupo quociente** de G por N, denotado por G/N, é o conjunto de todas as classes laterais de N em G,

$$G/N = \{gN \mid g \in G\}$$

munido da operação binária definida por:

$$(aN) * (bN) := (a * b)N$$

para quaisquer $aN, bN \in G/N$.

Para que esta definição seja válida, a operação deve ser **bem-definida**. Isso significa que o resultado da operação não pode depender dos representantes (a e b) escolhidos para as classes. É aqui que a condição de normalidade do subgrupo se torna indispensável.

Proposição 2.7.19. A operação $*$ no conjunto quociente G/N é bem-definida se, e somente se, N é um subgrupo normal de G.

Demonstração. Como se trata de uma equivalência, devemos provar as duas implicações.

($\Leftarrow$) Se N é normal, a operação é bem-definida.

Suponha que $N \triangleleft G$. Devemos provar que o resultado da operação independe dos representantes escolhidos. Sejam $a, a', b, b' \in G$ tais que $aN = a'N$ e $bN = b'N$. Isso

implica que existem $n_1, n_2 \in N$ tais que $a' = a * n_1$ e $b' = b * n_2$. Queremos mostrar que $(a' * b')N = (a * b)N$. Calculando o produto dos novos representantes:

$$a' * b' = (a * n_1) * (b * n_2) = a * (n_1 * b) * n_2$$

Como N é normal, temos $Nb = bN$. Logo, o elemento $n_1 * b \in Nb$ deve pertencer a bN. Isso significa que existe $n_3 \in N$ tal que $n_1 * b = b * n_3$. Substituindo na equação anterior:

$$a' * b' = a * (b * n_3) * n_2 = (a * b) * (n_3 * n_2)$$

Como N é subgrupo, $n_3 * n_2 \in N$. Logo, $a' * b' = (a * b) * n$, onde $n \in N$. Isso mostra que $a' * b' \in (a * b)N$, ou seja, $(a' * b')N = (a * b)N$. A operação é bem-definida.

($\Rightarrow$) Se a operação é bem-definida, então N é normal.

Suponha que a operação em G/N esteja bem-definida. Isso significa que, para quaisquer representantes $u \in aN$ e $v \in bN$, o produto $u * v$ deve pertencer à classe $(a * b)N$. Para provar que N é normal, vamos mostrar que $g * n * g^{-1} \in N$ para todo $g \in G$ e $n \in N$. Considere as classes gN e $g^{-1}N$. O produto canônico dessas classes é $(g * g^{-1})N = eN = N$. Agora, escolhamos outros representantes para essas mesmas classes:

- Como $n \in N$, temos que $g * n \in gN$. Vamos usar $g * n$ como representante da primeira classe.
- Vamos manter g^{-1} como representante da segunda classe.

Pela hipótese de que a operação é bem-definida, o produto desses representantes deve cair na mesma classe resultante (que calculamos ser N). Logo:

$$(g * n) * g^{-1} \in N$$

Pela associatividade, $g * n * g^{-1} \in N$. Como isso vale para qualquer $g \in G$ e $n \in N$, concluímos que N é um subgrupo normal de G. □

Com a operação bem-definida, podemos afirmar que $(G/N, *)$ é de fato um grupo:

- **Associatividade:** A associatividade é herdada da operação em G.

$$\begin{aligned}((aN)(bN))(cN) &= ((ab)N)(cN) \\ &= ((ab)c)N \\ &= (a(bc))N \\ &= (aN)((bc)N) \\ &= (aN)((bN)(cN))\end{aligned}$$

- **Elemento Identidade:** A classe lateral $eN = N$ é o elemento identidade, pois $(aN)(eN) = (a * e)N = aN$.
- **Elemento Inverso:** O inverso de um elemento gN é a classe $g^{-1}N$, pois $(gN)(g^{-1}N) = (g * g^{-1})N = eN = N$.

Exemplo 2.7.17 (O Grupo Quociente S_3/A_3)**.** Como vimos no exemplo anterior, $A_3 = \{e, (1,2,3), (1,3,2)\}$ é um subgrupo normal de S_3. O grupo quociente S_3/A_3 é o conjunto de suas classes laterais. Como o índice é 2, existem apenas dois elementos:

$$S_3/A_3 = \{A_3, \quad \tau_1 A_3\}$$

onde A_3 é a classe dos elementos de N e $\tau_1 A_3$ é a classe das transposições. A operação entre esses elementos se comporta da seguinte maneira:

- $A_3 \circ A_3 = (e \circ e)A_3 = eA_3 = A_3$
- $A_3 \circ (\tau_1 A_3) = (e \circ \tau_1)A_3 = \tau_1 A_3$
- $(\tau_1 A_3) \circ A_3 = (\tau_1 \circ e)A_3 = \tau_1 A_3$
- $(\tau_1 A_3) \circ (\tau_1 A_3) = (\tau_1 \circ \tau_1)A_3 = eA_3 = A_3$

Proposição 2.7.20. O grupo quociente $(S_3/A_3, \circ)$ é isomórfico ao grupo dos inteiros módulo 2, $(\mathbb{Z}_2, +)$. Formalmente:

$$S_3/A_3 \cong \mathbb{Z}_2$$

Demonstração. Para provar que o grupo quociente $(S_3/A_3, \circ)$ é isomórfico ao grupo $(\mathbb{Z}_2, +)$, devemos construir uma função $f : S_3/A_3 \to \mathbb{Z}_2$ que seja um homomorfismo bijetivo.

Os dois grupos em questão são:

- $G = S_3/A_3 = \{A_3, \tau_1 A_3\}$, com a operação de composição de classes laterais $(\circ)$.
- $H = (\mathbb{Z}_2, +) = \{[0]_2, [1]_2\}$, com a operação de adição modular.

Definição da Função

Definimos a função $f : S_3/A_3 \to \mathbb{Z}_2$ da forma mais natural: mapeando o elemento identidade de um grupo para o elemento identidade do outro.

- O elemento identidade de S_3/A_3 é a classe A_3.
- O elemento identidade de $\mathbb{Z}_2$ é a classe $[0]_2$.

Assim, definimos a função f da seguinte maneira:

$$f(A_3) = [0]_2$$

$$f(\tau_1 A_3) = [1]_2$$

Verificação da Bijeção

Como os dois conjuntos são finitos e possuem o mesmo número de elementos (ordem 2), para provar que a função é uma bijeção, basta mostrar que ela é injetiva ou sobrejetiva.

- **Injetividade:** Os dois elementos distintos do domínio, A_3 e $\tau_1 A_3$, são mapeados para dois elementos distintos no contradomínio, $[0]_2$ e $[1]_2$. Portanto, a função é injetiva.
- **Sobrejetividade:** Todo elemento do contradomínio ($\{[0]_2, [1]_2\}$) é a imagem de algum elemento do domínio. Portanto, a função é sobrejetiva.

Como f é injetiva e sobrejetiva, ela é uma bijeção.

Verificação do Homomorfismo

Devemos verificar se a função preserva a operação, ou seja, se $f(x \circ y) = f(x) + f(y)$ para todos os $x, y \in S_3/A_3$. Analisamos todas as quatro combinações possíveis, utilizando os resultados das operações já estabelecidos:

- **Caso 1:** $A_3 \circ A_3$
  - $f(A_3 \circ A_3) = f(A_3) = [0]_2$
  - $f(A_3) + f(A_3) = [0]_2 + [0]_2 = [0]_2$

  A igualdade se verifica.
- **Caso 2:** $A_3 \circ (\tau_1 A_3)$
  - $f(A_3 \circ (\tau_1 A_3)) = f(\tau_1 A_3) = [1]_2$
  - $f(A_3) + f(\tau_1 A_3) = [0]_2 + [1]_2 = [1]_2$

  A igualdade se verifica.
- **Caso 3:** $(\tau_1 A_3) \circ A_3$
  - $f((\tau_1 A_3) \circ A_3) = f(\tau_1 A_3) = [1]_2$
  - $f(\tau_1 A_3) + f(A_3) = [1]_2 + [0]_2 = [1]_2$

  A igualdade se verifica.

- **Caso 4:** $(\tau_1 A_3) \circ (\tau_1 A_3)$
  - $f((\tau_1 A_3) \circ (\tau_1 A_3)) = f(A_3) = [0]_2$
  - $f(\tau_1 A_3) + f(\tau_1 A_3) = [1]_2 + [1]_2 = [0]_2$

  A igualdade se verifica.

Como a função f preserva a operação para todas as combinações de elementos, ela é um homomorfismo.

Tendo demonstrado que a função f é um homomorfismo bijetivo, concluímos que ela é um isomorfismo. Portanto, os grupos $(S_3/A_3, \circ)$ e $(\mathbb{Z}_2, +)$ são isomórficos. □

Exemplo 2.7.18 (O Grupo Quociente $\mathbb{Z}/n\mathbb{Z}$ e sua Relação com $\mathbb{Z}_n$)**.** Como o grupo dos inteiros $(\mathbb{Z}, +)$ é abeliano, todo subgrupo da forma $n\mathbb{Z}$ (o conjunto infinito de números inteiros que são múltiplos de n) é normal. Isso nos permite construir o grupo quociente $\mathbb{Z}/n\mathbb{Z}$, que é o conjunto de todas as classes laterais de $n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} \mid k \in \mathbb{Z}\}$$

Este exemplo é fundamental, pois ele estabelece uma conexão direta entre a estrutura abstrata dos grupos quocientes e a aritmética modular que já estudamos. Vamos provar formalmente que as classes laterais de $n\mathbb{Z}$ são precisamente as classes de congruência módulo n, e que o grupo quociente resultante é isomórfico a $(\mathbb{Z}_n, +)$.

Proposição 2.7.21. Para qualquer $a \in \mathbb{Z}$, a classe lateral $a + n\mathbb{Z}$ é idêntica à classe de congruência $[a]_n$.

Demonstração. Para provar que os dois conjuntos são idênticos, devemos mostrar que cada um está contido no outro.

Prova de que $a + n\mathbb{Z} \subseteq [a]_n$: Seja x um elemento arbitrário da classe lateral $a + n\mathbb{Z}$. Por definição, existe um inteiro k tal que:

$$x = a + n \cdot k$$

Subtraindo a de ambos os lados, obtemos $x - a = n \cdot k$. Pela definição de divisibilidade em $\mathbb{Z}$, isso significa que $n \mid (x - a)$. Por sua vez, a definição de congruência nos diz que, se $n \mid (x - a)$, então $x \equiv a \pmod{n}$. Portanto, x pertence à classe de congruência $[a]_n$. Como x foi um elemento arbitrário, concluímos que $a + n\mathbb{Z} \subseteq [a]_n$.

Prova de que $[a]_n \subseteq a + n\mathbb{Z}$: Agora, seja y um elemento arbitrário da classe de congruência $[a]_n$. Por definição, $y \equiv a \pmod{n}$, o que significa que $n \mid (y - a)$. Pela

definição de divisibilidade, existe um inteiro j tal que:

$$y - a = n \cdot j$$

Adicionando a a ambos os lados, temos $y = a + n \cdot j$. Esta expressão mostra que y tem a forma de um elemento da classe lateral $a + n\mathbb{Z}$. Como y foi um elemento arbitrário, concluímos que $[a]_n \subseteq a + n\mathbb{Z}$.

Como provamos a inclusão em ambos os sentidos, os conjuntos são idênticos. □

Esta proposição revela a natureza do grupo quociente $\mathbb{Z}/n\mathbb{Z}$: seus elementos são as classes de congruência. Agora, provaremos que a estrutura do grupo quociente é idêntica à do grupo $(\mathbb{Z}_n, +)$, que já foi definido com base na aritmética modular.

Proposição 2.7.22. O grupo quociente $(\mathbb{Z}/n\mathbb{Z}, +)$ é isomórfico ao grupo dos inteiros módulo n, $(\mathbb{Z}_n, +)$.

Demonstração. Para provar o isomorfismo, definimos a função $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ da seguinte maneira:

$$\phi(k + n\mathbb{Z}) = [k]_n$$

Devemos mostrar que ϕ é um homomorfismo bijetivo e bem-definido.

A função é bem-definida: Suponha que duas classes laterais sejam iguais, $a + n\mathbb{Z} = b + n\mathbb{Z}$. Isso implica que $a - b \in n\mathbb{Z}$, ou seja, $a - b$ é um múltiplo de n. Pela definição de congruência, $a \equiv b \pmod{n}$, o que significa que as classes de congruência $[a]_n$ e $[b]_n$ são idênticas. Assim, $\phi(a + n\mathbb{Z}) = [a]_n = [b]_n = \phi(b + n\mathbb{Z})$, e a função não depende do representante escolhido.

A função é um homomorfismo: Devemos verificar se ϕ preserva a operação de grupo, $\phi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) = \phi(a + n\mathbb{Z}) + \phi(b + n\mathbb{Z})$. Sejam $a + n\mathbb{Z}$ e $b + n\mathbb{Z}$ dois elementos de $\mathbb{Z}/n\mathbb{Z}$.

- **Lado Esquerdo:** $\phi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) = \phi((a + b) + n\mathbb{Z}) = [a + b]_n$.
- **Lado Direito:** $\phi(a + n\mathbb{Z}) + \phi(b + n\mathbb{Z}) = [a]_n + [b]_n = [a + b]_n$. Como ambos os lados são iguais, a função é um homomorfismo.

A função é uma bijeção:

- **Injetividade:** Suponha $\phi(a + n\mathbb{Z}) = \phi(b + n\mathbb{Z})$. Isso implica $[a]_n = [b]_n$, que por sua vez significa $a \equiv b \pmod{n}$. Daí, $a - b$ é um múltiplo de n, então $a - b \in n\mathbb{Z}$, o que garante que $a + n\mathbb{Z} = b + n\mathbb{Z}$. A função é injetiva.

- **Sobrejetividade:** Para qualquer classe de congruência $[k]_n \in \mathbb{Z}_n$, existe uma classe lateral correspondente, $k + n\mathbb{Z}$, tal que $\phi(k + n\mathbb{Z}) = [k]_n$. A função é sobrejetiva.

Como ϕ é um homomorfismo bijetivo, ela é um isomorfismo, e concluímos que $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. O grupo quociente formado ao particionar a linha infinita dos inteiros ($\mathbb{Z}$) pelo subgrupo dos múltiplos de n ($n\mathbb{Z}$) resulta em uma estrutura finita de n elementos que é, algebricamente, idêntica ao grupo dos inteiros módulo n. □

2.8 Homomorfismos de Grupos

Assim como o conceito de isomorfismo nos permite afirmar que duas estruturas são algebricamente idênticas, a noção de homomorfismo nos permite descrever mapeamentos que preservam a estrutura entre grupos, mesmo que eles não sejam idênticos. Um homomorfismo revela uma relação fundamental entre a operação de um grupo e a de outro.

Definição 2.8.1 (Homomorfismo de Grupos)**.** Sejam $(G, *)$ e $(H, \#)$ dois grupos. Uma função $f : G \to H$ é chamada de **homomorfismo de grupos** se, para quaisquer elementos $a, b \in G$, a seguinte identidade é satisfeita:

$$f(a * b) = f(a) \# f(b)$$

Em outras palavras, operar os elementos em G e depois aplicar a função f ao resultado é o mesmo que aplicar f a cada elemento primeiro e depois operar os resultados em H.

Exemplo 2.8.1.

- **O Homomorfismo Trivial:** Para quaisquer grupos G e H, a função $f(g) = e_H$ para todo $g \in G$, onde e_H é o elemento identidade de H, é sempre um homomorfismo.
- **A Projeção Canônica:** Sejam o grupo dos inteiros $(\mathbb{Z}, +)$ e o grupo dos inteiros módulo n, $(\mathbb{Z}_n, +)$. A função de projeção $\pi : \mathbb{Z} \to \mathbb{Z}_n$ definida por $\pi(k) = [k]_n$ é um homomorfismo. Para quaisquer $a, b \in \mathbb{Z}$:

  $$\pi(a + b) = [a + b]_n = [a]_n + [b]_n = \pi(a) + \pi(b)$$

  A igualdade se deve à própria definição de adição em $\mathbb{Z}_n$.

2.8.1 Propriedades Fundamentais

Proposição 2.8.1. Seja $f : G \to H$ um homomorfismo de grupos. Então:

1. f mapeia o elemento identidade de G para o elemento identidade de H, ou seja, $f(e_G) = e_H$.

2. f mapeia o inverso de um elemento para o inverso de sua imagem, ou seja, $f(g^{-1}) = [f(g)]^{-1}$ para todo $g \in G$.

Demonstração.

1. Temos que $e_G = e_G * e_G$. Aplicando f a ambos os lados, obtemos:

$$f(e_G) = f(e_G * e_G) = f(e_G)\#f(e_G)$$

   Seja $y = f(e_G) \in H$. A equação é $y = y\#y$. Multiplicando ambos os lados à esquerda pelo inverso y^{-1} em H, temos:

$$y^{-1}\#y = y^{-1}\#(y\#y) \implies e_H = (y^{-1}\#y)\#y \implies e_H = e_H\#y \implies e_H = y$$

   Portanto, $f(e_G) = e_H$.

2. Pela definição de inverso em G, sabemos que:

$$g * g^{-1} = e_G \quad \text{e} \quad g^{-1} * g = e_G$$

   Aplicando o homomorfismo f a ambas as equações:

$$f(g * g^{-1}) = f(e_G) \quad \text{e} \quad f(g^{-1} * g) = f(e_G)$$

   Usando $f(a * b) = f(a)\#f(b)$ e o fato de que $f(e_G) = e_H$:

$$f(g)\#f(g^{-1}) = e_H \quad \text{e} \quad f(g^{-1})\#f(g) = e_H$$

   Estas duas equações mostram que o elemento $f(g^{-1})$ satisfaz as condições necessárias para ser o inverso do elemento $f(g)$ no grupo H. Como o inverso em um grupo é único, concluímos que:

$$f(g^{-1}) = [f(g)]^{-1}$$

□

2.8.2 Núcleo e Imagem

Associados a todo homomorfismo, existem dois subconjuntos fundamentais: o núcleo (ou kernel), que descreve o que é perdido ou colapsado pelo mapeamento, e a imagem, que descreve o que é alcançado.

Definição 2.8.2 (Núcleo e Imagem)**.** Seja $f : G \to H$ um homomorfismo de grupos.

- O **núcleo** (ou **kernel**) de f, denotado por $\ker(f)$, é o conjunto de todos os elementos em G que são mapeados para o elemento identidade de H.

$$\ker(f) = \{g \in G \mid f(g) = e_H\}$$

- A **imagem** de f, denotada por $\mathrm{Im}(f)$, é o subconjunto de H que consiste em todas as imagens de elementos de G.

$$\mathrm{Im}(f) = \{f(g) \mid g \in G\}$$

A importância destes conjuntos reside no fato de que eles próprios formam subgrupos, com o núcleo tendo a propriedade adicional de ser um subgrupo normal.

Proposição 2.8.2. Seja $f : G \to H$ um homomorfismo de grupos.

1. A imagem, $\mathrm{Im}(f)$, é um subgrupo de H.
2. O núcleo, $\ker(f)$, é um subgrupo **normal** de G.

Demonstração.

1. **Prova de que $\mathrm{Im}(f)$ é um subgrupo de H:** Usaremos o critério de subgrupo. Primeiro, $\mathrm{Im}(f)$ é não vazio, pois $e_G \in G$, então $f(e_G) = e_H \in \mathrm{Im}(f)$. Agora, sejam $h_1, h_2 \in \mathrm{Im}(f)$. Por definição, existem $g_1, g_2 \in G$ tais que $f(g_1) = h_1$ e $f(g_2) = h_2$.

   - *Fechamento:* $h_1 \# h_2 = f(g_1) \# f(g_2) = f(g_1 * g_2)$. Como $g_1 * g_2 \in G$, o resultado $h_1 \# h_2$ está na imagem.
   - *Inversos:* $h_1^{-1} = [f(g_1)]^{-1} = f(g_1^{-1})$. Como $g_1^{-1} \in G$, o resultado h_1^{-1} está na imagem.

   Portanto, $\mathrm{Im}(f)$ é um subgrupo de H.

2. **Prova de que $\ker(f)$ é um subgrupo normal de G:** Primeiro, provamos que é um subgrupo.
   É não vazio, pois $f(e_G) = e_H$, então $e_G \in \ker(f)$. Sejam $k_1, k_2 \in \ker(f)$, o que significa que $f(k_1) = e_H$ e $f(k_2) = e_H$.

   - *Fechamento:* $f(k_1 * k_2) = f(k_1) \# f(k_2) = e_H \# e_H = e_H$. Logo, $k_1 * k_2 \in \ker(f)$.
   - *Inversos:* $f(k_1^{-1}) = [f(k_1)]^{-1} = e_H^{-1} = e_H$. Logo, $k_1^{-1} \in \ker(f)$.

Assim, $\ker(f)$ é um subgrupo de G. Para provar a normalidade, usamos o critério de conjugação. Devemos mostrar que, para qualquer $g \in G$ e qualquer $k \in \ker(f)$, o elemento $g * k * g^{-1}$ também pertence ao núcleo.

$$f(g * k * g^{-1}) = f(g) \# f(k) \# f(g^{-1})$$

Como $k \in \ker(f)$, $f(k) = e_H$. A expressão se torna:

$$f(g) \# e_H \# f(g^{-1}) = f(g) \# [f(g)]^{-1} = e_H$$

Como $f(g * k * g^{-1}) = e_H$, o elemento $g * k * g^{-1}$ pertence, por definição, a $\ker(f)$. Portanto, $\ker(f)$ é um subgrupo normal de G.

□

Proposição 2.8.3 (Todo Subgrupo Normal é um Núcleo)**.** Seja N um subgrupo normal de um grupo G. Então, N é o núcleo do homomorfismo canônico $\pi : G \to G/N$, definido por $\pi(g) = gN$.

Demonstração. Seja $N \triangleleft G$. Consideremos o grupo quociente $G/N = \{gN \mid g \in G\}$, cuja operação é $(aN)(bN) = (ab)N$, e o elemento identidade é $e_G N = N$. Definimos a função $\pi : G \to G/N$ como $\pi(g) = gN$.

π **é um homomorfismo:** Devemos mostrar que $\pi(g_1 * g_2) = \pi(g_1) * \pi(g_2)$ para quaisquer $g_1, g_2 \in G$.

- Lado Esquerdo: $\pi(g_1 * g_2) = (g_1 * g_2)N$.
- Lado Direito: $\pi(g_1) * \pi(g_2) = (g_1 N) * (g_2 N)$. Pela definição da operação em G/N, $(g_1 N) * (g_2 N) = (g_1 * g_2)N$.

Como os dois lados são iguais, π é um homomorfismo.

Núcleo de π: O núcleo de π, $\ker(\pi)$, é o conjunto de todos os elementos $g \in G$ que são mapeados para o elemento identidade de G/N. O elemento identidade em G/N é a classe lateral N.

$$\ker(\pi) = \{g \in G \mid \pi(g) = N\}$$

Substituindo a definição de π:

$$\ker(\pi) = \{g \in G \mid gN = N\}$$

Vamos demonstrar que $\ker(\pi) = N$ por dupla inclusão:

- ($\subseteq$) Seja $g \in \ker(\pi)$. Então, por definição, $gN = N$. Sabemos que o elemento identidade e pertence ao subgrupo N. Logo, o elemento $g = g * e$ deve pertencer ao conjunto gN. Como $gN = N$, concluímos que $g \in N$. Portanto, $\ker(\pi) \subseteq N$.

- ($\supseteq$) Seja $n \in N$. Queremos mostrar que $n \in \ker(\pi)$, ou seja, que $\pi(n) = N$. Isso equivale a mostrar que $nN = N$. Como N é um subgrupo, ele é fechado sob a operação do grupo. Assim, para qualquer $h \in N$, o produto $n * h$ continua pertencendo a N. Isso implica que $nN \subseteq N$. (Analogamente, $N \subseteq nN$ pela multiplicação por n^{-1}). Dessa forma, $nN = N$, o que significa que $\pi(n) = N$. Portanto, $N \subseteq \ker(\pi)$.

Como provamos ambas as inclusões, concluímos que $\ker(\pi) = N$. Isso prova que o núcleo do homomorfismo canônico π é precisamente o subgrupo normal N. □

O núcleo de um homomorfismo não é apenas um subgrupo normal; ele também nos fornece uma maneira direta de determinar se o homomorfismo é injetivo.

Proposição 2.8.4. Um homomorfismo de grupos $f : G \to H$ é injetivo se, e somente se, seu núcleo é o subgrupo trivial, ou seja, $\ker(f) = \{e_G\}$.

Demonstração. Como esta é uma declaração de equivalência, devemos provar as duas implicações.

($\Rightarrow$) Se f é injetivo, então $\ker(f) = \{e_G\}$.

Assumimos como hipótese que f é injetivo. Por definição, o núcleo de f é o conjunto $\{g \in G \mid f(g) = e_H\}$. Seja k um elemento qualquer do núcleo, $k \in \ker(f)$. Isso significa que $f(k) = e_H$.

Já provamos que todo homomorfismo mapeia o elemento identidade para o elemento identidade, ou seja, $f(e_G) = e_H$. Agora, temos dois elementos, k e e_G, que são mapeados para o mesmo resultado:

$$f(k) = f(e_G) = e_H$$

Como nossa hipótese é que f é injetivo, se as imagens são iguais, os elementos originais devem ser iguais. Portanto,

$$k = e_G$$

Isso mostra que o único elemento que pode pertencer ao núcleo é a própria identidade. Logo, $\ker(f) = \{e_G\}$.

($\Leftarrow$) Se $\ker(f) = \{e_G\}$, então f é injetivo.

Agora, assumimos como hipótese que o núcleo de f é trivial. Para provar que f é injetivo, devemos mostrar que, para quaisquer $a, b \in G$, a condição $f(a) = f(b)$ implica que $a = b$.

Seja $f(a) = f(b)$. Vamos multiplicar ambos os lados da equação à direita pelo inverso de $f(b)$ em H, que é $[f(b)]^{-1}$.

$$f(a)\#[f(b)]^{-1} = f(b)\#[f(b)]^{-1}$$

$$f(a)\#[f(b)]^{-1} = e_H$$

Como f é um homomorfismo, sabemos que $[f(b)]^{-1} = f(b^{-1})$. Substituindo no lado esquerdo:

$$f(a)\#f(b^{-1}) = f(a * b^{-1})$$

A equação se torna:

$$f(a * b^{-1}) = e_H$$

Pela definição do núcleo, se a imagem de um elemento é a identidade de H, então este elemento deve pertencer ao núcleo de f. Portanto:

$$a * b^{-1} \in \ker(f)$$

Agora, usamos nossa hipótese: o núcleo contém apenas o elemento identidade. Logo, a única possibilidade é:

$$a * b^{-1} = e_G$$

Multiplicando ambos os lados à direita por b:

$$(a * b^{-1}) * b = e_G * b$$

$$a * (b^{-1} * b) = b$$

$$a * e_G = b \implies a = b$$

Como a premissa $f(a) = f(b)$ nos levou à conclusão de que $a = b$, provamos que a função f é injetiva. □

Exemplo 2.8.2 (Análise do Homomorfismo de Projeção Canônica)**.** Consideremos os grupos $G = (\mathbb{Z}, +)$ e $H = (\mathbb{Z}_n, +)$. A função $\pi : \mathbb{Z} \to \mathbb{Z}_n$ é definida por:

$$\pi(k) = [k]_n$$

Como já foi estabelecido, esta função é um homomorfismo, pois $\pi(a + b) = [a + b]_n = [a]_n + [b]_n = \pi(a) + \pi(b)$. Agora, vamos investigar detalhadamente sua imagem e seu núcleo.

Análise da Imagem Im(π)

A imagem de π é, por definição, o conjunto de todas as classes de congruência que são

alcançadas pela função:

$$\text{Im}(\pi) = \{\pi(k) \mid k \in \mathbb{Z}\} = \{[k]_n \mid k \in \mathbb{Z}\}$$

Nosso objetivo é mostrar que a imagem é o próprio grupo $\mathbb{Z}_n$. O conjunto $\mathbb{Z}_n$ é formado pelas n classes de equivalência distintas, representadas por $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

Para provar que o mapeamento é sobrejetivo (e, portanto, que a imagem é todo o contradomínio), devemos mostrar que cada uma dessas classes em $\mathbb{Z}_n$ é a imagem de algum inteiro em $\mathbb{Z}$.

Seja $[j]_n$ uma classe arbitrária em $\mathbb{Z}_n$, onde j é um inteiro tal que $0 \leq j < n$. O próprio inteiro j é um elemento do domínio $\mathbb{Z}$. Ao aplicarmos a função π a este inteiro j, obtemos:

$$\pi(j) = [j]_n$$

Como para qualquer classe $[j]_n \in \mathbb{Z}_n$ fomos capazes de encontrar um elemento $j \in \mathbb{Z}$ que a mapeia, a função é sobrejetiva. Consequentemente, a imagem do homomorfismo é o grupo inteiro:

$$\text{Im}(\pi) = \mathbb{Z}_n$$

Análise do Núcleo $\ker(\pi)$

O núcleo de π é, por definição, o conjunto de todos os elementos do domínio ($\mathbb{Z}$) que são mapeados para o elemento identidade do contradomínio ($\mathbb{Z}_n$). O elemento identidade em $(\mathbb{Z}_n, +)$ é a classe $[0]_n$.

$$\ker(\pi) = \{k \in \mathbb{Z} \mid \pi(k) = [0]_n\}$$

Vamos desdobrar a condição de pertencimento ao núcleo:

1. A condição $\pi(k) = [0]_n$ é, pela definição da função, o mesmo que $[k]_n = [0]_n$.
2. A igualdade de classes de congruência $[k]_n = [0]_n$ significa, por definição, que k é congruente a 0 módulo n, ou seja, $k \equiv 0 \pmod{n}$.
3. A relação de congruência $k \equiv 0 \pmod{n}$ significa, por sua vez, que n divide a diferença $(k - 0)$, ou seja, $n \mid k$.
4. Finalmente, a condição de divisibilidade $n \mid k$ significa que existe um inteiro j tal que $k = n \cdot j$.

O conjunto de todos os inteiros k que podem ser escritos na forma $n \cdot j$ é precisamente a definição do conjunto dos múltiplos de n, que é o subgrupo $n\mathbb{Z}$. Portanto, concluímos que:

$$\ker(\pi) = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

Esta análise se conecta com as proposições anteriores. Como já provado, o núcleo de qualquer homomorfismo de grupo é sempre um subgrupo normal. Nossa descoberta de que $\ker(\pi) = n\mathbb{Z}$ nos fornece uma confirmação de que $n\mathbb{Z}$ é um subgrupo normal de $\mathbb{Z}$, um fato que já conhecíamos, pois $\mathbb{Z}$ é abeliano.

2.8.3 O Teorema Fundamental dos Homomorfismos

Como já provamos, o núcleo de qualquer homomorfismo, $\ker(f)$, é sempre um subgrupo normal do domínio. Isso nos permite formar o grupo quociente $G/\ker(f)$. O próximo teorema, frequentemente chamado de Teorema do Isomorfismo, revela que a estrutura deste grupo quociente é precisamente a mesma da imagem do homomorfismo.

Teorema 2.8.1 (Teorema Fundamental dos Homomorfismos de Grupos)**.** Seja $f : (G, *) \to (H, \#)$ um homomorfismo de grupos. Então, o grupo quociente $G/\ker(f)$ é isomórfico à imagem de f, $\mathrm{Im}(f)$. Formalmente:

$$G/\ker(f) \cong \mathrm{Im}(f)$$

Demonstração. Para provar este teorema, devemos construir uma função $\phi : G/\ker(f) \to \mathrm{Im}(f)$ e demonstrar que ela é um isomorfismo, ou seja, que é um homomorfismo bijetivo e bem-definido. Seja $K = \ker(f)$ para simplificar a notação.

Definição da Função:

Os elementos do domínio G/K são as classes laterais gK, e os elementos do contradomínio $\mathrm{Im}(f)$ são os elementos da forma $f(g)$. Uma função que conecta esses dois conjuntos é:

$$\phi(gK) = f(g)$$

A Função é Bem-Definida:

A definição de ϕ depende do representante g escolhido para a classe lateral gK. Devemos mostrar que, se escolhermos um representante diferente para a mesma classe, o resultado da função não se altera. Suponha que $gK = g'K$ para $g, g' \in G$. Pela propriedade das classes laterais, isso significa que $g' = g * k$ para algum $k \in K$. Aplicando ϕ à classe $g'K$, temos:

$$\phi(g'K) = f(g') = f(g * k)$$

Como f é um homomorfismo, $f(g * k) = f(g)\#f(k)$. Mas, como $k \in K = \ker(f)$, por definição, $f(k) = e_H$. Portanto:

$$f(g)\#f(k) = f(g)\#e_H = f(g)$$

Assim, $\phi(g'K) = f(g)$. Como também tínhamos $\phi(gK) = f(g)$, mostramos que

$\phi(g'K) = \phi(gK)$. A função ϕ está bem-definida.

A Função é um Homomorfismo:

Devemos mostrar que ϕ preserva a operação de grupo. Sejam aK e bK duas classes laterais em G/K.

$$\begin{aligned}
\phi((aK) * (bK)) &= \phi((a * b)K) && \text{(Definição da operação em } G/K) \\
&= f(a * b) && \text{(Definição de } \phi) \\
&= f(a)\#f(b) && \text{(Pois } f \text{ é um homomorfismo)} \\
&= \phi(aK)\#\phi(bK) && \text{(Definição de } \phi)
\end{aligned}$$

A cadeia de igualdades mostra que ϕ é um homomorfismo.

A Função é Injetiva:

Devemos mostrar que, se $\phi(aK) = \phi(bK)$, então $aK = bK$. A igualdade $\phi(aK) = \phi(bK)$ implica, pela definição de ϕ, que $f(a) = f(b)$. Multiplicando ambos os lados à direita pelo inverso de $f(b)$ em H:

$$f(a)\#[f(b)]^{-1} = e_H$$

Como f é um homomorfismo, $[f(b)]^{-1} = f(b^{-1})$. A equação se torna:

$$f(a)\#f(b^{-1}) = f(a * b^{-1}) = e_H$$

Pela definição do núcleo, a condição $f(a * b^{-1}) = e_H$ implica que o elemento $a * b^{-1}$ pertence a K. Se $a * b^{-1} = k$ para algum $k \in K$, então podemos escrever $a = k * b$. Isso demonstra que a é um elemento da classe lateral à direita Kb. Como o núcleo K é um subgrupo normal, sabemos que $Kb = bK$, e portanto, a também é um elemento da classe lateral à esquerda bK. Conforme provado na proposição sobre a partição de um grupo, se duas classes laterais (neste caso, aK e bK) possuem um elemento em comum (o elemento a), elas devem ser idênticas. Portanto, $aK = bK$, e a função ϕ é injetiva.

A Função é Sobrejetiva:

Devemos mostrar que, para todo elemento h no contradomínio $\mathrm{Im}(f)$, existe um elemento no domínio G/K que é mapeado para ele. Seja $h \in \mathrm{Im}(f)$ um elemento arbitrário. Pela definição da imagem, deve existir um $g \in G$ tal que $f(g) = h$. A classe lateral gK é um elemento do domínio G/K. Aplicando ϕ a esta classe, obtemos:

$$\phi(gK) = f(g) = h$$

Encontramos um elemento no domínio que mapeia para h. Portanto, a função ϕ é sobrejetiva.

Como a função ϕ é um homomorfismo bijetivo, ela é um isomorfismo. Isso conclui a prova de que $G/\ker(f) \cong \text{Im}(f)$. □

Exemplo 2.8.3. O Teorema Fundamental dos Homomorfismos nos fornece uma maneira de reafirmar a conexão entre o grupo quociente $\mathbb{Z}/n\mathbb{Z}$ e o grupo dos inteiros módulo n, $(\mathbb{Z}_n, +)$, que foi provada diretamente na seção anterior.

Vamos analisar a aplicação do teorema ao homomorfismo de projeção canônica.

- **O Homomorfismo:** Considere os grupos $G = (\mathbb{Z}, +)$ e $H = (\mathbb{Z}_n, +)$. Como já estabelecido, a função $\pi : \mathbb{Z} \to \mathbb{Z}_n$ definida por $\pi(k) = [k]_n$ é um homomorfismo de grupos.

- **O Núcleo:** O núcleo de π é o conjunto de todos os inteiros $k \in \mathbb{Z}$ que são mapeados para o elemento identidade de $\mathbb{Z}_n$, que é a classe $[0]_n$.

  $$\ker(\pi) = \{k \in \mathbb{Z} \mid \pi(k) = [0]_n\}$$

  A condição $\pi(k) = [k]_n = [0]_n$ é, por definição, a mesma que a congruência $k \equiv 0 \pmod{n}$. Isso significa que n deve dividir k, ou seja, k deve ser um múltiplo de n. Portanto, o núcleo é precisamente o subgrupo dos múltiplos de n:

  $$\ker(\pi) = n\mathbb{Z}$$

- **A Imagem:** A imagem de π é o conjunto de todas as classes de congruência em $\mathbb{Z}_n$ que são alcançadas pela função. Para qualquer classe $[k]_n \in \mathbb{Z}_n$, o próprio inteiro k é um elemento de $\mathbb{Z}$ tal que $\pi(k) = [k]_n$. Isso significa que toda classe em $\mathbb{Z}_n$ é a imagem de algum elemento de $\mathbb{Z}$, e a função é sobrejetiva. Portanto, a imagem é o próprio grupo $\mathbb{Z}_n$:

  $$\text{Im}(\pi) = \mathbb{Z}_n$$

- **Aplicação do Teorema:** O Teorema Fundamental dos Homomorfismos afirma que $G/\ker(f) \cong \text{Im}(f)$. Substituindo os componentes que identificamos:

  $$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Este resultado confirma, a partir de uma perspectiva mais abstrata, o que demonstramos anteriormente: a estrutura algébrica que emerge ao particionar o grupo dos inteiros $\mathbb{Z}$ pelo seu subgrupo normal $n\mathbb{Z}$ é isomorfa (algebricamente idêntica) à estrutura do grupo dos inteiros módulo n, $\mathbb{Z}_n$.

Teorema 2.8.2 (Teorema de Cayley)**.** Todo grupo $(G, *)$ é isomórfico a um subgrupo do grupo de permutações de seus elementos, S_G.

Demonstração. A prova consiste em construir um homomorfismo injetivo Φ do grupo G para o grupo simétrico S_G. Pelo Teorema Fundamental dos Homomorfismos, isso garantirá que G é isomórfico à imagem de Φ, que é um subgrupo de S_G.

Construção das Permutações:

Para cada elemento $g \in G$, definimos uma função "multiplicação à esquerda por g", denotada por $\lambda_g : G \to G$, da seguinte forma:

$$\lambda_g(x) = g * x \quad \text{para todo } x \in G$$

Nosso primeiro passo é provar que cada função λ_g é uma permutação dos elementos de G, ou seja, uma bijeção de G em si mesmo.

- **Injetividade:** Suponha que $\lambda_g(x) = \lambda_g(y)$ para $x, y \in G$. Pela definição, isso significa $g*x = g*y$. Pela lei do cancelamento à esquerda, que é válida em qualquer grupo, podemos concluir que $x = y$. Portanto, λ_g é injetiva.

- **Sobrejetividade:** Seja y um elemento arbitrário de G. Precisamos encontrar um $x \in G$ tal que $\lambda_g(x) = y$. Considere o elemento $x = g^{-1} * y$, que pertence a G. Aplicando λ_g a este elemento, temos:

$$\lambda_g(g^{-1} * y) = g * (g^{-1} * y) = (g * g^{-1}) * y = e_G * y = y$$

  Como para todo y encontramos um x correspondente, a função λ_g é sobrejetiva.

Como λ_g é uma bijeção, ela é, por definição, um elemento do grupo simétrico S_G.

Construção do Homomorfismo:

Agora, definimos uma função $\Phi : G \to S_G$ que mapeia cada elemento g de G à sua permutação correspondente:

$$\Phi(g) = \lambda_g$$

Vamos provar que Φ é um homomorfismo de grupos. A operação em S_G é a composição de funções, $\circ$. Devemos mostrar que $\Phi(g * h) = \Phi(g) \circ \Phi(h)$.

- O lado esquerdo é $\Phi(g * h) = \lambda_{g*h}$.

- O lado direito é $\Phi(g) \circ \Phi(h) = \lambda_g \circ \lambda_h$.

Para verificar se as funções λ_{g*h} e $\lambda_g \circ \lambda_h$ são idênticas, as aplicamos a um elemento arbitrário $x \in G$:

$$\lambda_{g*h}(x) = (g * h) * x$$

$$(\lambda_g \circ \lambda_h)(x) = \lambda_g(\lambda_h(x)) = \lambda_g(h * x) = g * (h * x)$$

Pela propriedade associativa da operação $*$ em G, temos que $(g * h) * x = g * (h * x)$. Como as duas funções produzem o mesmo resultado para qualquer entrada, elas são idênticas. Portanto, Φ é um homomorfismo.

Injetividade do Homomorfismo:

Para provar que Φ é injetivo, mostraremos que seu núcleo é o subgrupo trivial $\{e_G\}$. O núcleo de Φ é o conjunto de todos os elementos $g \in G$ que são mapeados para o elemento identidade de S_G, que é a permutação identidade.

$$\ker(\Phi) = \{g \in G \mid \Phi(g) = \mathrm{id}_G\}$$

A condição $\Phi(g) = \mathrm{id}_G$ significa que $\lambda_g(x) = x$ para todo $x \in G$. Pela definição de λ_g, isso é:

$$g * x = x \quad \text{para todo } x \in G$$

Se $x = e_G$ temos que $g * e_G = e_G$ Assim, a única forma de esta igualdade ser verdadeira para todos os x em um grupo é se g for o elemento identidade, e_G. Portanto, $\ker(\Phi) = \{e_G\}$. Como o núcleo é trivial, o homomorfismo Φ é injetivo.

Conclusão pelo Teorema Fundamental:

Construímos um homomorfismo injetivo $\Phi : G \to S_G$. Pelo Teorema Fundamental dos Homomorfismos, sabemos que $G/\ker(\Phi) \cong \mathrm{Im}(\Phi)$.

- Como $\ker(\Phi) = \{e_G\}$, o grupo quociente $G/\{e_G\}$ é trivialmente isomórfico ao próprio G.
- A imagem, $\mathrm{Im}(\Phi)$, é um subgrupo do contradomínio, S_G.

Portanto, concluímos que $G \cong \mathrm{Im}(\Phi)$, onde $\mathrm{Im}(\Phi)$ é um subgrupo de S_G. Isso prova o teorema.

Em especial todo grupo finito de ordem n, é isomórfico a um subgrupo de S_n. □

2.9 A Estrutura de Anel em $\mathbb{Z}$

Até agora, analisamos o conjunto dos inteiros $\mathbb{Z}$ sob a ótica da teoria de grupos, focando na estrutura fornecida pela operação de adição, $(\mathbb{Z}, +)$. O próximo passo é incorporar a operação de multiplicação para estudar a estrutura algébrica completa de $(\mathbb{Z}, +, \cdot)$.

2.9.1 Definição e Exemplos de Anéis

Definição 2.9.1 (Anel)**.** Um **anel** é um conjunto não vazio A munido de duas operações binárias, denotadas por $+$ (adição) e $\cdot$ (multiplicação), que satisfazem os seguintes axiomas:

1. $(A, +)$ é um **grupo abeliano**. Isso implica que a adição é associativa, comutativa, possui um elemento neutro (0) e todo elemento possui um inverso aditivo.
2. A multiplicação é **associativa**: para quaisquer $a, b, c \in A$,
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
3. A multiplicação é **distributiva** sobre a adição: para quaisquer $a, b, c \in A$,
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{(Distributividade à esquerda)}$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad \text{(Distributividade à direita)}$$

Definição 2.9.2 (Anel Comutativo com Unidade)**.**

- Um anel $(A, +, \cdot)$ é dito **comutativo** se a operação de multiplicação for comutativa.
- Um anel é dito um **anel com unidade** se existir um elemento identidade para a multiplicação, denotado por 1, tal que $1 \cdot a = a \cdot 1 = a$ para todo $a \in A$.

O principal exemplo que motiva nosso estudo é o próprio conjunto dos inteiros.

Proposição 2.9.1. O conjunto dos números inteiros com as operações de adição e multiplicação, $(\mathbb{Z}, +, \cdot)$, forma um anel comutativo com unidade.

Demonstração. Devemos verificar se todos os axiomas são satisfeitos.

1. Conforme exaustivamente demonstrado nesse capítulo, $(\mathbb{Z}, +)$ é um grupo abeliano, com o 0 como elemento neutro e $-a$ como o inverso aditivo de a.
2. A associatividade da multiplicação em $\mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, é uma propriedade herdada da mesma propriedade já provada para os números naturais.
3. A distributividade da multiplicação sobre a adição, $a \cdot (b + c) = a \cdot b + a \cdot c$, também foi demonstrada na construção das operações em $\mathbb{Z}$.

Adicionalmente:

- A multiplicação em $\mathbb{Z}$ é comutativa ($a \cdot b = b \cdot a$).
- O número 1 atua como o elemento identidade para a multiplicação.

Como todas as condições são satisfeitas, $(\mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade. □

Exemplo 2.9.1 (Outros Anéis)**.**

- **O Anel dos Inteiros Módulo n:** O conjunto $(\mathbb{Z}_n, +, \cdot)$ das classes de congruência módulo n forma um anel comutativo com unidade. As propriedades de associatividade, comutatividade e distributividade são herdadas das operações correspondentes em $\mathbb{Z}$. O elemento $[0]_n$ é a identidade aditiva e $[1]_n$ é a identidade multiplicativa.

  No caso particular em que $n = 1$, o conjunto $\mathbb{Z}_1$ possui apenas um elemento: a classe $\{[0]_1\}$. Neste anel, temos a peculiaridade de que a identidade multiplicativa é igual à identidade aditiva ($[1]_1 = [0]_1$). Um anel no qual isso acontece é denominado **anel nulo** ou **anel trivial**.

- **Um Anel sem Unidade:** O conjunto dos inteiros pares, $(2\mathbb{Z}, +, \cdot)$, também forma um anel comutativo. Ele herda todas as propriedades de $\mathbb{Z}$, e as operações de adição e multiplicação são fechadas (a soma de dois pares é par, o produto de dois pares é par). No entanto, este anel não possui unidade, pois o elemento identidade da multiplicação, o 1, não é um número par e, portanto, não pertence ao conjunto $2\mathbb{Z}$.

2.9.2 Unidades e Divisores de Zero

A estrutura de anel nos permite analisar as propriedades multiplicativas dos elementos de uma forma mais rica do que na teoria de grupos. Duas classificações de elementos são particularmente importantes para entender a estrutura de um anel: os elementos que possuem inverso multiplicativo (unidades) e os elementos não nulos que, ao serem multiplicados por outro elemento não nulo, resultam em zero (divisores de zero).

Definição 2.9.3 (Unidade)**.** Seja $(A, +, \cdot)$ um anel com unidade 1. Um elemento $u \in A$ é chamado de **unidade** (ou elemento invertível) se existe um elemento $v \in A$ tal que:

$$u \cdot v = v \cdot u = 1$$

O elemento v é o inverso multiplicativo de u. O conjunto de todas as unidades de um anel A é denotado por $U(A)$.

Distinção de Terminologia

É importante atentar-se ao fato que apesar de usar o mesmo termo (unidade), estes são dois conceitos diferentes:

- **A Unidade Multiplicativa:** Refere-se a um *único e especial elemento* do anel, denotado por 1, cuja propriedade fundamental é ser o elemento neutro da

multiplicação para *todos* os elementos do anel ($1 \cdot a = a \cdot 1 = a$). Um anel pode ter ou não uma unidade multiplicativa, mas se tiver, ela é única, pois a estrutura multiplicativa $(A, \cdot)$ seria então um monoide. No anel dos inteiros $(\mathbb{Z}, +, \cdot)$, a unidade multiplicativa é o número 1.

- **As Unidades (ou Elementos Invertíveis):** Refere-se ao *conjunto de elementos* de um anel que possuem um inverso multiplicativo.

Proposição 2.9.2. No anel dos inteiros $(\mathbb{Z}, +, \cdot)$, as únicas unidades são 1 e -1.

Demonstração. Seja $u \in \mathbb{Z}$ uma unidade. Por definição, deve existir um $v \in \mathbb{Z}$ tal que $u \cdot v = 1$. Aplicando a função módulo (valor absoluto) a ambos os lados da equação, temos:

$$|u \cdot v| = |1| \implies |u| \cdot |v| = 1$$

Como u e v são inteiros, seus módulos, $|u|$ e $|v|$, são números naturais. A única forma de o produto de dois números naturais ser 1 é se ambos forem iguais a 1. Portanto:

$$|u| = 1 \quad \text{e} \quad |v| = 1$$

Os únicos inteiros u que satisfazem a condição $|u| = 1$ são $u = 1$ e $u = -1$.

- Se $u = 1$, seu inverso é $v = 1$, pois $1 \cdot 1 = 1$.
- Se $u = -1$, seu inverso é $v = -1$, pois $(-1) \cdot (-1) = 1$.

Logo, o conjunto das unidades de $\mathbb{Z}$ é $U(\mathbb{Z}) = \{1, -1\}$. □

Definição 2.9.4 (Divisor de Zero)**.** Seja $(A, +, \cdot)$ um anel. Um elemento não nulo $a \in A$ é chamado de **divisor de zero** se existe um outro elemento não nulo $b \in A$ tal que:

$$a \cdot b = 0 \quad \text{ou} \quad b \cdot a = 0$$

A ausência de divisores de zero é uma propriedade importante que $\mathbb{Z}$ herda dos números naturais, garantindo que a Lei do Cancelamento da multiplicação seja válida.

Proposição 2.9.3. O anel dos inteiros $(\mathbb{Z}, +, \cdot)$ não possui divisores de zero.

Demonstração. Para provar esta afirmação, devemos mostrar que se o produto de dois inteiros é zero, então pelo menos um deles deve ser zero. Sejam $a, b \in \mathbb{Z}$ tais que $a \cdot b = 0$.

Suponha, por contradição, que $a \neq 0$ e $b \neq 0$. Se $a \neq 0$, então seu módulo $|a|$ é um número natural estritamente positivo ($|a| \geq 1$). Da mesma forma, se $b \neq 0$, então $|b| \geq 1$. O módulo do produto é o produto dos módulos:

$$|a \cdot b| = |a| \cdot |b|$$

Como $|a| \geq 1$ e $|b| \geq 1$, e a ordem é compatível com a multiplicação, temos que $|a| \cdot |b| \geq 1 \cdot 1 = 1$. Isso implica que $|a \cdot b| \geq 1$, o que significa que o produto $a \cdot b$ não pode ser zero. Isso contradiz nossa hipótese inicial de que $a \cdot b = 0$. Portanto, a suposição de que ambos a e b são não nulos deve ser falsa. Concluímos que $a = 0$ ou $b = 0$. □

Exemplo 2.9.2 (O Anel $\mathbb{Z}_n$ e os Divisores de Zero)**.** Ao contrário de $\mathbb{Z}$, os anéis de inteiros módulo n podem possuir divisores de zero, especificamente quando n é um número composto. Consideremos o anel $(\mathbb{Z}_6, +, \cdot)$. Seus elementos são $\{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$. Neste anel, os elementos $[2]_6$ e $[3]_6$ são ambos diferentes do elemento nulo, $[0]_6$. No entanto, seu produto é:

$$[2]_6 \cdot [3]_6 = [2 \cdot 3]_6 = [6]_6 = [0]_6$$

Como encontramos dois elementos não nulos cujo produto é nulo, por definição, $[2]_6$ e $[3]_6$ são divisores de zero em $\mathbb{Z}_6$. Esta é uma diferença estrutural fundamental entre os anéis $\mathbb{Z}$ e $\mathbb{Z}_n$ (para n composto).

2.9.3 Domínios de Integridade

A ausência de divisores de zero é uma propriedade tão importante que os anéis que a possuem recebem uma classificação especial. Um domínio de integridade é, em essência, um anel onde a lei do cancelamento da multiplicação, familiar dos inteiros, continua válida.

Definição 2.9.5 (Domínio de Integridade)**.** Um **domínio de integridade** é um anel $(A, +, \cdot)$ que satisfaz simultaneamente três condições:

1. É um anel **comutativo**.
2. Possui **unidade** multiplicativa.
3. **Não possui divisores de zero**.

Com base no que já foi provado, a classificação de $\mathbb{Z}$ é uma consequência direta.

Proposição 2.9.4. O anel dos inteiros $(\mathbb{Z}, +, \cdot)$ é um domínio de integridade.

Demonstração. Conforme demonstrado nas subseções anteriores:

1. $(\mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade.
2. $(\mathbb{Z}, +, \cdot)$ não possui divisores de zero.

Como todas as condições da definição são satisfeitas, concluímos que $\mathbb{Z}$ é um domínio de integridade. □

A propriedade de não ter divisores de zero é equivalente à validade da lei do cancelamento para a multiplicação.

Proposição 2.9.5 (Lei do Cancelamento da Multiplicação)**.** Seja A um anel comutativo. Então, A é um domínio de integridade se, e somente se, para quaisquer $a, b, c \in A$ com $c \neq 0$, a igualdade $a \cdot c = b \cdot c$ implica $a = b$.

Demonstração. $(\Rightarrow)$ Suponha que A seja um domínio de integridade. Sejam $a, b, c \in A$ com $c \neq 0$ tais que $a \cdot c = b \cdot c$. Subtraindo $b \cdot c$ de ambos os lados, obtemos:

$$a \cdot c - b \cdot c = 0$$

Pela distributividade, podemos reescrever a expressão como:

$$(a - b) \cdot c = 0$$

Como A é um domínio de integridade, ele não possui divisores de zero. Uma vez que, por hipótese, $c \neq 0$, o outro fator na multiplicação deve ser zero. Portanto:

$$a - b = 0 \implies a = b$$

Isso prova que a lei do cancelamento é válida.

$(\Leftarrow)$ Agora, suponha que a lei do cancelamento seja válida em A. Devemos provar que A não possui divisores de zero. Sejam $x, y \in A$ tais que $x \cdot y = 0$. Suponha que $x \neq 0$. Nosso objetivo é mostrar que y deve ser 0. Podemos escrever a equação $x \cdot y = 0$ da seguinte forma, usando o fato de que $x \cdot 0 = 0$:

$$x \cdot y = x \cdot 0$$

Como, por hipótese, $x \neq 0$, podemos aplicar a lei do cancelamento (cancelando o x de ambos os lados). Isso nos leva diretamente à conclusão de que:

$$y = 0$$

Portanto, se o produto de dois elementos é zero e um deles não é zero, o outro deve ser zero. Isso significa que A não possui divisores de zero, e é um domínio de integridade. □

Outra propriedade estrutural importante de um domínio de integridade é sua característica.

Definição 2.9.6 (Característica de um Anel)**.** A **característica** de um anel com unidade

$(A, +, \cdot)$, denotada por $\text{char}(A)$, é o menor inteiro positivo n tal que

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ vezes}} = n \cdot 1 = 0$$

Se tal inteiro positivo não existe, dizemos que a característica é 0.

Observação: Considere o homomorfismo de anéis $\phi : \mathbb{Z} \to A$ definido por $\phi(k) = k \cdot 1_A$ (a soma de 1_A consigo mesmo k vezes, ou seu inverso aditivo se $k < 0$, ou 0_A se $k = 0$). O núcleo deste homomorfismo, $\ker(\phi) = \{k \in \mathbb{Z} \mid k \cdot 1_A = 0_A\}$, está diretamente relacionado à característica:

- Se $\text{char}(A) = n > 0$, então n é o menor inteiro positivo no núcleo, e $\ker(\phi) = n\mathbb{Z}$. Pelo Teorema do Isomorfismo para Anéis, a imagem $\text{Im}(\phi) = \{k \cdot 1_A \mid k \in \mathbb{Z}\}$ é um subanel de A isomórfico a $\mathbb{Z}/\ker(\phi) = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
- Se $\text{char}(A) = 0$, então $k \cdot 1_A = 0_A$ apenas para $k = 0$, logo $\ker(\phi) = \{0\}$. O Teorema do Isomorfismo implica que $\text{Im}(\phi)$ é um subanel de A isomórfico a $\mathbb{Z}/\{0\} \cong \mathbb{Z}$.

Portanto, todo anel com unidade contém um subanel que é isomórfico a $\mathbb{Z}_n$ (se $\text{char}(A) = n > 0$) ou a $\mathbb{Z}$ (se $\text{char}(A) = 0$). Isso faz de $\mathbb{Z}$ e $\mathbb{Z}_n$ os exemplos mais fundamentais de anéis comutativos com unidade, pois todo anel desta classe contém (uma cópia isomórfica de) um, e apenas um, deles.

Exemplo 2.9.3.

- O anel $\mathbb{Z}$ tem característica 0, pois a soma de qualquer quantidade números de 1s nunca resultará em 0.
- O anel $\mathbb{Z}_n$ tem característica n, pois $n \cdot [1]_n = [n]_n = [0]_n$, e nenhum inteiro positivo menor que n satisfaz essa condição.

Teorema 2.9.1. A característica de qualquer domínio de integridade é ou 0 ou um número primo.

Demonstração. Seja A um domínio de integridade. Se $\text{char}(A) = 0$, a afirmação é válida. Suponha, então, que a característica seja um inteiro positivo n. Devemos provar que n não pode ser um número composto.

Suponha, por contradição, que n seja composto. Isso significa que existem inteiros a, b tais que $n = ab$, com $1 < a < n$ e $1 < b < n$. Pela definição de característica, sabemos que $n \cdot 1 = 0$. Substituindo $n = ab$:

$$(ab) \cdot 1 = 0$$

Usando as propriedades de anel, podemos reescrever esta expressão como:

$$(a \cdot 1) \cdot (b \cdot 1) = 0$$

Como A é um domínio de integridade, ele não possui divisores de zero. Portanto, um dos fatores no produto acima deve ser zero:

$$a \cdot 1 = 0 \quad \text{ou} \quad b \cdot 1 = 0$$

No entanto, isso contradiz a definição de que n é o *menor* inteiro positivo para o qual $n \cdot 1 = 0$. Encontramos inteiros menores, a e b, que ao menos um deles satisfaz a condição. A contradição surgiu da nossa suposição de que n era composto. Portanto, n deve ser um número primo. □

2.9.4 Subanéis e Ideais

Assim como os grupos contêm subgrupos, os anéis contêm subestruturas que herdam suas propriedades. As duas subestruturas mais importantes são os subanéis, que são simplesmente anéis dentro de outros anéis, e os ideais, que são subconjuntos com uma propriedade de absorção multiplicativa.

Definição 2.9.7 (Subanel)**.** Seja $(A, +, \cdot)$ um anel. Um subconjunto não vazio $S \subseteq A$ é chamado de **subanel** de A se $(S, +, \cdot)$ for, ele próprio, um anel com as mesmas operações de A.

Para verificar se um subconjunto S é um subanel, basta mostrar que ele é fechado sob a subtração e a multiplicação.

Proposição 2.9.6 (Critério para Subanel)**.** Um subconjunto não vazio S de um anel A é um subanel se, e somente se, para quaisquer $a, b \in S$:

1. $a - b \in S$ (fechado sob a subtração, o que implica que $(S, +)$ é um subgrupo de $(A, +)$).
2. $a \cdot b \in S$ (fechado sob a multiplicação).

Demonstração. Como a proposição é uma equivalência, devemos provar as duas implicações.

(⇒) Suponha que S é um subanel de A. Por definição, $(S, +, \cdot)$ é, ele próprio, um anel. Isso implica que:

1. Como $(S, +)$ é um grupo (em particular, um subgrupo de $(A, +)$), ele é fechado para a subtração.

2. A operação de multiplicação é fechada em S. Portanto, se $a, b \in S$, o produto $a \cdot b$ deve pertencer a S. A segunda condição está satisfeita.

($\Leftarrow$) Agora, suponha que S é um subconjunto não vazio de A que satisfaz as duas condições da hipótese: para quaisquer $a, b \in S$, temos $a - b \in S$ e $a \cdot b \in S$. Nosso objetivo é provar que $(S, +, \cdot)$ satisfaz todos os axiomas de um anel.

- $(S, +)$ **é um grupo:** A primeira condição da hipótese, $a - b \in S$, é o critério de subgrupo para grupos aditivos. Como $(A, +)$ é um grupo, este critério é suficiente para garantir que $(S, +)$ é um subgrupo de $(A, +)$.
- **A multiplicação é fechada em S:** Por hipótese, $a \cdot b \in S$ para quaisquer $a, b \in S$. Sem essa condição, a operação nos levaria para fora do conjunto.
- **A multiplicação é associativa e distributiva em S:** A distributividade e associatividade valem para todos os elementos de A e, portanto, são herdadas pelos elementos de S.

Como $(S, +)$ é um grupo, a multiplicação é uma operação binária fechada e associativa em S, e a distributividade é válida, concluímos que $(S, +, \cdot)$ satisfaz todos os axiomas de um anel. Portanto, S é um subanel de A.

□

Exemplo 2.9.4. Para qualquer inteiro $n \geq 0$, o conjunto dos múltiplos de n, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, é um subanel do anel dos inteiros $(\mathbb{Z}, +, \cdot)$.

Demonstração. Sejam $a, b \in n\mathbb{Z}$. Por definição, existem inteiros k_1, k_2 tais que $a = nk_1$ e $b = nk_2$.

1. **Fechamento sob a subtração:** A diferença é $a - b = nk_1 - nk_2 = n(k_1 - k_2)$. Como $k_1 - k_2$ é um inteiro, o resultado é um múltiplo de n e, portanto, pertence a $n\mathbb{Z}$.
2. **Fechamento sob a multiplicação:** O produto é $a \cdot b = (nk_1)(nk_2) = n(nk_1k_2)$. Como nk_1k_2 é um inteiro, o resultado é um múltiplo de n e pertence a $n\mathbb{Z}$.

Como ambas as condições são satisfeitas, $n\mathbb{Z}$ é um subanel de $\mathbb{Z}$, visto que, evidentemente $n\mathbb{Z}$ é não vazio. □

O conceito de ideal é mais restritivo. Enquanto um subanel apenas exige que a multiplicação entre seus próprios elementos permaneça no subanel, um ideal exige que a multiplicação de um de seus elementos por *qualquer* elemento do anel maior puxe o resultado de volta para dentro do ideal.

Definição 2.9.8 (Ideal)**.** Seja $(A, +, \cdot)$ um anel. Um subconjunto $I \subseteq A$ é chamado de **ideal** de A se satisfaz as seguintes condições:

- $(I, +)$ é um subgrupo de $(A, +)$.
- I satisfaz a propriedade de absorção: para todo $a \in A$ e todo $i \in I$, os produtos $a \cdot i$ e $i \cdot a$ também pertencem a I.

$$\forall a \in A, \forall i \in I \implies a \cdot i \in I \quad \text{e} \quad i \cdot a \in I$$

O papel dos ideais na teoria dos anéis é análogo ao dos subgrupos normais na teoria dos grupos; eles são precisamente as subestruturas que nos permitem construir anéis quocientes.

Exemplo 2.9.5 (Os Ideais de $\mathbb{Z}$)**.** Vamos provar que, para qualquer $n \in \mathbb{N}$, o subconjunto $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ é um ideal do anel $(\mathbb{Z}, +, \cdot)$.

Demonstração. Como já demonstramos que $(n\mathbb{Z}, +)$ é sempre um subgrupo de $(\mathbb{Z}, +)$, só precisamos provar a propriedade de absorção.

Propriedade de Absorção: Devemos mostrar que para qualquer elemento do anel $a \in \mathbb{Z}$ e qualquer elemento do ideal $i \in n\mathbb{Z}$, os produtos $a \cdot i$ e $i \cdot a$ pertencem a $n\mathbb{Z}$.

Seja $a \in \mathbb{Z}$ um inteiro arbitrário. Seja $i \in n\mathbb{Z}$. Pela definição de $n\mathbb{Z}$, existe um inteiro k tal que $i = n \cdot k$.

Calculamos o produto $a \cdot i$:

$$a \cdot i = a \cdot (n \cdot k)$$

Usando a associatividade e a comutatividade da multiplicação em $\mathbb{Z}$:

$$a \cdot i = (a \cdot n) \cdot k = (n \cdot a) \cdot k = n \cdot (a \cdot k)$$

Seja $k' = a \cdot k$. Como a e k são inteiros, seu produto k' também é um inteiro. A expressão $n \cdot k'$ tem, portanto, a forma de um múltiplo de n. Isso significa, por definição, que o resultado $a \cdot i$ pertence a $n\mathbb{Z}$.

Como o anel $\mathbb{Z}$ é comutativo, o produto $i \cdot a$ é idêntico a $a \cdot i$:

$$i \cdot a = a \cdot i = n \cdot (a \cdot k)$$

Portanto, $i \cdot a$ também pertence a $n\mathbb{Z}$.

Como ambas as condições são satisfeitas, concluímos que $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. □

Proposição 2.9.7. Todo ideal do anel dos inteiros $(\mathbb{Z}, +, \cdot)$ é da forma $n\mathbb{Z}$ para algum $n \in \mathbb{N}$.

Demonstração. Seja I um ideal de $\mathbb{Z}$. Temos dois casos a considerar:

Caso 1: $I = \{0\}$**.** Neste caso, escolhendo $n = 0$, temos $I = 0\mathbb{Z} = \{0\}$. A proposição é válida.

Caso 2: $I \neq \{0\}$**.** Se I possui elementos não nulos, ele deve conter pelo menos um número positivo (pois se $x \in I$ e $x < 0$, então $-x \in I$ e $-x > 0$, já que ideais são subgrupos aditivos). Pelo Princípio da Boa Ordem, o conjunto dos elementos positivos de I possui um menor elemento. Seja n esse menor inteiro positivo.

Vamos provar que $I = n\mathbb{Z}$ demonstrando a dupla inclusão:

- **($n\mathbb{Z} \subseteq I$):** Como $n \in I$ e I é um ideal, pela propriedade de absorção, para qualquer inteiro k, o produto $k \cdot n$ deve pertencer a I. Logo, todos os múltiplos de n estão em I.

- **($I \subseteq n\mathbb{Z}$):** Seja a um elemento qualquer de I. Pelo Algoritmo da Divisão, podemos dividir a por n:

  $$a = n \cdot q + r, \quad \text{com } 0 \leq r < n$$

  Podemos reescrever o resto como:

  $$r = a - n \cdot q$$

  Sabemos que $a \in I$. Como $n \in I$, o múltiplo $n \cdot q$ também está em I. Como I é fechado para a subtração (pois é um subgrupo aditivo), a diferença $r = a - n \cdot q$ também pertence a I. Assim, temos um elemento $r \in I$ tal que $0 \leq r < n$. Como n foi definido como o *menor* inteiro positivo de I, r não pode ser um inteiro positivo. A única possibilidade restante é $r = 0$. Se $r = 0$, então $a = n \cdot q$, o que significa que a é um múltiplo de n. Logo, $a \in n\mathbb{Z}$.

Como $n\mathbb{Z} \subseteq I$ e $I \subseteq n\mathbb{Z}$, concluímos que $I = n\mathbb{Z}$. □

2.9.5 Anéis Quocientes

Assim como os subgrupos normais nos permitiram construir grupos quocientes, os ideais são precisamente a subestrutura necessária para construir um anel quociente. A propriedade de absorção de um ideal garante que a operação de multiplicação, quando definida sobre as classes laterais aditivas, seja bem-definida.

Definição 2.9.9 (Anel Quociente)**.** Sejam $(A, +, \cdot)$ um anel e I um ideal de A. O **anel quociente** de A por I, denotado por A/I, é o conjunto de todas as classes laterais aditivas de I em A:

$$A/I = \{a + I \mid a \in A\}$$

munido das seguintes operações de adição e multiplicação:

- Adição: $(a + I) + (b + I) := (a + b) + I$
- Multiplicação: $(a + I) \cdot (b + I) := (a \cdot b) + I$

para quaisquer $a + I, b + I \in A/I$.
Além disso, se A for comutativo, A/I também será comutativo.

Para que esta construção seja válida, devemos provar que as operações não dependem dos representantes escolhidos para as classes, e A/I apresenta as propriedades características de um anel.

Proposição 2.9.8. As operações de adição e multiplicação no anel quociente A/I são bem-definidas.

Demonstração. Sejam $a, b, a', b' \in A$ tais que $a + I = a' + I$ e $b + I = b' + I$. Por definição de igualdade de classes laterais, isso significa que $a - a' \in I$ e $b - b' \in I$. Podemos então escrever $a' = a + i_1$ e $b' = b + i_2$ para alguns $i_1, i_2 \in I$.

Adição: A adição é bem-definida, pois $(A, +)$ é um grupo abeliano e I é um subgrupo (normal) de $(A, +)$. Isso também garante que a adição em A/I é associativa e comutativa.

Multiplicação: Devemos mostrar que a classe do resultado da multiplicação é a mesma, ou seja, $(a \cdot b) + I = (a' \cdot b') + I$. Calculamos o produto dos novos representantes:

$$a' \cdot b' = (a + i_1) \cdot (b + i_2) = a \cdot b + a \cdot i_2 + i_1 \cdot b + i_1 \cdot i_2$$

Para que as classes sejam iguais, a diferença $(a' \cdot b') - (a \cdot b)$ deve pertencer a I. A diferença é:

$$(a' \cdot b') - (a \cdot b) = a \cdot i_2 + i_1 \cdot b + i_1 \cdot i_2$$

Analisamos cada termo do lado direito:

- $a \cdot i_2$: Como I é um ideal e $i_2 \in I$, a propriedade de absorção garante que $a \cdot i_2 \in I$.
- $i_1 \cdot b$: Da mesma forma, desde que $i_1 \in I$, $i_1 \cdot b \in I$.
- $i_1 \cdot i_2$: Como I é um subanel (e, portanto, fechado para a multiplicação), o produto $i_1 \cdot i_2$ pertence a I.

Como I é um subgrupo aditivo, a soma de elementos que estão em I também está em I. Logo, a diferença $(a' \cdot b') - (a \cdot b)$ pertence a I, o que prova que $(a \cdot b) + I = (a' \cdot b') + I$. A multiplicação está bem-definida.

Com a multiplicação bem definida, podemos demonstrar associatividade da multiplicação, e a distributividade desta em relação à adição:

Associatividade da multiplicação
Devemos provar que $((a+I)\cdot(b+I))\cdot(c+I) = (a+I)\cdot((b+I)\cdot(c+I))$.

$$\begin{aligned}((a+I)(b+I))(c+I) &= ((ab)+I)(c+I)\\ &= ((ab)c)+I\\ &= (a(bc))+I\\ &= (a+I)((bc)+I)\\ &= (a+I)((b+I)(c+I))\end{aligned}$$

A associatividade da multiplicação em A/I segue diretamente da associatividade da multiplicação no anel A.

Distributividade (à Esquerda)
Devemos provar que $(a+I)\cdot((b+I)+(c+I)) = ((a+I)\cdot(b+I))+((a+I)\cdot(c+I))$.

$$\begin{aligned}(a+I)((b+I)+(c+I)) &= (a+I)((b+c)+I)\\ &= (a(b+c))+I\\ &= (ab+ac)+I\\ &= (ab+I)+(ac+I)\\ &= ((a+I)(b+I))+((a+I)(c+I))\end{aligned}$$

A prova da distributividade à direita é análoga.

Como $(A/I,+)$ é um grupo abeliano, a multiplicação é associativa e a distributividade é válida, A/I satisfaz os axiomas de um anel.

□

2.9.6 O Teorema Fundamental dos Homomorfismos de Anéis

Definição 2.9.10 (Homomorfismo de Anéis)**.** Sejam $(A,+,\cdot)$ e $(B,\oplus,\odot)$ dois anéis. Uma função $f: A \to B$ é chamada de **homomorfismo de anéis** se, para quaisquer $a, b \in A$, ela preserva ambas as operações:

1. $f(a+b) = f(a) \oplus f(b)$ (Preservação da adição)
2. $f(a\cdot b) = f(a) \odot f(b)$ (Preservação da multiplicação)

Adicionalmente, se A e B são anéis com unidade (1_A e 1_B, respectivamente), a seguinte condição costuma ser exigida:

3. $f(1_A) = 1_B$ (Preservação da unidade multiplicativa)

Em anéis arbitrários, as duas primeiras condições garantem apenas que $f(1_A) \cdot f(1_A) = f(1_A)$, e não necessariamente $f(1_A) = 1_B$. Entretanto, se o contradomínio B for um **domínio de integridade** e f não for o homomorfismo nulo, a condição 3 torna-se uma consequência das anteriores.

Proposição 2.9.9. Sejam A um anel com unidade e B um domínio de integridade. Se $f : A \to B$ é um homomorfismo de anéis (que preserva soma e produto) e f não é nulo, então $f(1_A) = 1_B$.

Demonstração. Sabemos que $1_A \cdot 1_A = 1_A$. Aplicando a função f e usando a preservação da multiplicação:

$$f(1_A) = f(1_A \cdot 1_A) = f(1_A) \cdot f(1_A)$$

Seja $y = f(1_A) \in B$. A equação torna-se $y = y^2$, ou equivalentemente:

$$y^2 - y = 0_B \implies y \cdot (y - 1_B) = 0_B$$

Como B é um domínio de integridade, ele não possui divisores de zero. Logo, o produto só pode ser nulo se um dos fatores for nulo. Temos duas possibilidades:

1. $y = 0_B$: Neste caso, $f(1_A) = 0_B$. Para qualquer $a \in A$, teríamos $f(a) = f(a \cdot 1_A) = f(a) \cdot f(1_A) = f(a) \cdot 0_B = 0_B$. Isso implicaria que f é a função nula, o que contradiz a hipótese.

2. $y - 1_B = 0_B$: Isso implica $y = 1_B$, ou seja, $f(1_A) = 1_B$.

Portanto, se f não é nulo e B é um domínio, a preservação da unidade é automática. □

Proposição 2.9.10. O anel quociente $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ é isomórfico ao anel dos inteiros módulo n, $(\mathbb{Z}_n, +, \cdot)$.

Demonstração. Como já provamos, o conjunto $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. O anel quociente $\mathbb{Z}/n\mathbb{Z}$ é o conjunto das classes laterais $\{k + n\mathbb{Z} \mid k \in \mathbb{Z}\}$, que são idênticas às classes de congruência $\{[k]_n \mid k \in \mathbb{Z}\}$.

Para provar o isomorfismo de anéis, definimos a função $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ por:

$$\phi(k + n\mathbb{Z}) = [k]_n$$

Já demonstramos na seção sobre grupos que esta função é um isomorfismo de grupos para a operação de adição. Resta apenas verificar que ela também preserva a operação de multiplicação, ou seja, que é um homomorfismo de anéis.

Sejam $a + n\mathbb{Z}$ e $b + n\mathbb{Z}$ dois elementos de $\mathbb{Z}/n\mathbb{Z}$.

$$\begin{aligned}
\phi((a + n\mathbb{Z}) \cdot (b + n\mathbb{Z})) &= \phi((a \cdot b) + n\mathbb{Z}) && \text{(Definição de mult. em } \mathbb{Z}/n\mathbb{Z}) \\
&= [a \cdot b]_n && \text{(Definição de } \phi) \\
&= [a]_n \cdot [b]_n && \text{(Definição de mult. em } \mathbb{Z}_n) \\
&= \phi(a + n\mathbb{Z}) \cdot \phi(b + n\mathbb{Z}) && \text{(Definição de } \phi)
\end{aligned}$$

Finalmente, devemos verificar se ϕ mapeia a unidade multiplicativa de $\mathbb{Z}/n\mathbb{Z}$ na unidade multiplicativa de $\mathbb{Z}_n$. A unidade em $\mathbb{Z}/n\mathbb{Z}$ é a classe $1 + n\mathbb{Z}$, e a unidade em $\mathbb{Z}_n$ é a classe $[1]_n$. Aplicando a definição de ϕ:

$$\phi(1 + n\mathbb{Z}) = [1]_n$$

Como a função ϕ é uma bijeção que preserva ambas as operações de anel e mapeia a unidade na unidade, ela é um isomorfismo de anéis (com unidade).

□

Definição 2.9.11 (Núcleo de um Homomorfismo de Anéis)**.** O **núcleo** (ou **kernel**) de um homomorfismo de anéis $f : A \to B$, denotado por $\ker(f)$, é o conjunto de todos os elementos em A que são mapeados para o elemento identidade aditivo (0_B) de B.

$$\ker(f) = \{a \in A \mid f(a) = 0_B\}$$

Proposição 2.9.11. O núcleo de um homomorfismo de anéis $f : A \to B$ é sempre um ideal do anel de domínio A.

Demonstração. Seja $K = \ker(f) = \{a \in A \mid f(a) = 0_B\}$. Para provar que K é um ideal de A, devemos verificar as duas condições da definição de ideal:

1. $(K, +)$ **é um subgrupo de** $(A, +)$**:** Por definição, um homomorfismo de anéis $f : (A, +, \cdot) \to (B, \oplus, \odot)$ é também um homomorfismo de grupos entre as estruturas aditivas $(A, +)$ e $(B, \oplus)$. O núcleo K definido acima é precisamente o núcleo deste homomorfismo de grupos (elementos mapeados para a identidade aditiva 0_B). Conforme demonstrado na secção sobre propriedades do núcleo de homomorfismos de grupos, o núcleo de um homomorfismo de grupos é sempre um subgrupo (normal) do grupo de domínio. Portanto, $(K, +)$ é um subgrupo de $(A, +)$.

2. K **satisfaz a propriedade de absorção:** Devemos mostrar que, para qualquer elemento $a \in A$ e qualquer elemento $k \in K$, os produtos $a \cdot k$ e $k \cdot a$ também pertencem a K.

   Sejam $a \in A$ e $k \in K$. Por definição de K, sabemos que $f(k) = 0_B$.

Calculamos $f(a \cdot k)$:

$$\begin{aligned} f(a \cdot k) &= f(a) \odot f(k) && \text{(f preserva a multiplicação)} \\ &= f(a) \odot 0_B && \text{(pois } k \in K\text{)} \\ &= 0_B \end{aligned}$$

Como $f(a \cdot k) = 0_B$, o elemento $a \cdot k$ pertence a K.

Calculamos $f(k \cdot a)$:

$$\begin{aligned} f(k \cdot a) &= f(k) \odot f(a) && \text{(f preserva a multiplicação)} \\ &= 0_B \odot f(a) && \text{(pois } k \in K\text{)} \\ &= 0_B \end{aligned}$$

Como $f(k \cdot a) = 0_B$, o elemento $k \cdot a$ pertence a K.

Portanto, K satisfaz a propriedade de absorção.

Como $(K, +)$ é um subgrupo aditivo e K satisfaz a propriedade de absorção, concluímos que $\ker(f)$ é um ideal de A.

□

Proposição 2.9.12 (Caracterização da Injetividade pelo Núcleo)**.** Seja $f : A \to B$ um homomorfismo de anéis (ou grupos). A função f é injetiva se, e somente se, o seu núcleo é trivial, isto é, $\ker(f) = \{0_A\}$.

Demonstração. Como se trata de uma equivalência, provamos as duas implicações.

(⇒) Se f é injetiva, então $\ker(f) = \{0_A\}$. Seja $x \in \ker(f)$. Por definição, $f(x) = 0_B$. Sabemos que todo homomorfismo mapeia o zero no zero, logo $f(0_A) = 0_B$. Assim, temos $f(x) = f(0_A)$. Como f é injetiva, isso implica que $x = 0_A$. Portanto, o único elemento no núcleo é o zero.

(⇐) Se $\ker(f) = \{0_A\}$, então f é injetiva. Sejam $a, b \in A$ tais que $f(a) = f(b)$. Como f é um homomorfismo, ele preserva a subtração (pois preserva a soma e o inverso aditivo):

$$f(a) - f(b) = 0_B \implies f(a - b) = 0_B$$

Isso significa que o elemento $(a - b)$ pertence ao núcleo de f.

$$(a - b) \in \ker(f)$$

Pela nossa hipótese, o núcleo contém apenas o elemento zero. Logo:

$$a - b = 0_A \implies a = b$$

Como $f(a) = f(b)$ implica $a = b$, concluímos que f é injetiva. □

Note que um homomorfismo $f : A \to B$ pode falhar em ser um isomorfismo (uma bijeção) por dois motivos:

1. **Falta de Sobrejetividade:** A imagem de f pode não cobrir todo o anel B. Podemos resolver isso restringindo o contradomínio apenas à imagem, $\text{Im}(f)$.

2. **Falta de Injetividade:** Elementos distintos de A podem ser mapeados no mesmo elemento de B. Isso ocorre quando o núcleo, $\ker(f)$, contém mais elementos além do zero.

O Teorema a seguir nos diz que, se colapsarmos todos os elementos do domínio que causam a falha de injetividade (agrupando-os nas classes do anel quociente $A/\ker(f)$) e restringirmos o contradomínio à imagem, a função resultante torna-se uma bijeção, preservando a estrutura algébrica original.

Teorema 2.9.2 (Teorema Fundamental dos Homomorfismos de Anéis)**.** Seja $f : A \to B$ um homomorfismo de anéis. Então, o anel quociente $A/\ker(f)$ é isomórfico à imagem de f, $\text{Im}(f)$. Formalmente:

$$A/\ker(f) \cong \text{Im}(f)$$

Demonstração. Seja $I = \ker(f)$. Sabemos que I é um ideal de A. Consideremos as estruturas aditivas: $(A, +)$ é um grupo abeliano, I é um subgrupo normal de $(A, +)$, e $(B, \oplus)$ é um grupo. A função f, vista apenas como um homomorfismo entre estes grupos aditivos, tem núcleo I e imagem $\text{Im}(f)$.

O Teorema Fundamental dos Homomorfismos para Grupos estabelece que a função $\phi : A/I \to \text{Im}(f)$ definida por:

$$\phi(a + I) = f(a)$$

é um **isomorfismo de grupos** aditivos. Isso já garante que:

- ϕ é bem-definida.
- ϕ preserva a operação de adição: $\phi((a + I) + (b + I)) = \phi(a + I) + \phi(b + I)$.
- ϕ é uma bijeção (injetiva e sobrejetiva).

A demonstração destas propriedades é idêntica àquela realizada na teoria dos grupos e, portanto, não será repetida aqui.

Para completar a prova de que ϕ é um **isomorfismo de anéis**, resta apenas verificar se ϕ também preserva a segunda operação do anel, a multiplicação.

Preservação da Multiplicação: Devemos mostrar que $\phi((a+I)\cdot(b+I)) = \phi(a+I)\cdot\phi(b+I)$.

$$\begin{aligned}
\phi((a+I)\cdot(b+I)) &= \phi((a\cdot b)+I) && \text{(Def. } \cdot \text{ em } A/I) \\
&= f(a\cdot b) && \text{(Def. de } \phi) \\
&= f(a)\odot f(b) && \text{(f é homomorfismo de anéis)} \\
&= \phi(a+I)\odot\phi(b+I) && \text{(Def. de } \phi)
\end{aligned}$$

A multiplicação é preservada.

Preservação da Unidade Multiplicativa (quando aplicável): Se os anéis A e B possuem unidades multiplicativas 1_A e 1_B, respectivamente, e se o homomorfismo f satisfaz a condição adicional de preservar a unidade, então o isomorfismo ϕ também preserva a unidade. A unidade multiplicativa no anel quociente A/I é a classe $1_A + I$. A unidade multiplicativa na imagem $\mathrm{Im}(f)$ é $f(1_A)$, que por hipótese é 1_B. Aplicando a definição de ϕ à unidade de A/I:

$$\phi(1_A + I) = f(1_A) = 1_B$$

Assim, ϕ mapeia a identidade multiplicativa de A/I na identidade multiplicativa de $\mathrm{Im}(f)$.

Como ϕ é uma bijeção que preserva tanto a adição quanto a multiplicação (e, se aplicável, mapeia $1_A + I$ para $f(1_A) = 1_B$, caso estejamos exigindo homomorfismos com unidade), ϕ é um isomorfismo de anéis. Isso conclui a prova. □

Exemplo 2.9.6. Considere o anel dos inteiros, $A = (\mathbb{Z}, +, \cdot)$, e o anel dos inteiros módulo n, $B = (\mathbb{Z}_n, +, \cdot)$. Definimos a função de projeção canônica $f : \mathbb{Z} \to \mathbb{Z}_n$ da seguinte forma:

$$f(k) = [k]_n$$

Esta função mapeia cada inteiro para a sua respectiva classe de congruência módulo n. Vamos provar que f é um homomorfismo de anéis e aplicar o Teorema Fundamental.

Demonstração. Para provar que f é um homomorfismo de anéis, devemos verificar se ela preserva a adição, a multiplicação e a unidade.

Preservação da Adição

A função f, vista como um mapeamento entre os grupos aditivos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$, é o homomorfismo canônico que leva um elemento à sua classe de equivalência. Já foi estabelecido que tal mapeamento é um homomorfismo de grupos, ou seja,

$f(a+b) = [a+b]_n = [a]_n + [b]_n = f(a) + f(b)$. A adição é preservada.

Preservação da Multiplicação

Devemos mostrar que $f(a \cdot b) = f(a) \cdot f(b)$ para quaisquer $a, b \in \mathbb{Z}$.

- Lado esquerdo: Aplicando a definição de f ao produto $a \cdot b$, temos:

$$f(a \cdot b) = [a \cdot b]_n$$

- Lado direito: Aplicando f a cada termo separadamente, temos:

$$f(a) \cdot f(b) = [a]_n \cdot [b]_n$$

De forma análoga à adição, a operação de multiplicação em $\mathbb{Z}_n$ é definida como a classe do produto dos representantes. Portanto, por definição:

$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

Como o lado esquerdo é igual ao lado direito, a função f também preserva a multiplicação.

Preservação da Unidade

A unidade multiplicativa em $\mathbb{Z}$ é 1. A unidade multiplicativa em $\mathbb{Z}_n$ é $[1]_n$. Aplicando f à unidade de $\mathbb{Z}$:

$$f(1) = [1]_n$$

Como f mapeia a unidade na unidade, a condição é satisfeita.

Como f preserva a adição, a multiplicação e a unidade, f é um homomorfismo de anéis (com unidade).

Aplicação do Teorema Fundamental

Considerando f como um homomorfismo de grupos aditivos, já sabemos que:

- **O Núcleo:** $\ker(f) = \{k \in \mathbb{Z} \mid f(k) = [0]_n\} = \{k \in \mathbb{Z} \mid [k]_n = [0]_n\}$. Esta condição significa que k é um múltiplo de n, logo $\ker(f) = n\mathbb{Z}$.
- **A Imagem:** $\mathrm{Im}(f) = \{f(k) \mid k \in \mathbb{Z}\} = \{[k]_n \mid k \in \mathbb{Z}\}$. Como todo elemento $[k]_n$ de $\mathbb{Z}_n$ é a imagem do inteiro k, a função é sobrejetiva, e $\mathrm{Im}(f) = \mathbb{Z}_n$.

O Teorema Fundamental dos Homomorfismos de Anéis afirma que $A/\ker(f) \cong \mathrm{Im}(f)$. Substituindo as estruturas que identificamos:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Este resultado demonstra que o anel $\mathbb{Z}_n$, construído a partir da noção de aritmética modular, é algebricamente idêntico (isomórfico) ao anel quociente $\mathbb{Z}/n\mathbb{Z}$, que é construído a partir da perspectiva mais abstrata de particionar o anel dos inteiros por um de seus ideais. □

Capítulo 3

Racionais

No capítulo anterior, analisamos a estrutura algébrica dos números inteiros. Vimos que $(\mathbb{Z}, +)$ forma um grupo abeliano, no qual todo elemento a possui um inverso aditivo único, $-a$. Esta estrutura resolveu a deficiência do monoide $(\mathbb{N}, +)$, que não era fechado para a subtração.

Contudo, ao analisarmos a multiplicação, vimos que o monoide $(\mathbb{Z}, \cdot, 1)$ **não é** um grupo. A falha reside na ausência de elementos inversos para a maioria de seus membros. Por exemplo, o inteiro 2 não possui um inverso multiplicativo em $\mathbb{Z}$, pois não existe um inteiro k que satisfaça a equação $2 \cdot k = 1$.

Esta limitação da multiplicação em $\mathbb{Z}$ é a motivação para a nossa próxima construção. O método será uma analogia direta ao que foi feito para construir $\mathbb{Z}$ a partir de $\mathbb{N}$. Usaremos pares ordenados do conjunto dos inteiros e definiremos uma relação de equivalência sobre eles para formalizar a noção de que diferentes pares, como $(1, 2)$ e $(2, 4)$, podem representar a mesma ideia.

3.1 Construção de $\mathbb{Q}$ via Relação de Equivalência em $\mathbb{Z} \times \mathbb{Z}^*$

Nosso objetivo ao construir este novo conjunto é criar uma estrutura onde equações da forma $b \cdot x = a$ sempre possuam uma solução. Devemos, no entanto, analisar o caso em que $b = 0$. A equação se tornaria $0 \cdot x = a$. Se $a \neq 0$, não existe solução em $\mathbb{Z}$, pois o produto de qualquer inteiro por zero é zero, e não a. Se $a = 0$, a equação se torna $0 \cdot x = 0$, que é satisfeita por qualquer inteiro x, não fornecendo uma solução única.

Visto que o caso $b = 0$ não produz soluções consistentes ou únicas, ele não serve ao nosso propósito de estender a estrutura multiplicativa para incluir inversos. Por esta razão, restringimos nossa construção para pares ordenados (a, b) onde o segundo componente é explicitamente não nulo.

Seja $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ o conjunto dos inteiros não nulos. O conjunto sobre o qual

trabalharemos é $\mathbb{Z} \times \mathbb{Z}^*$.

Definição 3.1.1 (Relação de Equivalência em $\mathbb{Z}\times\mathbb{Z}^*$)**.** Seja o conjunto $\mathbb{Z}\times\mathbb{Z}^*$. Definimos a relação $\sim$ sobre este conjunto da seguinte forma: para quaisquer pares (a, b) e (c, d), com $b, d \neq 0$:

$$(a, b) \sim (c, d) \iff a \cdot d = b \cdot c$$

Proposição 3.1.1. A relação $\sim$ é uma relação de equivalência.

Demonstração. Devemos verificar as três propriedades: reflexividade, simetria e transitividade, usando as propriedades do anel dos inteiros.

Reflexividade: *Devemos provar que* $(a, b) \sim (a, b)$. Pela definição da relação, isso significa provar que $a \cdot b = b \cdot a$. Isso é verdade devido à comutatividade da multiplicação em $\mathbb{Z}$.

Simetria: *Devemos provar que se* $(a, b) \sim (c, d)$*, então* $(c, d) \sim (a, b)$. A hipótese $(a, b) \sim (c, d)$ nos diz que $a \cdot d = b \cdot c$. Queremos provar que $c \cdot b = d \cdot a$. Pela comutatividade da multiplicação e da igualdade em $\mathbb{Z}$, podemos reescrever a hipótese:

$$a \cdot d = b \cdot c \implies b \cdot c = a \cdot d \implies c \cdot b = d \cdot a$$

Isso é exatamente a condição para que $(c, d) \sim (a, b)$.

Transitividade: *Devemos provar que se* $(a, b) \sim (c, d)$ *e* $(c, d) \sim (e, f)$*, então* $(a, b) \sim (e, f)$. Temos como hipóteses:

1. $(a, b) \sim (c, d) \implies a \cdot d = b \cdot c$
2. $(c, d) \sim (e, f) \implies c \cdot f = d \cdot e$

Nosso objetivo é provar que $a \cdot f = b \cdot e$.

Da hipótese (1), multiplicamos ambos os lados por f (o que é permitido em $\mathbb{Z}$):

$$(a \cdot d) \cdot f = (b \cdot c) \cdot f$$

Usando a associatividade e a comutatividade da multiplicação em $\mathbb{Z}$:

$$(a \cdot f) \cdot d = b \cdot (c \cdot f)$$

Agora, usamos a hipótese (2) para substituir o termo $(c \cdot f)$:

$$(a \cdot f) \cdot d = b \cdot (d \cdot e)$$

Reorganizando o lado direito:

$$(a \cdot f) \cdot d = (b \cdot e) \cdot d$$

Nós sabemos que $d \in \mathbb{Z}^*$, ou seja, $d \neq 0$, podemos aplicar a Lei do Cancelamento para a multiplicação:

$$a \cdot f = b \cdot e$$

Esta é a condição para que $(a, b) \sim (e, f)$. A transitividade está provada.

Como a relação $\sim$ é reflexiva, simétrica e transitiva, ela é uma relação de equivalência. □

3.1.1 Definição do Conjunto dos Racionais

Tendo estabelecido que $\sim$ é uma relação de equivalência, sabemos que ela particiona o conjunto $\mathbb{Z} \times \mathbb{Z}^*$ em classes de equivalência. Cada uma dessas classes será, por definição, um número racional.

Definição 3.1.2 (O Conjunto dos Números Racionais)**.** O conjunto dos números racionais, denotado por $\mathbb{Q}$, é definido como o conjunto quociente de $\mathbb{Z} \times \mathbb{Z}^*$ pela relação de equivalência $\sim$.

$$\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/\sim$$

Cada elemento de $\mathbb{Q}$ é uma classe de equivalência, $\overline{(a, b)}$.

3.2 Adição e Multiplicação em $\mathbb{Q}$

Agora que definimos o conjunto $\mathbb{Q}$ como o conjunto de todas as classes de equivalência $\overline{(a, b)}$, precisamos definir as operações de adição e multiplicação sobre este novo conjunto.

Definição 3.2.1 (Adição de Racionais)**.** Sejam $\overline{(a, b)}$ e $\overline{(c, d)}$ dois números racionais. A **soma** deles é definida como:

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

Note que, como $b \neq 0$ e $d \neq 0$, o produto $b \cdot d$ também é diferente de zero, garantindo que a classe resultante pertença a $\mathbb{Q}$.

Definição 3.2.2 (Multiplicação de Racionais)**.** Sejam $\overline{(a, b)}$ e $\overline{(c, d)}$ dois números racionais. O **produto** deles é definido como:

$$\overline{(a, b)} \cdot \overline{(c, d)} := \overline{(a \cdot c, b \cdot d)}$$

Novamente, como $b \neq 0$ e $d \neq 0$, o produto $b \cdot d$ é diferente de zero, e a classe resultante pertence a $\mathbb{Q}$.

Proposição 3.2.1. As operações de adição e multiplicação em $\mathbb{Q}$ são bem-definidas.

Demonstração. Para que as operações sejam bem-definidas, devemos mostrar que se tomarmos representantes diferentes para as mesmas classes, o resultado da operação pertencerá à mesma classe de equivalência.

Sejam $\overline{(a,b)} = \overline{(a',b')}$ e $\overline{(c,d)} = \overline{(c',d')}$. Isto nos fornece como hipóteses as seguintes igualdades em $\mathbb{Z}$:

1. $a \cdot b' = b \cdot a'$
2. $c \cdot d' = d \cdot c'$

Adição: Devemos provar que $\overline{(a,b)} + \overline{(c,d)} = \overline{(a',b')} + \overline{(c',d')}$. Ou seja, provar que:

$$\overline{(ad+bc,bd)} = \overline{(a'd'+b'c',b'd')}$$

Pela definição da nossa relação de equivalência, isso é o mesmo que provar a igualdade em $\mathbb{Z}$:

$$(ad+bc)\cdot(b'd') = (bd)\cdot(a'd'+b'c')$$

Vamos expandir o lado esquerdo (LE) usando a distributividade e a comutatividade em $\mathbb{Z}$:

$$(LE) = (ad)(b'd') + (bc)(b'd') = (ab')(dd') + (cd')(bb')$$

Agora, usamos nossas hipóteses (1) e (2) para substituir ab' e cd':

$$(LE) = (ba')(dd') + (dc')(bb')$$

Reorganizando os termos usando associatividade e comutatividade:

$$(LE) = (a'd')(bd) + (b'c')(bd)$$

Colocando bd em evidência:

$$(LE) = (a'd'+b'c')\cdot(bd)$$

Isso é exatamente o lado direito (LD) da equação que queríamos provar. Portanto, a adição está bem-definida.

Multiplicação: Devemos provar que $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(a',b')} \cdot \overline{(c',d')}$. Ou seja, provar que:

$$\overline{(ac,bd)} = \overline{(a'c',b'd')}$$

Isso é o mesmo que provar a igualdade:

$$(ac)\cdot(b'd') = (bd)\cdot(a'c')$$

Reorganizando os termos em ambos os lados:

$$(ab')(cd') = (ba')(dc')$$

A validade desta igualdade segue diretamente das hipóteses (1) e (2). Portanto, a multiplicação também está bem-definida. □

3.2.1 A Notação Fracionária

Até este ponto, utilizamos a notação $\overline{(a,b)}$ para denotar um elemento de $\mathbb{Q}$, ou seja, uma classe de equivalência de pares de inteiros. Esta notação é precisa, mas logisticamente inconveniente para manipulações algébricas.

Vamos, portanto, **definir** uma nova notação para representar estes elementos.

Definição 3.2.3 (Notação Fracionária)**.** Seja $\overline{(a,b)}$ um número racional, onde $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$. Definimos o símbolo $\frac{a}{b}$ como uma notação para a classe de equivalência $\overline{(a,b)}$.

$$\frac{a}{b} := \overline{(a,b)}$$

Nesta notação, o inteiro a é chamado de **numerador** e o inteiro não-nulo b é chamado de **denominador**.

Equivalência: Nossa definição de equivalência $\overline{(a,b)} \sim \overline{(c,d)} \iff a \cdot d = b \cdot c$ se traduz para:

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

Adição: Nossa definição de adição $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$ se traduz para:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

Multiplicação: Nossa definição de multiplicação $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$ se traduz para:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

3.2.2 Propriedades das Operações em $\mathbb{Q}$

Definimos as operações de adição e multiplicação em $\mathbb{Q}$. Agora, devemos provar que essas operações possuem as propriedades fundamentais (comutatividade, associatividade e distributividade) que esperamos de um sistema numérico.

Sejam $q_1 = \frac{a}{b}$, $q_2 = \frac{c}{d}$ e $q_3 = \frac{e}{f}$ números racionais arbitrários.

Proposição 3.2.2 (Comutatividade das Operações)**.** Tanto a adição quanto a multiplicação em $\mathbb{Q}$ são comutativas.

Demonstração. **Adição**
Devemos provar que $q_1 + q_2 = q_2 + q_1$. Calculamos os dois lados da equação usando a definição de adição:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{c}{d} + \frac{a}{b} = \frac{cb + da}{db}$$

Para mostrar que estas duas classes são iguais, basta mostrar que os numeradores e denominadores são iguais. Usando a comutatividade da adição e da multiplicação em $\mathbb{Z}$:

- Numerador: $ad + bc = da + cb = cb + da$.
- Denominador: $bd = db$.

Como os numeradores e denominadores são idênticos, as classes resultantes são idênticas.

Multiplicação
Devemos provar que $q_1 \cdot q_2 = q_2 \cdot q_1$. Calculamos os dois lados da equação usando a definição de multiplicação:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$
$$\frac{c}{d} \cdot \frac{a}{b} = \frac{ca}{db}$$

Usando a comutatividade da multiplicação em $\mathbb{Z}$:

- Numerador: $ac = ca$.
- Denominador: $bd = db$.

Novamente, as classes resultantes são idênticas. □

Proposição 3.2.3 (Associatividade das Operações)**.** Tanto a adição quanto a multiplicação em $\mathbb{Q}$ são associativas.

Demonstração. **Adição**
Devemos provar que $(q_1 + q_2) + q_3 = q_1 + (q_2 + q_3)$. Calculamos o Lado Esquerdo (LE):

$$(LE) = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{(ad + bc)f + (bd)e}{(bd)f}$$

Usando a distributividade e associatividade em $\mathbb{Z}$, o numerador é $adf + bcf + bde$ e o denominador é bdf.

$$(LE) = \frac{adf + bcf + bde}{bdf}$$

Calculamos o Lado Direito (LD):

$$(LD) = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{a(df) + b(cf + de)}{b(df)}$$

Usando a distributividade e associatividade em $\mathbb{Z}$, o numerador é $adf + bcf + bde$ e o denominador é bdf.

$$(LD) = \frac{adf + bcf + bde}{bdf}$$

Como $LE = LD$, a adição é associativa.

Multiplicação

Devemos provar que $(q_1 \cdot q_2) \cdot q_3 = q_1 \cdot (q_2 \cdot q_3)$. Calculamos o Lado Esquerdo (LE):

$$(LE) = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f}$$

Calculamos o Lado Direito (LD):

$$(LD) = \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a(ce)}{b(df)}$$

Pela associatividade da multiplicação em $\mathbb{Z}$, $(ac)e = a(ce)$ e $(bd)f = b(df)$. Portanto, $LE = LD$, e a multiplicação é associativa. □

Proposição 3.2.4 (Distributividade da Multiplicação sobre a Adição)**.** A multiplicação em $\mathbb{Q}$ distribui sobre a adição.

$$q_1 \cdot (q_2 + q_3) = (q_1 \cdot q_2) + (q_1 \cdot q_3)$$

Demonstração. Calculamos o Lado Esquerdo (LE):

$$(LE) = \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{a(cf + de)}{b(df)}$$

Usando a distributividade em $\mathbb{Z}$, o numerador é $acf + ade$ e o denominador é bdf.

$$(LE) = \frac{acf + ade}{bdf}$$

Calculamos o Lado Direito (LD):

$$(LD) = \left(\frac{a}{b} \cdot \frac{c}{d}\right) + \left(\frac{a}{b} \cdot \frac{e}{f}\right) = \frac{ac}{bd} + \frac{ae}{bf}$$

Para somar estas duas classes, usamos a definição de adição:

$$(LD) = \frac{(ac)(bf) + (bd)(ae)}{(bd)(bf)} = \frac{acbf + bdae}{bdbf}$$

Agora, devemos mostrar que as classes de LE e LD são equivalentes:

$$\frac{acf + ade}{bdf} = \frac{acbf + bdae}{bdbf}$$

Pela definição de equivalência, devemos verificar se $(acf + ade) \cdot (bdbf) = (bdf) \cdot (acbf + bdae)$. Expandindo o Lado Esquerdo da equivalência:

$$(acf + ade)(bdbf) = (acf)(bdbf) + (ade)(bdbf) = acfbdbf + adebdbf$$

Expandindo o Lado Direito da equivalência:

$$(bdf)(acbf + bdae) = (bdf)(acbf) + (bdf)(bdae) = bdfacbf + bdfbdae$$

Usando a associatividade e comutatividade da multiplicação em $\mathbb{Z}$, vemos que:
$acfbdbf = bdfacbf$ (ambos são $a \cdot b \cdot b \cdot c \cdot d \cdot f \cdot f$)
$adebdbf = bdfbdae$ (ambos são $a \cdot b \cdot b \cdot d \cdot d \cdot e \cdot f$)
Como as duas expressões são idênticas, a equivalência é verdadeira. Portanto, a distributividade é válida. □

3.3 A Inserção dos Inteiros em $\mathbb{Q}$

Consideremos o subconjunto $Q_{\mathbb{Z}}$ de $\mathbb{Q}$ que consiste em todas as classes de equivalência com denominador 1:

$$Q_{\mathbb{Z}} = \left\{ \frac{n}{1} \mid n \in \mathbb{Z} \right\}$$

Proposição 3.3.1. A estrutura dos números inteiros $(\mathbb{Z}, +, \cdot)$ é isomórfica à estrutura $(Q_{\mathbb{Z}}, +, \cdot)$.

Demonstração. Para provar que as duas estruturas são algebricamente idênticas, devemos construir uma bijeção $f : \mathbb{Z} \to Q_{\mathbb{Z}}$ que preserve ambas as operações.

Definimos a função f da seguinte maneira:

$$f(n) = \frac{n}{1}$$

Devemos provar que f é injetiva, sobrejetiva e preserva as operações.

Injetividade: Suponha que $f(n) = f(m)$ para $n, m \in \mathbb{Z}$.

$$\frac{n}{1} = \frac{m}{1}$$

Pela definição da nossa relação de equivalência, isso significa que $n \cdot 1 = 1 \cdot m$, o que implica $n = m$. Portanto, f é injetiva.

Sobrejetividade: Seja q um elemento arbitrário de $Q_{\mathbb{Z}}$. Pela definição de $Q_{\mathbb{Z}}$, q deve ter a forma $\frac{n}{1}$ para algum $n \in \mathbb{Z}$. Este n pertence ao domínio $\mathbb{Z}$, e $f(n) = \frac{n}{1} = q$. Como todo elemento de $Q_{\mathbb{Z}}$ é a imagem de algum elemento de $\mathbb{Z}$, a função f é sobrejetiva.

Preservação da Adição: Devemos mostrar que $f(n + m) = f(n) + f(m)$.

- Lado Esquerdo (LE): $f(n + m) = \frac{n+m}{1}$.
- Lado Direito (LD): $f(n) + f(m) = \frac{n}{1} + \frac{m}{1}$. Pela definição de adição em $\mathbb{Q}$:

$$\frac{n}{1} + \frac{m}{1} = \frac{n \cdot 1 + 1 \cdot m}{1 \cdot 1} = \frac{n + m}{1}$$

Como $LE = LD$, a adição é preservada.

Preservação da Multiplicação: Devemos mostrar que $f(n \cdot m) = f(n) \cdot f(m)$.

- Lado Esquerdo (LE): $f(n \cdot m) = \frac{n \cdot m}{1}$.
- Lado Direito (LD): $f(n) \cdot f(m) = \frac{n}{1} \cdot \frac{m}{1}$. Pela definição de multiplicação em $\mathbb{Q}$:

$$\frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1 \cdot 1} = \frac{nm}{1}$$

Como $LE = LD$, a multiplicação é preservada.

Como f é uma bijeção que preserva ambas as operações, ela é um isomorfismo. Isso prova que $\mathbb{Z}$ e $Q_{\mathbb{Z}}$ são algebricamente indistinguíveis. □

Este isomorfismo nos permite, sem ambiguidade, identificar o inteiro n com o número racional $\frac{n}{1}$. Assim, podemos tratar $\mathbb{Z}$ como um subconjunto de $\mathbb{Q}$, escrevendo $\mathbb{Z} \subset \mathbb{Q}$.

3.3.1 Inversos Aditivos e Multiplicativos em $\mathbb{Q}$

Antes de podermos discutir inversos, devemos primeiro identificar formalmente os elementos identidade para cada uma das nossas operações em $\mathbb{Q}$.

Proposição 3.3.2 (Identidade Aditiva)**.** A classe de equivalência $\frac{0}{1}$ é o elemento identidade aditivo de $\mathbb{Q}$.

Demonstração. Seja $q = \frac{a}{b}$ um número racional qualquer. Devemos provar que $q + \frac{0}{1} = q$.

Pela definição de adição em $\mathbb{Q}$:

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1}$$

Usando as propriedades do 0 e 1 em $\mathbb{Z}$, o numerador se torna $a + 0 = a$ e o denominador $b \cdot 1 = b$.

$$\frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}$$

Esta é a classe $\frac{a}{b}$ original, q. □

Definição 3.3.1 (Elemento Inverso Aditivo)**.** Seja $q = \frac{a}{b}$ um número racional. Seu inverso aditivo, denotado por $-q$, é uma classe $\frac{x}{y}$ tal que $q + \frac{x}{y} = 0_{\mathbb{Q}}$, onde $0_{\mathbb{Q}} = \frac{0}{1}$ é o elemento identidade aditivo. A escolha mais simples é a classe $\frac{-a}{b}$. Verificamos:

$$\frac{a}{b} + \frac{-a}{b} = \frac{a \cdot b + b \cdot (-a)}{b \cdot b} = \frac{ab - ba}{b^2} = \frac{0}{b^2}$$

Como $(0, b^2) \sim (0, 1)$ (pois $0 \cdot 1 = b^2 \cdot 0 = 0$), a classe $\frac{0}{b^2}$ é a própria identidade aditiva $\frac{0}{1}$. Portanto, o inverso aditivo de $\frac{a}{b}$ é a classe $\frac{-a}{b}$.

$$-\left(\frac{a}{b}\right) = \frac{-a}{b}$$

Proposição 3.3.3 (Identidade Multiplicativa)**.** A classe de equivalência $\frac{1}{1}$ é o elemento identidade multiplicativo de $\mathbb{Q}$.

Demonstração. Seja $q = \frac{a}{b}$ um número racional qualquer. Devemos provar que $q \cdot \frac{1}{1} = q$.

Pela definição de multiplicação em $\mathbb{Q}$:

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$$

□

Definição 3.3.2 (Elemento Inverso Multiplicativo)**.** Seja $q = \frac{a}{b}$ um número racional não-nulo ($a \neq 0$ e $b \neq 0$). Seu inverso multiplicativo, que denotamos por q^{-1} ou $\left(\frac{a}{b}\right)^{-1}$, é uma classe $\frac{x}{y}$ tal que $\frac{a}{b} \cdot \frac{x}{y} = \frac{1}{1}$, que é o nosso elemento identidade multiplicativo.

$$\frac{a \cdot x}{b \cdot y} = \frac{1}{1} \implies (a \cdot x) \cdot 1 = (b \cdot y) \cdot 1 \implies a \cdot x = b \cdot y$$

A escolha mais simples para x e y que satisfaz esta condição é $x = b$ e $y = a$. Como $a \neq 0$ (pois q é não-nulo), a classe $\frac{b}{a}$ é um elemento bem-definido em $\mathbb{Q}$. Portanto, o inverso de $\frac{a}{b}$ é a classe $\frac{b}{a}$.

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

Inverso Multiplicativo de um Inteiro. Como um caso particular desta definição, podemos encontrar o inverso de um inteiro $a \in \mathbb{Z}^*$, que identificamos com o racional $\frac{a}{1}$. Aplicando a regra (com $b = 1$), temos:

$$\left(\frac{a}{1}\right)^{-1} = \frac{1}{a}$$

3.3.2 Divisão em $\mathbb{Q}$

Agora que estabelecemos a existência de inversos multiplicativos para todos os elementos não-nulos, podemos definir a operação de divisão. A divisão não é uma operação fundamental; ela é formalmente definida como a multiplicação pelo inverso multiplicativo.

Definição 3.3.3 (Divisão de Racionais)**.** Sejam $q_1, q_2 \in \mathbb{Q}$, com $q_2 \neq 0_{\mathbb{Q}}$. Definimos a **divisão** de q_1 por q_2, denotada $q_1 \div q_2$, como:

$$q_1 \div q_2 := q_1 \cdot (q_2)^{-1}$$

Divisão de Racionais Genéricos. Vamos aplicar esta definição aos representantes das classes. Sejam $q_1 = \frac{a}{b}$ e $q_2 = \frac{c}{d}$ (onde $c \neq 0$, $b \neq 0$, $d \neq 0$).

$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1}$$

Usando a proposição anterior, sabemos que $\left(\frac{c}{d}\right)^{-1} = \frac{d}{c}$.

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

Pela definição de multiplicação racional:

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

Divisão de Inteiros em $\mathbb{Q}$. Vamos agora analisar o caso especial que motivou esta construção: a divisão de um inteiro a por um inteiro b (com $b \neq 0$). Dentro de $\mathbb{Q}$, identificamos a com $\frac{a}{1}$ e b com $\frac{b}{1}$. Vamos aplicar a nossa definição de divisão a estes dois elementos:

$$\frac{a}{1} \div \frac{b}{1} = \frac{a}{1} \cdot \left(\frac{b}{1}\right)^{-1}$$

Como já provamos, o inverso de $\frac{b}{1}$ é $\frac{1}{b}$.

$$\frac{a}{1} \div \frac{b}{1} = \frac{a}{1} \cdot \frac{1}{b}$$

Aplicando a definição de multiplicação:

$$\frac{a}{1} \cdot \frac{1}{b} = \frac{a \cdot 1}{1 \cdot b} = \frac{a}{b}$$

Este resultado mostra que a operação divisão de a por b, quando definida formalmente como $a \cdot b^{-1}$ dentro da estrutura dos racionais, resulta exatamente na classe de equivalência $\frac{a}{b}$, portanto, a notação $\frac{a}{b}$ não é meramente uma conveniência tipográfica que se assemelha a uma divisão. A notação $\frac{a}{b}$ e a operação $a \div b$ (entendida como $a \cdot b^{-1}$) são formalmente equivalentes em seu resultado. Isso justifica o uso do símbolo de fração para denotar tanto a classe de equivalência que representa um número racional quanto o resultado da operação de divisão.

3.4 Relações de Ordem em $\mathbb{Q}$

Agora que estabelecemos a estrutura algébrica de $(\mathbb{Q}, +, \cdot)$, o próximo passo é dotar este conjunto de uma relação de ordem, assim como fizemos para $\mathbb{N}$ e $\mathbb{Z}$. A nossa definição de ordem em $\mathbb{Q}$ deve ser consistente com a ordem que já definimos em $\mathbb{Z}$.

Para evitar ambiguidade, primeiro estabelecemos que qualquer número racional pode ser representado por uma fração com denominador positivo.

Definição 3.4.1 (Ordem em $\mathbb{Q}$)**.** Sejam $q_1, q_2 \in \mathbb{Q}$. Escolhemos seus representantes $\frac{a}{b}$ e $\frac{c}{d}$ de tal forma que seus denominadores sejam positivos, ou seja, $b > 0$ e $d > 0$. Dizemos que q_1 é **menor ou igual a** q_2, e escrevemos $q_1 \leq q_2$, se e somente se a seguinte relação for válida no conjunto dos números inteiros:

$$a \cdot d \leq b \cdot c$$

Para que esta definição seja válida, devemos provar que a relação não depende dos representantes específicos que escolhemos (desde que tenham denominadores positivos).

Proposição 3.4.1 (Representação com Denominador Positivo)**.** Toda classe de equivalência $q \in \mathbb{Q}$ admite um representante da forma $\frac{a}{b}$ com $a \in \mathbb{Z}$ e $b \in \mathbb{Z}$ tal que $b > 0$.

Demonstração. Seja q um número racional. Por definição, $q = \frac{a}{b}$ para alguns inteiros a e b, com $b \neq 0$. Temos dois casos possíveis para o inteiro b:

1. **Caso 1:** $b > 0$**.** Neste caso, o representante $\frac{a}{b}$ já satisfaz a condição da proposição.

2. **Caso 2:** $b < 0$**.** Se $b < 0$, então seu inverso aditivo, $-b$, é um inteiro positivo $(-b > 0)$. Considere a classe $\frac{-a}{-b}$. Esta classe é bem-definida, pois $-b \neq 0$. Vamos

provar que esta classe é equivalente a $\frac{a}{b}$. Pela definição de equivalência, devemos verificar se:

$$a \cdot (-b) = b \cdot (-a)$$

Usando as propriedades de multiplicação em $\mathbb{Z}$, sabemos que $a \cdot (-b) = -(ab)$ e $b \cdot (-a) = -(ba)$. Como a multiplicação em $\mathbb{Z}$ é comutativa, $ab = ba$, e, portanto, $-(ab) = -(ba)$. A equivalência $\frac{a}{b} = \frac{-a}{-b}$ é verdadeira.

Assim, encontramos um representante, $\frac{a'}{b'}$ (onde $a' = -a$ e $b' = -b$), que possui um denominador $b' > 0$.

□

Proposição 3.4.2. A relação de ordem $\leq$ em $\mathbb{Q}$ é bem-definida.

Demonstração. Sejam $q_1 = \frac{a}{b} = \frac{a'}{b'}$ (com $b > 0, b' > 0$) e $q_2 = \frac{c}{d} = \frac{c'}{d'}$ (com $d > 0, d' > 0$). As hipóteses de equivalência nos dão as igualdades em $\mathbb{Z}$:

1. $a \cdot b' = b \cdot a'$
2. $c \cdot d' = d \cdot c'$

Devemos provar que $a \cdot d \leq b \cdot c \iff a' \cdot d' \leq b' \cdot c'$. Vamos provar a implicação ($\Rightarrow$). Assumimos que $a \cdot d \leq b \cdot c$. Como $b' > 0$ e $d' > 0$, a multiplicação por $b' \cdot d' > 0$ preserva a ordem em $\mathbb{Z}$:

$$(a \cdot d) \cdot (b' \cdot d') \leq (b \cdot c) \cdot (b' \cdot d')$$

Usando a associatividade e comutatividade em $\mathbb{Z}$:

$$(a \cdot b') \cdot (d \cdot d') \leq (c \cdot d') \cdot (b \cdot b')$$

Agora, usamos nossas hipóteses (1) e (2) para substituir $a \cdot b'$ e $c \cdot d'$:

$$(b \cdot a') \cdot (d \cdot d') \leq (d \cdot c') \cdot (b \cdot b')$$

Reorganizando novamente:

$$(a' \cdot d') \cdot (b \cdot d) \leq (b' \cdot c') \cdot (b \cdot d)$$

Sabemos que $b > 0$ e $d > 0$, então $b \cdot d > 0$. Pela Lei do Cancelamento para a Ordem em $\mathbb{Z}$, podemos cancelar o termo $b \cdot d$:

$$a' \cdot d' \leq b' \cdot c'$$

Como todos os passos acima são inversíveis, implicação ($\Leftarrow$) é automática. □

Proposição 3.4.3. A relação $\leq$ definida sobre o conjunto $\mathbb{Q}$ é uma **relação de ordem total**.

Demonstração. Devemos provar que a relação é reflexiva, antissimétrica, transitiva e total, usando as propriedades da ordem em $\mathbb{Z}$.

Reflexividade ($q \leq q$) Seja $q = \frac{a}{b}$ com $b > 0$. Devemos mostrar que $\frac{a}{b} \leq \frac{a}{b}$. Pela definição, isso requer $a \cdot b \leq b \cdot a$. Pela comutatividade da multiplicação em $\mathbb{Z}$, $a \cdot b = b \cdot a$, o que satisfaz a condição.

Antissimetria ($q_1 \leq q_2 \wedge q_2 \leq q_1 \implies q_1 = q_2$) Sejam $q_1 = \frac{a}{b}$ e $q_2 = \frac{c}{d}$ $(b, d > 0)$. Assumimos $q_1 \leq q_2$ e $q_2 \leq q_1$.

- $q_1 \leq q_2 \implies a \cdot d \leq b \cdot c$
- $q_2 \leq q_1 \implies b \cdot c \leq a \cdot d$

Pela antissimetria da ordem em $\mathbb{Z}$, estas duas condições implicam $a \cdot d = b \cdot c$. Pela definição de equivalência em $\mathbb{Q}$, $a \cdot d = b \cdot c$ significa que $\frac{a}{b} = \frac{c}{d}$. Portanto, $q_1 = q_2$.

Transitividade ($q_1 \leq q_2 \wedge q_2 \leq q_3 \implies q_1 \leq q_3$) Sejam $q_1 = \frac{a}{b}$, $q_2 = \frac{c}{d}$ e $q_3 = \frac{e}{f}$ (com $b, d, f > 0$). Assumimos $q_1 \leq q_2$ e $q_2 \leq q_3$.

- $q_1 \leq q_2 \implies a \cdot d \leq b \cdot c$
- $q_2 \leq q_3 \implies c \cdot f \leq d \cdot e$

Nosso objetivo é provar $q_1 \leq q_3$, ou seja, $a \cdot f \leq b \cdot e$. Da primeira hipótese, multiplicando por f (que é > 0):

$$(a \cdot d) \cdot f \leq (b \cdot c) \cdot f \implies (a \cdot f) \cdot d \leq b \cdot (c \cdot f)$$

Da segunda hipótese, multiplicando por b (que é > 0):

$$(c \cdot f) \cdot b \leq (d \cdot e) \cdot b \implies b \cdot (c \cdot f) \leq (b \cdot e) \cdot d$$

Pela transitividade da ordem em $\mathbb{Z}$, combinando as duas novas inequações:

$$(a \cdot f) \cdot d \leq (b \cdot e) \cdot d$$

Como $d > 0$, podemos cancelar o d, preservando a inequação:

$$a \cdot f \leq b \cdot e$$

Isso é precisamente a definição de $q_1 \leq q_3$.

Totalidade Sejam $q_1 = \frac{a}{b}$ e $q_2 = \frac{c}{d}$ $(b, d > 0)$. Devemos mostrar que $q_1 \leq q_2$ ou $q_2 \leq q_1$. Consideremos os inteiros $a \cdot d$ e $b \cdot c$. Como $\mathbb{Z}$ é totalmente ordenado, sabemos que uma das duas condições deve ser verdadeira:

- $a \cdot d \leq b \cdot c$, o que implica $q_1 \leq q_2$.
- $b \cdot c \leq a \cdot d$, o que implica $q_2 \leq q_1$.

Como quaisquer dois racionais são comparáveis, a relação é uma ordem total. □

Proposição 3.4.4 (Compatibilidade da Ordem com a Adição)**.** Sejam $q_1, q_2, q_3 \in \mathbb{Q}$.

$$q_1 \leq q_2 \implies q_1 + q_3 \leq q_2 + q_3$$

Demonstração. Sejam $q_1 = \frac{a}{b}$, $q_2 = \frac{c}{d}$ e $q_3 = \frac{e}{f}$, todos com denominadores positivos. A hipótese $q_1 \leq q_2$ significa $a \cdot d \leq b \cdot c$. Queremos provar que $q_1 + q_3 \leq q_2 + q_3$.

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

$$\frac{af + be}{bf} \leq \frac{cf + de}{df}$$

Como $b, d, f > 0$, os novos denominadores bf e df são positivos. Pela definição de ordem:

$$(af + be)(df) \leq (bf)(cf + de)$$

Expandindo ambos os lados usando as propriedades de $\mathbb{Z}$:

$$adf^2 + bedf \leq bcf^2 + bdef$$

Pela compatibilidade da ordem com a adição em $\mathbb{Z}$, podemos cancelar $bedf$ de ambos os lados:

$$adf^2 \leq bcf^2$$

Como $f > 0$, temos que $f^2 > 0$. Pela compatibilidade da ordem com a multiplicação em $\mathbb{Z}$, podemos cancelar f^2:

$$a \cdot d \leq b \cdot c$$

Esta é a nossa hipótese original. Como todos os passos são reversíveis, a proposição é verdadeira. □

3.5 Representação Decimal dos Racionais

Até agora, estabelecemos que todo número racional pode ser representado por uma classe de equivalência da forma $\frac{a}{b}$. No entanto, esta não é a única forma de representar

estes números. A notação que usamos no cotidiano é a **notação decimal**.

Vamos formalizar esta notação usando as estruturas que acabamos de construir.

3.5.1 Notação Decimal

Conforme introduzido no Capítulo 1, a sequência de algarismos $d_n d_{n-1} \dots d_1 d_0$, onde cada $d_i \in \{0, 1, \dots, 9\}$, é uma convenção para representar um número natural. Formalmente, esta notação é uma abreviação para uma soma de potências do inteiro 10:

$$d_n d_{n-1} \dots d_1 d_0 := \sum_{i=0}^{n} d_i \cdot 10^i = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \dots + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

Um inteiro negativo é simplesmente o inverso aditivo deste número, denotado com o prefixo "$-$".

Esta notação pode ser estendida para representar números racionais que não são inteiros, introduzindo o **separador decimal** (denotado por vírgula em português ou ponto em inglês) e algarismos que representam potências do inverso multiplicativo de 10 (ou seja, $\frac{1}{10}$).

Definição 3.5.1 (Notação Decimal Finita)**.** Sejam I um inteiro não-negativo (representado por sua notação posicional) e $d_1, d_2, \dots, d_k$ uma sequência finita de algarismos. A notação decimal $I, d_1 d_2 \dots d_k$ é definida como a representação do seguinte número racional:

$$I, d_1 d_2 \dots d_k := I + \left(\frac{d_1}{10^1} + \frac{d_2}{10^2} + \dots + \frac{d_k}{10^k} \right)$$

A parte I é chamada de **parte inteira**, e a parte $0, d_1 d_2 \dots d_k$ é a **parte fracionária**.

Exemplo 3.5.1. Vamos analisar o número racional representado pela notação $13,45$. De acordo com a definição:

$$13,45 := 13 + \left(\frac{4}{10^1} + \frac{5}{10^2} \right) = 13 + \frac{4}{10} + \frac{5}{100}$$

Para descobrir a representação desse número na notação $\frac{a}{b}$, basta encontrarmos um denominador comum (usando as operações de $\mathbb{Q}$):

$$13 + \frac{40}{100} + \frac{5}{100} = \frac{1300}{100} + \frac{40+5}{100} = \frac{1300+45}{100} = \frac{1345}{100}$$

Assim, a notação decimal $13,45$ é simplesmente uma convenção de escrita para o número racional $\frac{1345}{100}$, que, por sua vez, é a classe de equivalência $\overline{(1345, 100)}$.

Dízimas Periódicas. Nem todo número racional pode ser escrito com uma sequência finita de algarismos decimais. Por exemplo, o racional $\frac{1}{3}$ não pode. Ao tentarmos aplicar

o algoritmo da divisão (que será formalizado adiante), obtemos a representação infinita $0,333\ldots$.

Esta notação (chamada de **dízima periódica**) representa uma soma infinita:

$$\frac{3}{10} + \frac{3}{100} + \frac{3}{1000} + \ldots$$

3.5.2 O Algoritmo de Divisão Euclidiana em $\mathbb{Q}$

Mencionamos que a notação decimal $I, d_1 d_2 \ldots$ é uma representação para um número racional. Agora, formalizamos o algoritmo (o processo) pelo qual encontramos esses algarismos I e d_k a partir de um racional $q = \frac{a}{b}$ (assumindo $a, b > 0$).

Este processo é fundamentalmente uma aplicação repetida do **Algoritmo da Divisão Euclidiana**.

Passo 1: Obtenção da Parte Inteira (I) Pelo Algoritmo da Divisão, aplicamos a divisão de a por b:

$$a = b \cdot I + r_0, \quad \text{onde } 0 \leq r_0 < b$$

O quociente I é a **parte inteira** da representação decimal. O resto r_0 é o que resta a ser representado. Podemos escrever:

$$\frac{a}{b} = \frac{b \cdot I + r_0}{b} = \frac{bI}{b} + \frac{r_0}{b} = I + \frac{r_0}{b}$$

Agora, o problema se reduz a encontrar a representação decimal da fração $\frac{r_0}{b}$.

Passo 2: Obtenção do Primeiro Dígito Decimal (d_1) Seguindo a definição de notação decimal, esta parte fracionária $\frac{r_0}{b}$ é o número que queremos representar como a soma $\frac{d_1}{10} + \frac{d_2}{100} + \ldots$. Nosso objetivo imediato é isolar o algarismo d_1. Para fazer isso, multiplicamos ambos os lados da equação pelo racional $\frac{10}{1}$:

$$\frac{r_0}{b} = \frac{d_1}{10} + \frac{d_2}{100} + \frac{d_3}{1000} + \ldots$$

$$\frac{10}{1} \cdot \frac{r_0}{b} = \frac{10}{1} \cdot \left(\frac{d_1}{10} + \frac{d_2}{100} + \ldots \right)$$

Usando a distributividade e a associatividade em $\mathbb{Q}$, obtemos:

$$\frac{10 \cdot r_0}{b} = d_1 + \left(\frac{d_2}{10} + \frac{d_3}{100} + \ldots \right)$$

Esta equação é a chave: ela nos mostra que o algarismo d_1 que procuramos é, por definição, a **parte inteira** do número racional $\frac{10 \cdot r_0}{b}$, enquanto o restante $\left(\frac{d_2}{10} + \frac{d_3}{100} + \ldots\right)$ é a nova parte fracionária.

Portanto, para encontrar d_1 e o novo resto r_1, aplicamos este algoritmo aos inteiros $10 \cdot r_0$ (dividendo) e b (divisor):

$$10 \cdot r_0 = b \cdot d_1 + r_1, \quad \text{onde } 0 \leq r_1 < b$$

O quociente d_1 é precisamente o algarismo inteiro que procuramos, e o novo resto r_1 é o que será usado para encontrar d_2 no próximo passo.

Podemos verificar que d_1 é um algarismo válido (entre 0 e 9). Como sabemos que $r_0 < b$, multiplicando por 10 (uma vez que $10 > 0$, a ordem é preservada) temos $10 \cdot r_0 < 10 \cdot b$. Na divisão $10 \cdot r_0 = b \cdot d_1 + r_1$, como $r_1 \geq 0$, temos $b \cdot d_1 \leq 10 \cdot r_0$. Juntando as inequações, $b \cdot d_1 < 10 \cdot b$, o que implica $d_1 < 10$. Sendo d_1 um inteiro não-negativo, $d_1 \in \{0, 1, \ldots, 9\}$.

Ao substituir $10 \cdot r_0 = b \cdot d_1 + r_1$ de volta na expressão $\frac{r_0}{b}$, podemos ver a decomposição:

$$\frac{r_0}{b} = \frac{10 \cdot r_0}{10 \cdot b} = \frac{b \cdot d_1 + r_1}{10b} = \frac{b \cdot d_1}{10b} + \frac{r_1}{10b} = \frac{d_1}{10} + \frac{r_1}{10b}$$

Juntando com o resultado do Passo 1, a representação de $\frac{a}{b}$ se torna:

$$\frac{a}{b} = I + \frac{d_1}{10} + \frac{r_1}{10b}$$

O problema agora se reduz a encontrar a representação de $\frac{r_1}{b}$, o que é feito repetindo o mesmo processo.

Passo 3: Obtenção dos Dígitos Subsequentes (d_k) Repetimos o processo com o novo resto r_1 para encontrar d_2:

$$10 \cdot r_1 = b \cdot d_2 + r_2, \quad \text{onde } 0 \leq r_2 < b$$

Isso nos fornece d_2 como o segundo dígito decimal. A expressão se torna:

$$\frac{a}{b} = I + \frac{d_1}{10} + \frac{d_2}{100} + \frac{r_2}{100b}$$

Generalizando, para qualquer passo $k \geq 1$, encontramos o dígito d_k e o próximo resto r_k a partir do resto anterior r_{k-1} pela fórmula:

$$10 \cdot r_{k-1} = b \cdot d_k + r_k, \quad \text{onde } 0 \leq r_k < b$$

É importante destacar que a suposição de que $a > 0$ é feita por uma questão de clareza, pois a notação decimal $I, d_1 d_2 \ldots$ é mais intuitivamente definida como a soma $I + 0, d_1 d_2 \ldots$ para números não-negativos.

Esta suposição, no entanto, não invalida a generalidade do algoritmo. O **Algoritmo**

da Divisão Euclidiana, que é a base do Passo 1, é válido para qualquer $a \in \mathbb{Z}$, seja ele positivo ou negativo. Para qualquer $a \in \mathbb{Z}$ e $b > 0$, ele nos garante a existência de únicos $I \in \mathbb{Z}$ e $r_0 \in \mathbb{Z}$ tais que $a = b \cdot I + r_0$ e $0 \leq r_0 < b$.

O ponto crucial é que, independentemente do sinal de a, o resto r_0 é **sempre** não-negativo. O algoritmo de expansão decimal (Passos 2 e 3) opera inteiramente sobre a fração $\frac{r_0}{b}$, que, sendo $r_0 \geq 0$ e $b > 0$, é sempre não-negativa.

Portanto, o caso $a < 0$ é tratado da mesma forma: o Passo 1 extrai um inteiro I (que será negativo ou nulo) e uma parte fracionária não-negativa $\frac{r_0}{b}$. O restante do algoritmo se aplica sem qualquer modificação a esta parte fracionária.

Uma abordagem alternativa para encontrar a representação decimal de um racional negativo $q = \frac{a}{b}$ (com $a < 0$ e $b > 0$) é colocar o fator -1 em evidência e calcular $q = -1 \cdot (\frac{-a}{b})$. Desta forma, o algoritmo de expansão decimal descrito é aplicado à fração agora positiva $(\frac{-a}{b})$, e o sinal negativo é aplicado ao resultado final.

Terminação e Periodicidade. O algoritmo pode ter dois resultados:

1. **Terminação (Decimal Finito):** Se em algum passo k, o resto r_k se torna 0, o processo para. O termo $\frac{r_k}{10^k b}$ se anula e a representação é finita.
2. **Periodicidade (Dízima Periódica):** Se o resto r_k nunca se torna 0, ele deve assumir valores no conjunto $\{1, 2, \ldots, b-1\}$. Como este conjunto de restos possíveis é finito, após no máximo $b - 1$ passos, um resto deve se repetir. Quando um resto r_j se repete (digamos, $r_j = r_{j+p}$), a sequência de quocientes d_k também se repetirá a partir daquele ponto, gerando uma dízima periódica.

Exemplo 3.5.2. Vamos aplicar o algoritmo para encontrar a representação decimal do número racional $q = \frac{-12}{11}$. Para encontrar a representação de q, usaremos a propriedade $\frac{-12}{11} = -1 \cdot \left(\frac{12}{11}\right)$. Portanto, basta encontrar a representação decimal do número positivo $\frac{12}{11}$ e, ao final, aplicar o sinal negativo ao resultado.

Vamos focar em $q' = \frac{12}{11}$, onde $a = 12$ e $b = 11$.

Passo 1: Obtenção da Parte Inteira (I) Pelo Algoritmo da Divisão Euclidiana, devemos encontrar os únicos inteiros I e r_0 tais que $a = b \cdot I + r_0$ e $0 \leq r_0 < b$.

$$12 = 11 \cdot I + r_0 \quad (\text{com } 0 \leq r_0 < 11)$$

A única solução é:

$$12 = 11 \cdot 1 + 1$$

- A parte inteira é $I = 1$.
- O resto inicial é $r_0 = 1$.

A decomposição do nosso número positivo é:

$$\frac{12}{11} = I + \frac{r_0}{b} = 1 + \frac{1}{11}$$

Passo 2: Obtenção do Primeiro Dígito Decimal (d_1) Agora, aplicamos o processo à parte fracionária $\frac{r_0}{b} = \frac{1}{11}$. Encontramos d_1 e r_1 usando a fórmula $10 \cdot r_0 = b \cdot d_1 + r_1$:

$$10 \cdot 1 = 11 \cdot d_1 + r_1$$

$$10 = 11 \cdot 0 + 10$$

- O primeiro dígito decimal é $d_1 = 0$.
- O segundo resto é $r_1 = 10$.

Passo 3: Obtenção dos Dígitos Subsequentes (d_k) Repetimos o processo usando $r_1 = 10$ para encontrar d_2:

$$10 \cdot r_1 = b \cdot d_2 + r_2 \implies 10 \cdot 10 = 11 \cdot d_2 + r_2$$

$$100 = 11 \cdot 9 + 1$$

- O segundo dígito decimal é $d_2 = 9$.
- O terceiro resto é $r_2 = 1$.

Repetimos o processo usando $r_2 = 1$ para encontrar d_3:

$$10 \cdot r_2 = b \cdot d_3 + r_3 \implies 10 \cdot 1 = 11 \cdot d_3 + r_3$$

$$10 = 11 \cdot 0 + 10$$

- O terceiro dígito decimal é $d_3 = 0$.
- O quarto resto é $r_3 = 10$.

Terminação e Periodicidade. Neste ponto, a sequência de restos $r_0, r_1, r_2, r_3, \ldots$ é $1, 10, 1, 10, \ldots$. O resto $r_2 = 1$ é uma repetição do resto $r_0 = 1$. A sequência de dígitos $d_1, d_2, d_3, d_4, \ldots$ será $0, 9, 0, 9, \ldots$.

O algoritmo produziu a parte inteira $I = 1$ e a parte fracionária $0,0909\ldots$. O resultado para o número positivo é:

$$\frac{12}{11} = 1 + 0,0909\cdots = 1,0909\ldots$$

Aplicando o sinal negativo que deixamos em evidência no início:

$$\frac{-12}{11} = -\left(\frac{12}{11}\right) = -(1,0909\ldots) = -1,0909\ldots$$

Note que, se o algoritmo fosse aplicado diretamente ao par $a = -12$ e $b = 11$, o Passo 1 (baseado no Algoritmo da Divisão Euclidiana) nos daria a decomposição $\frac{-12}{11} = -2 + \frac{10}{11}$, levando ao resultado $-2 + 0,9090\ldots$. Ambas as representações, $-1,0909\ldots$ e $-2 + 0,9090\ldots$, descrevem o mesmo número real.

3.6 Estruturas de Grupo e Anel em $\mathbb{Q}$

Com a construção do conjunto dos números racionais ($\mathbb{Q}$) e a definição das operações de adição e multiplicação sobre ele, podemos agora investigar as estruturas algébricas formadas. Assim como fizemos para os inteiros, analisaremos $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, e a combinação $(\mathbb{Q}, +, \cdot)$.

3.6.1 Grupo aditivo

Começamos analisando a estrutura formada pelo conjunto $\mathbb{Q}$ com a operação de adição.

Proposição 3.6.1. A estrutura $(\mathbb{Q}, +)$ é um **grupo abeliano**.

Demonstração. Para provar esta afirmação, devemos verificar os axiomas de um grupo abeliano:

1. **Fechamento:** Como já demonstrado, a adição em $\mathbb{Q}$ é bem-definida, e o resultado da soma de dois racionais é sempre um racional. A operação é fechada.

2. **Associatividade:** Conforme provado anteriormente, a adição em $\mathbb{Q}$ é associativa. $(q_1 + q_2) + q_3 = q_1 + (q_2 + q_3)$.

3. **Elemento Identidade:** Como provado, o número racional $\frac{0}{1}$ (que identificamos com o inteiro 0) é o elemento identidade aditivo, pois $q + \frac{0}{1} = q$ para todo $q \in \mathbb{Q}$.

4. **Elemento Inverso:** Como demonstrado, para cada racional $q = \frac{a}{b}$, o racional $-q = \frac{-a}{b}$ é o seu inverso aditivo.

5. **Comutatividade:** Conforme provado anteriormente, a adição em $\mathbb{Q}$ é comutativa. $q_1 + q_2 = q_2 + q_1$.

Como todos os axiomas são satisfeitos, $(\mathbb{Q}, +)$ é um grupo abeliano. □

3.6.2 Grupo Multiplicativo

Analisando a multiplicação, vimos que $(\mathbb{Z}, \cdot)$ era apenas um monoide, pois a maioria dos elementos não possuía inverso multiplicativo. Vejamos o que ocorre em $\mathbb{Q}$.

A estrutura $(\mathbb{Q}, \cdot)$ não pode formar um grupo, pois o elemento identidade aditivo, $0_{\mathbb{Q}} = \frac{0}{1}$, não possui um inverso multiplicativo. Por definição, um inverso para $0_{\mathbb{Q}}$ seria um elemento $q \in \mathbb{Q}$ tal que $0_{\mathbb{Q}} \cdot q = 1_{\mathbb{Q}}$. Se $q = \frac{x}{y}$, teríamos $\frac{0}{1} \cdot \frac{x}{y} = \frac{0 \cdot x}{1 \cdot y} = \frac{0}{y}$. A equação se torna $\frac{0}{y} = \frac{1}{1}$, o que implica $0 \cdot 1 = y \cdot 1$, ou seja, $y = 0$. Contudo, o denominador de um número racional não pode ser zero, por definição. Assim, não existe tal q.

Para obter uma estrutura de grupo com a multiplicação, devemos, portanto, excluir o elemento zero.

Proposição 3.6.2. A estrutura $(\mathbb{Q}^*, \cdot)$ é um **grupo abeliano**.

Demonstração. Devemos verificar os axiomas de grupo abeliano para o conjunto $\mathbb{Q}^*$ com a operação de multiplicação:

1. **Fechamento:** Se $q_1 = \frac{a}{b}$ e $q_2 = \frac{c}{d}$ pertencem a $\mathbb{Q}^*$, então por definição $a, b, c, d \neq 0$. O produto é $q_1 \cdot q_2 = \frac{ac}{bd}$. Como $\mathbb{Z}$ é um domínio de integridade, o produto de dois inteiros não nulos é não nulo, então $ac, bd \neq 0$. Portanto, o resultado $\frac{ac}{bd}$ pertence a $\mathbb{Q}^*$.

2. **Associatividade:** Conforme provado anteriormente, a multiplicação em $\mathbb{Q}$ é associativa. A propriedade é, portanto, herdada pelo subconjunto $\mathbb{Q}^*$.

3. **Elemento Identidade:** O elemento identidade multiplicativo é $1_{\mathbb{Q}} = \frac{1}{1}$. Como seu numerador é $1 \neq 0$, o elemento identidade pertence a $\mathbb{Q}^*$.

4. **Elemento Inverso:** Conforme provado na seção sobre inversos multiplicativos em $\mathbb{Q}$, todo elemento não-nulo $q = \frac{a}{b} \in \mathbb{Q}^*$ (com $a, b \neq 0$) possui um inverso multiplicativo único, $q^{-1} = \frac{b}{a}$. Como com $a, b \neq 0$, o inverso q^{-1} pertence a $\mathbb{Q}^*$.

5. **Comutatividade:** Conforme provado anteriormente, a multiplicação em $\mathbb{Q}$ é comutativa. A propriedade é herdada por $\mathbb{Q}^*$.

Como todos os axiomas são satisfeitos, $(\mathbb{Q}^*, \cdot)$ é um grupo abeliano. □

3.6.3 Anel

Agora, combinamos as duas operações para analisar a estrutura $(\mathbb{Q}, +, \cdot)$. Já sabemos que $(\mathbb{Q}, +)$ é um grupo abeliano, a multiplicação é associativa e distributiva sobre a adição, e que a multiplicação é comutativa e possui unidade $(\frac{1}{1})$. Isso já classifica $(\mathbb{Q}, +, \cdot)$ como um **anel comutativo com unidade**.

Além disso, como $\mathbb{Z}$ é um domínio de integridade, podemos mostrar que $\mathbb{Q}$ também o é.

Proposição 3.6.3. O anel dos racionais $(\mathbb{Q}, +, \cdot)$ não possui divisores de zero.

Demonstração. Sejam $q_1 = \frac{a}{b}$ e $q_2 = \frac{c}{d}$ dois racionais tais que $q_1 \cdot q_2 = 0_{\mathbb{Q}} = \frac{0}{1}$. Suponha que $q_1 \neq 0$. Queremos provar que $q_2 = 0$. A equação $q_1 \cdot q_2 = 0$ se traduz para:

$$\frac{ac}{bd} = \frac{0}{1}$$

Pela definição de equivalência, isso significa $(ac) \cdot 1 = (bd) \cdot 0$, ou seja, $ac = 0$. Como $q_1 \neq 0$, seu numerador a deve ser diferente de zero $(a \neq 0)$. Como $\mathbb{Z}$ é um domínio de integridade e $a \neq 0$, a única forma de o produto ac ser zero é se $c = 0$. Se $c = 0$, então o racional $q_2 = \frac{c}{d} = \frac{0}{d}$. Como $(0, d) \sim (0, 1)$ (pois $0 \cdot 1 = d \cdot 0$), temos $q_2 = \frac{0}{1} = 0_{\mathbb{Q}}$. Portanto, $\mathbb{Q}$ não possui divisores de zero. □

Como $(\mathbb{Q}, +, \cdot)$ é um anel comutativo, com unidade, e sem divisores de zero, ele é um **domínio de integridade**.

3.7 A Estrutura de Corpo nos Racionais

A propriedade distintiva de $\mathbb{Q}$, que o diferencia de $\mathbb{Z}$, é a existência de inversos multiplicativos para todos os elementos não nulos. Essa propriedade adicional eleva a estrutura de anel para a de um **corpo**.

Definição 3.7.1 (Corpo)**.** Um **corpo** é um conjunto não vazio F munido de duas operações binárias, $+$ e $\cdot$, que satisfazem os seguintes axiomas:

1. $(F, +)$ é um **grupo abeliano** (com identidade 0).
2. $(F^*, \cdot)$, onde $F^* = F \setminus \{0\}$, é um **grupo abeliano** (com identidade 1).
3. A multiplicação é **distributiva** sobre a adição.

Equivalentemente, um corpo é um **anel comutativo com unidade** no qual todo elemento não nulo possui um **inverso multiplicativo**.

Proposição 3.7.1. A estrutura $(\mathbb{Q}, +, \cdot)$ é um **corpo**.

Demonstração. Verificamos as condições da definição:

1. Como provado, $(\mathbb{Q}, +)$ é um grupo abeliano.
2. Como provado, $(\mathbb{Q}^*, \cdot)$ é um grupo abeliano.
3. Como provado, a multiplicação é distributiva sobre a adição em $\mathbb{Q}$.

Alternativamente, usando a segunda definição:

1. Como provado, $(\mathbb{Q}, +, \cdot)$ é um anel comutativo com unidade.
2. Como provado, todo elemento não nulo $q \in \mathbb{Q}^*$ possui um inverso multiplicativo $q^{-1} \in \mathbb{Q}^*$.

Como todas as condições são satisfeitas, $(\mathbb{Q}, +, \cdot)$ é um corpo. É conhecido como o **corpo dos números racionais**. □

A estrutura de corpo é fundamental em álgebra, pois garante que as quatro operações aritméticas básicas (adição, subtração, multiplicação e divisão por elementos não nulos) podem ser realizadas sem sair do conjunto e mantendo as propriedades

Proposição 3.7.2 (Ideais de um Corpo)**.** Seja $(K, +, \cdot)$ um corpo. Os únicos ideais de K são os ideais triviais: o ideal nulo $\{0_K\}$ e o próprio corpo K.

Demonstração. Seja I um ideal do corpo K. Por definição, $(I, +)$ é um subgrupo de $(K, +)$, e I é fechado sob a multiplicação por qualquer elemento de K. Temos dois casos a considerar para I:

- **Caso 1:** $I = \{0_K\}$**.** Neste caso, I é o ideal nulo, que é um dos ideais triviais.
- **Caso 2:** $I \neq \{0_K\}$**.** Se o ideal I não é o ideal nulo, então ele deve conter pelo menos um elemento $x \in I$ tal que $x \neq 0_K$.

  Como K é um corpo, todo elemento não nulo possui um inverso multiplicativo. Portanto, existe $x^{-1} \in K$ tal que $x \cdot x^{-1} = 1_K$.

  Pela propriedade de absorção de um ideal, se $x \in I$ e $k \in K$, então $k \cdot x \in I$. Como x^{-1} é um elemento de K, temos:

$$x^{-1} \cdot x \in I$$

  Isso implica que a identidade multiplicativa, 1_K, pertence ao ideal:

$$1_K \in I$$

Agora, usamos a propriedade de absorção novamente. Como $1_K \in I$, para qualquer elemento $k \in K$, o produto $k \cdot 1_K$ deve pertencer a I.

$$\forall k \in K, \quad k \cdot 1_K = k \implies k \in I$$

Isso mostra que todo elemento de K pertence a I, ou seja, $K \subseteq I$.

Como I é um subconjunto de K ($I \subseteq K$) e K é um subconjunto de I ($K \subseteq I$), a única possibilidade é $I = K$.

Como estes são os únicos dois casos possíveis, provamos que os únicos ideais de um corpo K são $\{0_K\}$ e K. □

Proposição 3.7.3. Todo corpo $(F, +, \cdot)$ é um domínio de integridade.

Demonstração. Por definição, um corpo é um anel comutativo com unidade. Resta-nos provar que F não possui divisores de zero. Sejam $a, b \in F$ tais que $a \cdot b = 0_F$. Suponha, por contradição, que $a \neq 0_F$ e $b \neq 0_F$. Como $a \neq 0_F$, ele pertence ao grupo multiplicativo F^* e, portanto, possui um inverso multiplicativo a^{-1}. Multiplicando ambos os lados da equação $a \cdot b = 0_F$ à esquerda por a^{-1}:

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_F$$

Pela associatividade da multiplicação e pela propriedade do zero:

$$(a^{-1} \cdot a) \cdot b = 0_F$$

$$1_F \cdot b = 0_F$$

$$b = 0_F$$

Isso contradiz nossa suposição de que $b \neq 0_F$. Portanto, a suposição inicial de que a e b eram ambos não-nulos é falsa. Concluímos que $a = 0_F$ ou $b = 0_F$, e F não possui divisores de zero. □

A estrutura de corpo não se limita a conjuntos infinitos como $\mathbb{Q}$. No Capítulo 2, analisamos o anel dos inteiros módulo n, $(\mathbb{Z}_n, +, \cdot)$. Podemos agora determinar exatamente quando essa estrutura também forma um corpo.

Teorema 3.7.1. O anel dos inteiros módulo n, $(\mathbb{Z}_n, +, \cdot)$, é um corpo se, e somente se, n é um número primo.

Demonstração. Sabemos que $(\mathbb{Z}_n, +, \cdot)$ é um anel comutativo com unidade. Para ser um corpo, todo elemento não nulo $[a]_n \in \mathbb{Z}_n$ (com $[a]_n \neq [0]_n$) deve possuir um inverso

multiplicativo.

($\Rightarrow$) Se $\mathbb{Z}_n$ é um corpo, então n é primo.
Provamos pela contrapositiva. Suponha que n **não** é primo. Se $n = 1$, $\mathbb{Z}_1 = \{[0]\}$, que não é um corpo pois $1 \neq 0$. Se n é composto, então $n = a \cdot b$ para inteiros a, b com $1 < a < n$ e $1 < b < n$. Isso significa que $[a]_n \neq [0]_n$ e $[b]_n \neq [0]_n$. No entanto, o produto deles em $\mathbb{Z}_n$ é:

$$[a]_n \cdot [b]_n = [ab]_n = [n]_n = [0]_n$$

Encontramos dois elementos não nulos cujo produto é nulo. Pela proposição anterior (de que todo corpo é um domínio de integridade), $\mathbb{Z}_n$ não pode ser um corpo, pois possui divisores de zero. Portanto, se $\mathbb{Z}_n$ é um corpo, n deve ser primo.

($\Leftarrow$) Se $n = p$ é primo, então $\mathbb{Z}_p$ é um corpo.
Seja p um número primo. Devemos mostrar que todo elemento $[a]_p \in \mathbb{Z}_p$, com $[a]_p \neq [0]_p$, possui um inverso multiplicativo. A condição $[a]_p \neq [0]_p$ significa que $p \nmid a$. Como p é primo, a única possibilidade é que a e p sejam primos entre si, ou seja, $\text{mdc}(a, p) = 1$. Pela Identidade de Bèzout, se $\text{mdc}(a, p) = 1$, então existem inteiros x e y tais que:

$$a \cdot x + p \cdot y = 1$$

Agora, vamos aplicar o homomorfismo de projeção canônica $\pi : \mathbb{Z} \to \mathbb{Z}_p$:

$$\pi(a \cdot x + p \cdot y) = \pi(1)$$

$$\pi(ax) + \pi(py) = [1]_p$$

$$([a]_p \cdot [x]_p) + ([p]_p \cdot [y]_p) = [1]_p$$

Como $[p]_p = [0]_p$, o segundo termo se anula:

$$([a]_p \cdot [x]_p) + ([0]_p \cdot [y]_p) = [1]_p$$

$$[a]_p \cdot [x]_p = [1]_p$$

Isso demonstra que o elemento $[x]_p$ é o inverso multiplicativo de $[a]_p$. Como todo elemento não nulo possui um inverso, $(\mathbb{Z}_p, +, \cdot)$ é um corpo. □

3.7.1 Corpos Ordenados

Definimos a relação de ordem $\leq$ em $\mathbb{Q}$ e provamos que ela é uma ordem total. Agora, investigamos como essa ordem interage com a estrutura de corpo.

Definição 3.7.2 (Corpo Ordenado)**.** Um corpo $(K, +, \cdot)$ é dito um **corpo ordenado** se ele for munido de uma relação de ordem total $\leq$ que seja compatível com ambas as operações do corpo:

1. **Compatibilidade com a Adição:** $\forall a, b, c \in K, \quad a \leq b \implies a + c \leq b + c.$
2. **Compatibilidade com a Multiplicação:** $\forall a, b, c \in K, \quad (a \leq b \wedge c \geq 0_K) \implies a \cdot c \leq b \cdot c.$

Proposição 3.7.4. O corpo dos racionais $(\mathbb{Q}, +, \cdot)$, com a relação de ordem $\leq$ definida anteriormente, é um corpo ordenado.

Demonstração. Já provamos que $(\mathbb{Q}, \leq)$ é um conjunto totalmente ordenado e que a ordem é compatível com a adição. Resta-nos provar a compatibilidade com a multiplicação.

Sejam $q_1 = \frac{a}{b}$, $q_2 = \frac{c}{d}$ e $q_3 = \frac{e}{f}$ números racionais, com $b, d, f > 0$. Assumimos as hipóteses $q_1 \leq q_2$ e $q_3 \geq 0_{\mathbb{Q}}$.

- $q_1 \leq q_2 \implies a \cdot d \leq b \cdot c$ (em $\mathbb{Z}$).
- $q_3 \geq 0_{\mathbb{Q}} \implies \frac{e}{f} \geq \frac{0}{1} \implies e \cdot 1 \geq f \cdot 0 \implies e \geq 0$ (em $\mathbb{Z}$).

Queremos provar que $q_1 \cdot q_3 \leq q_2 \cdot q_3$. Note que

$$\frac{a}{b} \cdot \frac{e}{f} \leq \frac{c}{d} \cdot \frac{e}{f} \iff \frac{ae}{bf} \leq \frac{ce}{df}$$

Como $b, d, f > 0$, os novos denominadores bf e df são positivos. Pela definição de ordem em $\mathbb{Q}$, devemos verificar se:

$$(ae)(df) \leq (bf)(ce)$$

Usando a associatividade e comutatividade em $\mathbb{Z}$:

$$(ad)(ef) \leq (bc)(ef)$$

Seja $k = ef$. Como $e \geq 0$ e $f > 0$, temos $k \geq 0$. Partimos da nossa hipótese $a \cdot d \leq b \cdot c$. Como a ordem em $\mathbb{Z}$ é compatível com a multiplicação por um inteiro não-negativo, podemos multiplicar ambos os lados por $k = ef$:

$$(ad)k \leq (bc)k \implies (ad)(ef) \leq (bc)(ef)$$

Esta é a condição que queríamos provar. Portanto, a ordem em $\mathbb{Q}$ é compatível com a multiplicação. □

Proposição 3.7.5 (Corpos Ordenados são Densamente Ordenados)**.** Todo corpo ordenado $(K, +, \cdot, \leq)$ é **densamente ordenado**. Isto é, para quaisquer $x, y \in K$ com $x < y$, existe um outro elemento $z \in K$ tal que $x < z < y$.

Demonstração. Sejam $x, y \in K$ com $x < y$. Em qualquer corpo ordenado, por convenção $1 > 0$ (onde 1 é a identidade multiplicativa). Pela compatibilidade com a adição, $2 = 1 + 1 > 1 + 0 = 1$, então $2 > 0$. Como $2 \neq 0$, seu inverso multiplicativo, $\frac{1}{2}$, existe em K. Além disso, como $2 > 0$, seu inverso $\frac{1}{2}$ também deve ser positivo.

Consideremos o elemento $z = (x + y) \cdot \frac{1}{2}$.

1. z pertence a K: Como K é um corpo, ele é fechado sob adição $(x+y)$ e multiplicação (multiplicar por $\frac{1}{2}$), portanto z pertence a K.

2. $z > x$: Partimos da hipótese $x < y$. Pela compatibilidade da ordem com a adição, somamos x a ambos os lados:

$$x + x < y + x \implies 2x < x + y$$

   Como $\frac{1}{2}$ é positivo, multiplicamos ambos os lados (compatibilidade da multiplicação):

$$\frac{1}{2}(2x) < \frac{1}{2}(x + y) \implies x < z$$

3. $z < y$: Partimos da hipótese $x < y$. Somamos y a ambos os lados (compatibilidade da adição):

$$x + y < y + y \implies x + y < 2y$$

   Multiplicando pelo elemento positivo $\frac{1}{2}$:

$$\frac{1}{2}(x + y) < \frac{1}{2}(2y) \implies z < y$$

Como $x < z$ e $z < y$, encontramos um elemento $z \in K$ estritamente entre x e y. □

Corolário 3.7.1.1. O corpo ordenado $(\mathbb{Q}, +, \cdot, \leq)$ é **densamente ordenado**.

Demonstração. Conforme demonstrado anteriormente, $(\mathbb{Q}, +, \cdot, \leq)$ satisfaz todos os axiomas de um corpo ordenado. A proposição anterior estabelece que *todo* corpo ordenado é densamente ordenado. Portanto, como um caso particular dessa proposição, $\mathbb{Q}$ é densamente ordenado. □

Proposição 3.7.6 (Propriedade Arquimediana)**.** O corpo ordenado $\mathbb{Q}$ é **Arquimediano.** Isto é, para quaisquer $x, y \in \mathbb{Q}$ com $x > 0$, existe um inteiro $n \in \mathbb{N}^*$ (identificado com $\frac{n}{1} \in \mathbb{Q}$) tal que $n \cdot x > y$.

Demonstração. Sejam $x = \frac{a}{b}$ e $y = \frac{c}{d}$. Como $x > 0$, podemos escolher seus representantes tais que $a > 0$ e $b > 0$. Para y, podemos escolher $d > 0$ (o sinal de c será o sinal de y). Queremos encontrar $n \in \mathbb{N}^*$ tal que $n \cdot \frac{a}{b} > \frac{c}{d}$, isto é,

$$\frac{na}{b} > \frac{c}{d}$$

Pela definição de ordem, como $b, d > 0$, isso é equivalente a provar em $\mathbb{Z}$:

$$(na)d > bc \implies n(ad) > bc$$

Como $a > 0$ e $d > 0$, o produto ad é um inteiro positivo, $ad \geq 1$. O produto bc é um inteiro (positivo, negativo ou nulo). Se $bc \leq 0$, qualquer $n \geq 1$ satisfaz a inequação, pois $n(ad)$ é positivo. Se $bc > 0$, estamos procurando um n tal que $n > \frac{bc}{ad}$. Como $\mathbb{N}$ não é limitado superiormente em $\mathbb{Q}$, podemos sempre escolher o inteiro $n = (bc) + 1$. Como $ad \geq 1$, temos $n(ad) \geq n = (bc) + 1 > bc$. Em ambos os casos, tal n existe. □

3.7.2 A Incompletude de $\mathbb{Q}$

A propriedade de densidade sugere que a reta numérica está completa os racionais. No entanto, esta intuição está incorreta. Apesar de denso, o conjunto $\mathbb{Q}$ é incompleto. Demonstraremos esta incompletude provando que existe uma equação algébrica simples, $q^2 = 2$, que não possui solução dentro do corpo dos racionais.

Proposição 3.7.7. Não existe número racional $q \in \mathbb{Q}$ tal que $q^2 = 2$.

Demonstração. A prova será feita por contradição. Suponha que exista tal $q \in \mathbb{Q}$. Podemos escrevê-lo como $q = \frac{a}{b}$, onde $a, b \in \mathbb{Z}$ e $b \neq 0$. Podemos, adicionalmente, assumir que a fração está em sua forma irredutível, ou seja, a e b não possuem fatores primos em comum (o que implica $\text{mdc}(a, b) = 1$).

A equação $q^2 = 2$ se torna:

$$\left(\frac{a}{b}\right)^2 = 2 \implies \frac{a^2}{b^2} = \frac{2}{1}$$

Pela definição de equivalência, isso nos fornece uma equação em $\mathbb{Z}$:

$$a^2 \cdot 1 = b^2 \cdot 2 \implies a^2 = 2b^2$$

Esta equação mostra que a^2 é um número par (múltiplo de 2). Pelo Lema de Euclides, sabemos que se um número primo p divide um produto $x \cdot y$, então p deve dividir x ou p deve dividir y. Como 2 é primo e divide a^2 (que é $a \cdot a$), concluímos que 2 deve dividir a. Portanto, a é um número par.

Podemos, então, escrever $a = 2k$ para algum $k \in \mathbb{Z}$. Substituindo $a = 2k$ na equação original $a^2 = 2b^2$:

$$(2k)^2 = 2b^2 \implies 4k^2 = 2b^2$$

Dividindo ambos os lados por 2 (pela lei do cancelamento em $\mathbb{Z}$):

$$2k^2 = b^2$$

Esta nova equação mostra que b^2 também é um número par. Se b^2 é par, b também deve ser par.

Chegamos a uma contradição. Concluímos que:

1. a é par (portanto, $2 \mid a$).
2. b é par (portanto, $2 \mid b$).

Isso significa que a e b compartilham o fator primo 2. Isso contradiz diretamente nossa suposição inicial de que a fração $\frac{a}{b}$ era irredutível ($\text{mdc}(a, b) = 1$).

Como a suposição inicial nos levou a uma contradição, ela deve ser falsa. Portanto, não existe número racional q tal que $q^2 = 2$. □

Esta demonstração revela que, embora possamos encontrar números racionais cujo quadrado é tão próximo de 2 quanto quisermos (por exemplo, $1.41^2 = 1.9881$, $1.414^2 = 1.999396$), o valor exato que satisfaz a equação $q^2 = 2$ não pertence ao conjunto $\mathbb{Q}$. Esta falha é a motivação para a construção do próximo conjunto numérico, os Números Reais ($\mathbb{R}$).

Capítulo 4

Reais

4.1 A Ideia de Aproximação

No capítulo anterior, estabelecemos que o corpo dos racionais $(\mathbb{Q}, +, \cdot, \leq)$ é um corpo densamente ordenado e arquimediano. No entanto, encerramos o capítulo demonstrando a sua **incompletude**: provamos que não existe um número racional q tal que $q^2 = 2$.

Esta descoberta revela a existência de buracos na reta numérica racional. Embora não exista um racional tal que seu quadrado seja igual a 2, podemos encontrar racionais que se aproximam dele tanto quanto quisermos. Por exemplo, a sequência de números racionais:

$$\begin{aligned} s_0 = 1 \quad &\to \quad s_0^2 = 1 \\ s_1 = 1,4 \quad &\to \quad s_1^2 = 1,96 \\ s_2 = 1,41 \quad &\to \quad s_2^2 = 1,9881 \\ s_3 = 1,414 \quad &\to \quad s_3^2 = 1,999396 \\ s_4 = 1,4142 \quad &\to \quad s_4^2 = 1,99996164 \\ \vdots \quad &\to \quad \vdots \end{aligned}$$

parece estar chegando perto de algum valor. A ideia fundamental da construção dos números reais é definir os buracos através das próprias sequências que os aproximam.

Para que essa ideia seja rigorosa, não podemos definir uma aproximação com base em sua distância a um limite que ainda não provamos existir. Em vez disso, focamos em uma propriedade da própria sequência: seus termos se tornam arbitrariamente próximos uns dos outros.

Para entender melhor esse conceito, precisamos da noção de distância entre dois números racionais.

Definição 4.1.1 (Valor Absoluto em $\mathbb{Q}$)**.** Seja $q \in \mathbb{Q}$. O **valor absoluto** (ou **módulo**)

de q, denotado por $|q|$, é definido com base na ordem total de $\mathbb{Q}$:

$$|q| = \begin{cases} q, & \text{se } q \geq 0 \\ -q, & \text{se } q < 0 \end{cases}$$

A **distância** entre dois racionais x e y é definida como $|x - y|$.

Proposição 4.1.1 (Propriedades do Valor Absoluto)**.** Sejam $x, y \in \mathbb{Q}$. As seguintes propriedades são válidas:

1. $|x| \geq 0$
2. $|x| = 0 \iff x = 0$
3. $|x \cdot y| = |x| \cdot |y|$
4. **(Desigualdade Triangular)** $|x + y| \leq |x| + |y|$

Demonstração. As três primeiras propriedades decorrem diretamente da definição e das propriedades de ordem em $\mathbb{Q}$. Vamos provar a quarta propriedade, a Desigualdade Triangular.

Pela definição de valor absoluto, sabemos que para qualquer $q \in \mathbb{Q}$, temos $q \leq |q|$ e $-q \leq |q|$. Sejam $x, y \in \mathbb{Q}$. Temos:

$$x \leq |x| \quad \text{e} \quad y \leq |y|$$

Usando a compatibilidade da ordem com a adição, podemos somar as duas inequações:

$$x + y \leq |x| + |y| \quad (1)$$

Da mesma forma, temos:

$$-x \leq |x| \quad \text{e} \quad -y \leq |y|$$

Somando estas duas inequações:

$$(-x) + (-y) \leq |x| + |y|$$

$$-(x + y) \leq |x| + |y| \quad (2)$$

Agora, consideramos o valor absoluto de $|x + y|$. Pela definição de valor absoluto, $|x + y|$ é igual a $x + y$ ou $-(x + y)$.

- Se $|x + y| = x + y$, a inequação (1) nos fornece diretamente $|x + y| \leq |x| + |y|$.
- Se $|x + y| = -(x + y)$, a inequação (2) nos fornece diretamente $|x + y| \leq |x| + |y|$.

Como em todos os casos a relação é válida, a Desigualdade Triangular está provada. □

Corolário 4.1.0.1 (Desigualdade Triangular Inversa)**.** Para quaisquer $x, y \in \mathbb{Q}$, temos:

$$||x| - |y|| \leq |x - y|$$

Demonstração. Pela Desigualdade Triangular:

$$|x| = |(x - y) + y| \leq |x - y| + |y|$$

Isolando $|x| - |y|$, obtemos:

$$|x| - |y| \leq |x - y| \quad (1)$$

Trocando os papéis de x e y:

$$|y| = |(y - x) + x| \leq |y - x| + |x|$$

Isolando:

$$|y| - |x| \leq |y - x|$$

Como $|y - x| = |x - y|$, podemos multiplicar por -1 (invertendo a desigualdade):

$$-(|x| - |y|) \leq |x - y| \quad (2)$$

As inequações (1) e (2) mostram que $|x - y|$ é um limite superior para $(|x| - |y|)$ e $-([x| - |y|)$. Isso é, por definição, equivalente a:

$$||x| - |y|| \leq |x - y|$$

□

4.2 O Anel das Sequências Racionais $\mathbb{Q}^{\mathbb{N}}$

Definição 4.2.1 (Sequência de Racionais)**.** Uma **sequência** de números racionais é uma função $f : \mathbb{N} \to \mathbb{Q}$. Denotamos a imagem de n por $f(n)$ ou f_n, e a sequência inteira por $(f_n)_{n\in\mathbb{N}}$.

$$(f_n) = (f_0, f_1, f_2, \dots)$$

Exemplo 4.2.1 (Exemplos de Sequências Racionais)**.**

- $(1, 1, 1, \dots)$: Uma sequência constante, onde $q_n = 1$ para todo n.
- $\left(\frac{1}{n+1}\right)_{n\in\mathbb{N}} = \left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right)$.

- $(n)_{n\in\mathbb{N}} = (0, 1, 2, 3, \dots)$.

Definição 4.2.2 (Anel de Sequências $\mathbb{Q}^{\mathbb{N}}$)**.** Seja $\mathbb{Q}^{\mathbb{N}}$ o conjunto de todas as sequências de números racionais. Definimos duas operações binárias, adição $(+)$ e multiplicação $(\cdot)$, de forma pontual (ou componente a componente). Para quaisquer $f, g \in \mathbb{Q}^{\mathbb{N}}$:

- **Adição:** A sequência $f + g$ é definida por $(f + g)(n) := f(n) + g(n)$ para todo $n \in \mathbb{N}$.
- **Multiplicação:** A sequência $f \cdot g$ é definida por $(f \cdot g)(n) := f(n) \cdot g(n)$ para todo $n \in \mathbb{N}$.

Proposição 4.2.1. A estrutura $(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$ é um **anel comutativo com unidade**.

Demonstração. Para demonstrar que $\mathbb{Q}^{\mathbb{N}}$ é um anel comutativo com unidade, devemos verificar que $(\mathbb{Q}^{\mathbb{N}}, +)$ é um grupo comutativo, que $(\mathbb{Q}^{\mathbb{N}}, \cdot)$ é um monoide comutativo, e que a multiplicação distribui sobre a adição.

Todas essas propriedades são herdadas diretamente das propriedades do corpo $(\mathbb{Q}, +, \cdot)$, aplicadas a cada componente $n \in \mathbb{N}$. Sejam $f, g, h \in \mathbb{Q}^{\mathbb{N}}$.

- $(\mathbb{Q}^{\mathbb{N}}, +)$ **é um Grupo comutativo:**
  - Fechamento: A soma $f(n) + g(n)$ é uma soma de racionais, resultando em um racional. Logo, a sequência $f + g$ pertence a $\mathbb{Q}^{\mathbb{N}}$.
  - Associatividade: Para todo n,

    $$((f+g)+h)(n) = (f(n)+g(n))+h(n) = f(n)+(g(n)+h(n)) = (f+(g+h))(n)$$

    Isso se deve à associatividade da adição em $\mathbb{Q}$.
  - Comutatividade: Para todo n,

    $$(f + g)(n) = f(n) + g(n) = g(n) + f(n) = (g + f)(n)$$

    Isso se deve à comutatividade da adição em $\mathbb{Q}$.
  - Identidade Aditiva: Seja $\mathbf{0}$ a sequência constante definida por $\mathbf{0}(n) = 0$ para todo n. Então:

    $$(f + \mathbf{0})(n) = f(n) + \mathbf{0}(n) = f(n) + 0 = f(n)$$

    Logo, $\mathbf{0}$ é o elemento identidade aditivo.

– Inverso Aditivo: Para uma sequência f, seja $-f$ a sequência definida por $(-f)(n) = -f(n)$. Então:

$$(f + (-f))(n) = f(n) + (-f(n)) = f(n) - f(n) = 0 = \mathbf{0}(n)$$

Logo, toda sequência f possui um inverso aditivo $-f \in \mathbb{Q}^{\mathbb{N}}$.

- $(\mathbb{Q}^{\mathbb{N}}, \cdot)$ **é um Monoide comutativo:**

  – Fechamento: O produto $f(n) \cdot g(n)$ é um racional. Logo, a sequência $f \cdot g$ pertence a $\mathbb{Q}^{\mathbb{N}}$.

  – Associatividade: Para todo n,

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

Isso se deve à associatividade da multiplicação em $\mathbb{Q}$.

– Comutatividade: Para todo n,

$$(f \cdot g)(n) = f(n) \cdot g(n) = g(n) \cdot f(n) = (g \cdot f)(n)$$

Isso se deve à comutatividade da multiplicação em $\mathbb{Q}$.

– Identidade Multiplicativa: Seja $\mathbf{1}$ a sequência constante definida por $\mathbf{1}(n) = 1$ para todo n. Então:

$$(f \cdot \mathbf{1})(n) = f(n) \cdot \mathbf{1}(n) = f(n) \cdot 1 = f(n)$$

Logo, $\mathbf{1}$ é o elemento identidade multiplicativo (a unidade).

- **Distributividade:** Devemos verificar $f \cdot (g + h) = (f \cdot g) + (f \cdot h)$. Para todo n:

$$\begin{aligned}(f \cdot (g + h))(n) &= f(n) \cdot (g + h)(n) \\ &= f(n) \cdot (g(n) + h(n)) \\ &= (f(n) \cdot g(n)) + (f(n) \cdot h(n)) \quad \text{(Distributividade em } \mathbb{Q}) \\ &= (f \cdot g)(n) + (f \cdot h)(n) \\ &= ((f \cdot g) + (f \cdot h))(n)\end{aligned}$$

Como a multiplicação é comutativa, o mesmo vale para a distributividade à direita.

Como todas as condições são satisfeitas, $(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$ é um anel comutativo com unidade.

□

4.3 O Anel das Sequências de Cauchy

4.3.1 Definição de Sequências de Cauchy

Nosso objetivo é formalizar a noção de uma sequência de aproximação em $\mathbb{Q}$, cujos termos se tornam arbitrariamente próximos uns dos outros.

Definição 4.3.1 (Sequência de Cauchy)**.** Uma sequência de números racionais $(q_n)_{n\in\mathbb{N}}$ é dita uma **Sequência de Cauchy**, se seus termos se tornam arbitrariamente próximos uns dos outros à medida que n aumenta. Ou seja, se para qualquer $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, for possível encontrar um ponto na sequência, $N \in \mathbb{N}$, a partir do qual a distância entre quaisquer dois termos é menor que ϵ. Formalmente:

$$\forall \epsilon > 0, \exists N \in \mathbb{N} \text{ tal que } \forall m, n \geq N, |q_m - q_n| < \epsilon$$

Proposição 4.3.1. Toda Sequência de Cauchy em $\mathbb{Q}$ é limitada.

Demonstração. Seja (q_n) uma sequência de Cauchy. Pela definição, para $\epsilon = 1$, existe um $N \in \mathbb{N}$ tal que para todos $m, n \geq N$, temos $|q_m - q_n| < 1$.

Fixando $n = N$, isso implica que para todo $m \geq N$, temos $|q_m - q_N| < 1$. Pela Desigualdade Triangular Inversa, sabemos que $||q_m| - |q_N|| \leq |q_m - q_N|$. Combinando as duas inequações, temos $||q_m| - |q_N|| < 1$, o que implica:

$$-1 < |q_m| - |q_N| < 1$$

Da primeira parte da inequação, $|q_m| - |q_N| < 1$, obtemos:

$$|q_m| < |q_N| + 1$$

Isso nos dá um limite para todos os termos da sequência *a partir de* N.

Agora, devemos considerar todos os termos. Seja M o valor máximo do conjunto finito de números racionais:

$$M = \max\{|q_0|, |q_1|, \ldots, |q_{N-1}|, |q_N| + 1\}$$

Como este conjunto é finito, M está bem-definido.

- Para $n < N$, temos $|q_n| \leq M$ pela definição de M.
- Para $n \geq N$, temos $|q_n| < |q_N| + 1 \leq M$.

Portanto, encontramos um $M > 0$ tal que $|q_n| \leq M$ para *todo* $n \in \mathbb{N}$, e a sequência é limitada. □

4.3.2 O Anel $\mathcal{C}(\mathbb{Q})$

Definimos $\mathcal{C}(\mathbb{Q})$ como o conjunto de todas as sequências de Cauchy de números racionais. Este é um subconjunto do anel de todas as sequências, $(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$, onde as operações são definidas ponto-a-ponto. Vamos agora provar que $\mathcal{C}(\mathbb{Q})$ é fechado sob essas operações, formando um subanel.

Definição 4.3.2. Seja $\mathcal{C}(\mathbb{Q})$ o conjunto de todas as sequências de Cauchy de números racionais.

$$\mathcal{C}(\mathbb{Q}) = \{(q_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid (q_n) \text{ é uma Sequência de Cauchy}\}$$

Para $(q_n), (p_n) \in \mathcal{C}(\mathbb{Q})$, as operações de adição e multiplicação são herdadas de $\mathbb{Q}^{\mathbb{N}}$:

- **Soma:** $(q_n) + (p_n) := (q_n + p_n)$
- **Multiplicação:** $(q_n) \cdot (p_n) := (q_n \cdot p_n)$

Proposição 4.3.2. A estrutura $(\mathcal{C}(\mathbb{Q}), +, \cdot)$ é um subanel comutativo com unidade do anel $(\mathbb{Q}^{\mathbb{N}}, +, \cdot)$.

Demonstração. Para provar que $\mathcal{C}(\mathbb{Q})$ é um subanel de $\mathbb{Q}^{\mathbb{N}}$, devemos verificar três condições, utilizando o critério para subanéis:

1. $\mathcal{C}(\mathbb{Q})$ não é vazio.
2. $\mathcal{C}(\mathbb{Q})$ é fechado sob a subtração.
3. $\mathcal{C}(\mathbb{Q})$ é fechado sob a multiplicação.

1. Não Vazio: A sequência nula, $\mathbf{0} = (0, 0, 0, \dots)$, é uma sequência de Cauchy. Para qualquer $\epsilon > 0$, podemos escolher $N = 0$, e para todos $n, m \geq 0$, temos $|0 - 0| = 0 < \epsilon$. Como $\mathbf{0} \in \mathcal{C}(\mathbb{Q})$, o conjunto não é vazio. (Da mesma forma, a sequência unidade $\mathbf{1} = (1, 1, \dots)$ também é de Cauchy).

2. Fechamento sob Subtração: Sejam (q_n) e (p_n) duas sequências de Cauchy. Devemos mostrar que a sequência diferença $(d_n) = (q_n - p_n)$ também é de Cauchy.

Dado $\epsilon > 0$:

- Como (q_n) é Cauchy, existe N_1 tal que $\forall m, n \geq N_1, |q_m - q_n| < \epsilon/2$.
- Como (p_n) é Cauchy, existe N_2 tal que $\forall m, n \geq N_2, |p_m - p_n| < \epsilon/2$.

Seja $N = \max(N_1, N_2)$. Para $m, n \geq N$, aplicamos a Desigualdade Triangular:

$$\begin{aligned} |d_m - d_n| &= |(q_m - p_m) - (q_n - p_n)| \\ &= |(q_m - q_n) + (p_n - p_m)| \\ &\leq |q_m - q_n| + |p_n - p_m| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon \end{aligned}$$

Portanto, $(q_n - p_n)$ é uma sequência de Cauchy.

3. Fechamento sob Multiplicação: Sejam (q_n) e (p_n) duas sequências de Cauchy. Devemos mostrar que a sequência produto $(m_n) = (q_n \cdot p_n)$ também é de Cauchy.

Primeiro, como toda sequência de Cauchy é limitada, existem racionais $M_q > 0$ e $M_p > 0$ tais que $|q_n| \leq M_q$ e $|p_n| \leq M_p$ para todo n.

Seja $\epsilon > 0$. Queremos mostrar que $|m_m - m_n| = |q_m p_m - q_n p_n| < \epsilon$ para m, n suficientemente grandes. Usamos o artifício de somar e subtrair o termo $q_m p_n$:

$$\begin{aligned} |q_m p_m - q_n p_n| &= |q_m p_m - q_m p_n + q_m p_n - q_n p_n| \\ &\leq |q_m(p_m - p_n)| + |p_n(q_m - q_n)| \\ &= |q_m| \cdot |p_m - p_n| + |p_n| \cdot |q_m - q_n| \\ &\leq M_q \cdot |p_m - p_n| + M_p \cdot |q_m - q_n| \end{aligned}$$

Como (q_n) e (p_n) são de Cauchy, podemos tornar as diferenças pequenas. Dado $\epsilon > 0$, existem N_1, N_2 tais que:

- Para $m, n \geq N_1$, $|q_m - q_n| < \frac{\epsilon}{2M_p}$
- Para $m, n \geq N_2$, $|p_m - p_n| < \frac{\epsilon}{2M_q}$

Seja $N = \max(N_1, N_2)$. Para $m, n \geq N$, temos:

$$|q_m p_m - q_n p_n| \leq M_q \cdot \left(\frac{\epsilon}{2M_q}\right) + M_p \cdot \left(\frac{\epsilon}{2M_p}\right) = \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

Portanto, $(q_n \cdot p_n)$ é uma sequência de Cauchy.

Como $\mathcal{C}(\mathbb{Q})$ é um subconjunto não vazio de $\mathbb{Q}^{\mathbb{N}}$ fechado sob subtração e multiplicação, ele é um subanel. Além disso, como $\mathbb{Q}^{\mathbb{N}}$ é comutativo e possui unidade $\mathbf{1}$, e $\mathbf{1} = (1, 1, \dots)$ é uma sequência de Cauchy, $\mathcal{C}(\mathbb{Q})$ é um anel comutativo com unidade. □

4.4 O Ideal das Sequências Nulas

A intuição é que duas sequências de Cauchy que convergem para o mesmo valor (mesmo que esse valor não exista em $\mathbb{Q}$) devem ser consideradas equivalentes. Isso acontece se, e somente se, a diferença entre elas convergir para zero.

4.4.1 Definição de I

Primeiro, definimos formalmente o que significa para uma sequência de racionais convergir para zero.

Definição 4.4.1 (Sequência Nula)**.** Dizemos que uma sequência de números racionais (q_n) **converge para zero** (ou é uma **sequência nula**) se, para todo número racional $\epsilon > 0$, existe um número natural N tal que para todo $n \geq N$, $|q_n| < \epsilon$. Escrevemos $\lim_{n\to\infty} q_n = 0$.

Definição 4.4.2 (O Ideal I)**.** Seja $\mathcal{C}(\mathbb{Q})$ o anel das sequências de Cauchy. O conjunto I é definido como o subconjunto de $\mathcal{C}(\mathbb{Q})$ que consiste em todas as sequências de Cauchy que convergem para zero.

$$I = \{(q_n) \in \mathcal{C}(\mathbb{Q}) \mid \lim_{n\to\infty} q_n = 0\}$$

4.4.2 I como um Ideal de $\mathcal{C}(\mathbb{Q})$

Proposição 4.4.1. O conjunto I é um ideal do anel $(\mathcal{C}(\mathbb{Q}), +, \cdot)$.

Demonstração. Para provar que I é um ideal de $\mathcal{C}(\mathbb{Q})$, devemos verificar que I é um subgrupo aditivo de $\mathcal{C}(\mathbb{Q})$ e que satisfaz a propriedade de absorção.

1. I é um Subgrupo Aditivo de $\mathcal{C}(\mathbb{Q})$: Usaremos o critério de subgrupo para grupos aditivos.

- *Não Vazio:* A sequência nula, $\mathbf{0} = (0, 0, \dots)$, converge para 0. Portanto, $\mathbf{0} \in I$ e $I \neq \emptyset$.
- *Fechamento sob Subtração:* Sejam (q_n) e (p_n) duas sequências em I. Devemos mostrar que $(q_n - p_n) \in I$.

  Dado $\epsilon > 0$: Como $(q_n) \in I$, $\exists N_1$ tal que $n \geq N_1 \implies |q_n| < \epsilon/2$. Como $(p_n) \in I$, $\exists N_2$ tal que $n \geq N_2 \implies |p_n| < \epsilon/2$.

  Seja $N = \max(N_1, N_2)$. Para $n \geq N$, pela Desigualdade Triangular:

$$|q_n - p_n| \leq |q_n| + |-p_n| = |q_n| + |p_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

  Logo, $\lim_{n\to\infty}(q_n - p_n) = 0$, e $(q_n - p_n) \in I$.

Portanto, $(I, +)$ é um subgrupo de $(\mathcal{C}(\mathbb{Q}), +)$.

2. Propriedade de Absorção: Devemos mostrar que para qualquer sequência $(c_n) \in \mathcal{C}(\mathbb{Q})$ (o anel) e qualquer sequência $(q_n) \in I$ (o ideal), o produto $(c_n \cdot q_n)$ também pertence a I.

Como (c_n) é uma sequência de Cauchy, ela é limitada. Portanto, existe um racional $M > 0$ tal que $|c_n| \leq M$ para todo $n \in \mathbb{N}$.

Queremos provar que $\lim_{n\to\infty}(c_n \cdot q_n) = 0$. Dado $\epsilon > 0$. Como $(q_n) \in I$, ela converge para 0. Assim, para o racional positivo $\frac{\epsilon}{M} > 0$, existe um N tal que para todo $n \geq N$, temos:

$$|q_n| < \frac{\epsilon}{M}$$

Agora, analisamos o produto para $n \geq N$:

$$|c_n \cdot q_n| = |c_n| \cdot |q_n| \leq M \cdot |q_n| < M \cdot \left(\frac{\epsilon}{M}\right) = \epsilon$$

Isso mostra que $\lim_{n\to\infty}(c_n \cdot q_n) = 0$, e portanto $(c_n \cdot q_n) \in I$.

Como I é um subgrupo aditivo e satisfaz a propriedade de absorção, I é um ideal de $\mathcal{C}(\mathbb{Q})$. □

4.5 Construção de $\mathbb{R}$ como Anel Quociente

Tendo definido o anel $\mathcal{C}(\mathbb{Q})$ e provado que I é um ideal, podemos agora definir formalmente o conjunto dos números reais, $\mathbb{R}$, como o anel quociente $\mathcal{C}(\mathbb{Q})/I$. Como já foi estabelecido na teoria dos anéis, as operações em um anel quociente são herdadas naturalmente do anel original e são bem-definidas precisamente porque estamos quocientando por um ideal.

4.5.1 Definição de $\mathbb{R}$

Definição 4.5.1 (O Anel dos Números Reais)**.** O conjunto dos números reais, denotado por $\mathbb{R}$, é definido como o anel quociente do anel das sequências de Cauchy $\mathcal{C}(\mathbb{Q})$ pelo seu ideal de sequências nulas I.

$$\mathbb{R} := \mathcal{C}(\mathbb{Q})/I$$

Cada elemento $x \in \mathbb{R}$ é uma classe de equivalência $[(q_n)]$ de uma sequência de Cauchy (q_n). A relação de equivalência é dada por:

$$[(q_n)] = [(p_n)] \iff (q_n) - (p_n) \in I \iff \lim_{n\to\infty}(q_n - p_n) = 0$$

As operações de anel em $\mathbb{R}$ são definidas pelas operações nas classes:

- **Adição em $\mathbb{R}$:** $[(q_n)] + [(p_n)] := [(q_n + p_n)]$
- **Multiplicação em $\mathbb{R}$:** $[(q_n)] \cdot [(p_n)] := [(q_n \cdot p_n)]$

Como $\mathcal{C}(\mathbb{Q})$ é um anel comutativo com unidade, a estrutura resultante $(\mathbb{R}, +, \cdot)$ é também um anel comutativo com unidade. Os elementos identidade são:

- Identidade Aditiva: $0_{\mathbb{R}} = \mathbf{0} + I = [(0, 0, 0, \dots)]$
- Identidade Multiplicativa: $1_{\mathbb{R}} = \mathbf{1} + I = [(1, 1, 1, \dots)]$

4.5.2 A Inserção de $\mathbb{Q}$ em $\mathbb{R}$

O corpo $\mathbb{Q}$ não é um subconjunto de $\mathbb{R}$ (pois um racional não é uma classe de sequências), mas $\mathbb{R}$ contém uma cópia exata de $\mathbb{Q}$. Provamos isso mostrando que existe um homomorfismo de anéis injetivo de $\mathbb{Q}$ em $\mathbb{R}$.

Proposição 4.5.1. A função $\phi : \mathbb{Q} \to \mathbb{R}$ que mapeia cada número racional q para a classe de equivalência de sua sequência constante,

$$\phi(q) := [(q, q, q, \dots)]$$

é um homomorfismo de anéis injetivo.

Demonstração. Primeiro, notamos que a sequência constante (q) é de Cauchy, logo $\phi(q) \in \mathbb{R}$ está bem-definida. Devemos verificar as propriedades de homomorfismo e a injetividade.

1. **Homomorfismo de Anéis:** Sejam $q_1, q_2 \in \mathbb{Q}$.

- *Adição:*

$$\begin{aligned} \phi(q_1 + q_2) &= [(q_1 + q_2, q_1 + q_2, \dots)] \\ &= [(q_1, q_1, \dots) + (q_2, q_2, \dots)] \\ &= [(q_1, q_1, \dots)] + [(q_2, q_2, \dots)] \\ &= \phi(q_1) + \phi(q_2) \end{aligned}$$

- *Multiplicação:*

$$\begin{aligned}\phi(q_1 \cdot q_2) &= [(q_1q_2, q_1q_2, \dots)] \\ &= [(q_1, q_1, \dots) \cdot (q_2, q_2, \dots)] \\ &= [(q_1, q_1, \dots)] \cdot [(q_2, q_2, \dots)] \\ &= \phi(q_1) \cdot \phi(q_2)\end{aligned}$$

- *Unidade:* $\phi(1_{\mathbb{Q}}) = \phi(1) = [(1, 1, \dots)] = 1_{\mathbb{R}}$.

Portanto, ϕ é um homomorfismo de anéis.

2. Injetividade:

Para provar a injetividade, mostramos que o núcleo do homomorfismo é trivial, $\ker(\phi) = \{0_{\mathbb{Q}}\}$. O núcleo é o conjunto de $q \in \mathbb{Q}$ tais que $\phi(q) = 0_{\mathbb{R}}$.

$$\phi(q) = 0_{\mathbb{R}} \implies [(q, q, q, \dots)] = [(0, 0, 0, \dots)]$$

Pela definição de equivalência, isso significa que a sequência $(q, q, \dots) - (0, 0, \dots) = (q, q, \dots)$ deve pertencer ao ideal I.

$$(q, q, q, \dots) \in I \implies \lim_{n\to\infty} q = 0$$

Uma sequência constante (q) só converge para 0 se $q = 0$. Portanto, $\ker(\phi) = \{0\}$, e o homomorfismo ϕ é injetivo. □

Este homomorfismo injetivo nos permite identificar o corpo $\mathbb{Q}$ com sua imagem $\phi(\mathbb{Q})$ dentro de $\mathbb{R}$. Assim, tratamos $\mathbb{Q}$ como um sub-corpo de $\mathbb{R}$, e o número racional q é o mesmo que o número real $[(q, q, \dots)]$.

4.6 Estrutura de Corpo em $\mathbb{R}$

Já estabelecemos que $(\mathbb{R}, +, \cdot)$ é um anel comutativo com unidade. Nesta seção, provamos que o anel comutativo $\mathbb{R}$ é, de fato, um corpo. Para isso, mostramos que todo elemento não-nulo possui um inverso multiplicativo.

4.6.1 A Tricotomia das Sequências de Cauchy

Antes de provar a existência de inversos, precisamos de uma propriedade fundamental que classifica todas as sequências de Cauchy. Mostramos que toda sequência $(q_n) \in \mathcal{C}(\mathbb{Q})$ satisfaz exatamente uma de três condições: (1) ela converge para 0 (pertence a I), (2)

ela é eventualmente positiva (se afasta de 0 positivamente), ou (3) ela é eventualmente negativa (se afasta de 0 negativamente).

Proposição 4.6.1 (Tricotomia das Sequências de Cauchy)**.** Seja $(s_n) \in \mathcal{C}(\mathbb{Q})$ uma sequência de Cauchy. Então, exatamente uma das três seguintes condições ocorre:

1. $(s_n) \in I$ (ou seja, $\lim_{n\to\infty} s_n = 0$).
2. **(Eventualmente Positiva)** Existe $\epsilon \in \mathbb{Q}, \epsilon > 0$, e $N \in \mathbb{N}$ tal que $s_n > \epsilon$ para todo $n \geq N$.
3. **(Eventualmente Negativa)** Existe $\epsilon \in \mathbb{Q}, \epsilon > 0$, e $N \in \mathbb{N}$ tal que $s_n < -\epsilon$ para todo $n \geq N$.

Demonstração. A prova é dividida em duas partes. Primeiro, provamos que se uma sequência (s_n) não converge para zero (não satisfaz a condição 1), ela deve estar eventualmente longe de zero (satisfazendo a condição 2 ou 3). Segundo, provamos que as condições 2 e 3 são mutuamente exclusivas e que, se uma sequência não converge para zero, ela deve satisfazer uma delas.

Parte 1: Se $(s_n) \notin I$, então (s_n) é eventualmente longe de zero.

Vamos provar a contrapositiva: Se (s_n) **não** está eventualmente longe de zero (ou seja, nega as condições 2 e 3), então ela **deve** convergir para zero (ou seja, $(s_n) \in I$).

Se (s_n) satisfaz a condição (2) ou (3), então existe $\epsilon > 0$ e N tal que $\forall n \geq N, |s_n| > \epsilon$. A negação disso é, portanto:

$$\forall \epsilon > 0, \forall N \in \mathbb{N}, \exists n \geq N \text{ tal que } |s_n| \leq \epsilon$$

Esta negação nos diz que, para qualquer $\epsilon > 0$, não importa o quão longe formos na sequência, sempre encontraremos um termo subsequente s_n que está próximo de zero (ou seja, $|s_n| \leq \epsilon$). Se isso vale para todo N, significa que a sequência deve ter **infinitos termos** arbitrariamente próximos de zero.

Agora, usamos esta suposição (que existem infinitos termos próximos de zero) junto com o fato de que (s_n) é uma sequência de Cauchy, para provar que (s_n) deve convergir para zero.

Pela propriedade de Cauchy: Como (s_n) é Cauchy, para o valor $\epsilon/2$, sabemos que existe um índice N_c tal que todos os termos após N_c estão próximos uns dos outros:

$$\forall n, m \geq N_c \implies |s_n - s_m| < \frac{\epsilon}{2}$$

Pela nossa suposição: Sabemos que existem infinitos termos s_k tais que $|s_k| < \epsilon/2$. Como existem infinitos termos s_k próximos de zero, podemos certamente encontrar um deles, que chamaremos de s_{k_0}, cujo índice k_0 seja maior que N_c. Assim, encontramos um índice $k_0 \geq N_c$ que satisfaz $|s_{k_0}| < \epsilon/2$.

Segue que para $n, k_0 \geq N_c$, temos:

$$|s_n - s_{k_0}| < \frac{\epsilon}{2}$$

Usando a Desigualdade Triangular:

$$|s_n| = |(s_n - s_{k_0}) + s_{k_0}| \leq |s_n - s_{k_0}| + |s_{k_0}|$$

Substituindo os valores que encontramos:

$$|s_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

Mostramos que para qualquer $\epsilon > 0$, existe um N tal que $\forall n \geq N, |s_n| < \epsilon$. Esta é a definição de $\lim_{n\to\infty} s_n = 0$, o que implica $(s_n) \in I$.

Provamos a contrapositiva. Portanto, se $(s_n) \notin I$, ela deve ser eventualmente longe de zero.

Parte 2: Exclusividade de (2) e (3).

Se $(s_n) \notin I$, então existe $\epsilon_0 > 0$ e N_0 tal que $n \geq N_0 \implies |s_n| > \epsilon_0$. Queremos ver que para $n \geq N_0$, ou $s_n > \epsilon_0$ (sempre positivo) ou $s_n < -\epsilon_0$ (sempre negativo).

As duas condições (2) e (3) não podem ocorrer simultaneamente, pois isso exigiria que a sequência fosse, eventualmente, positiva e negativa, o que é impossível.

Devemos mostrar que ela não pode transitar entre $s_n > \epsilon_0$ e $s_m < -\epsilon_0$ indefinidamente após N_0. Usamos o fato de que (s_n) é Cauchy. Para $\epsilon = \epsilon_0$, existe $N_c \geq N_0$ tal que $\forall n, m \geq N_c, |s_n - s_m| < \epsilon_0$.

Suponha que existam $n, m \geq N_c$ tais que $s_n > \epsilon_0$ e $s_m < -\epsilon_0$. A distância entre eles seria:

$$|s_n - s_m| = s_n - s_m > \epsilon_0 - (-\epsilon_0) = 2\epsilon_0$$

Isso contradiz o fato de que a distância deve ser $|s_n - s_m| < \epsilon_0$.

Portanto, após o índice N_c, todos os termos devem permanecer do mesmo lado: ou todos são maiores que ϵ_0 (satisfazendo a condição 2) ou todos são menores que $-\epsilon_0$ (satisfazendo a condição 3).

Como as condições (1), (2) e (3) são mutuamente exclusivas e cobrem todas as

possibilidades, exatamente uma delas deve ocorrer. □

4.6.2 Existência do Inverso Multiplicativo

Proposição 4.6.2. Todo elemento não-nulo $x \in \mathbb{R}$ possui um inverso multiplicativo $x^{-1} \in \mathbb{R}$.

Demonstração. Seja $x = [(s_n)]$ um elemento de $\mathbb{R}$ tal que $x \neq 0_{\mathbb{R}}$. Pela definição de $0_{\mathbb{R}}$, isso significa que a sequência (s_n) não converge para zero, ou seja, $(s_n) \notin I$.

Pela Proposição da Tricotomia, se $(s_n) \notin I$, ela deve estar eventualmente longe de zero. Ou seja, existe um $\epsilon \in \mathbb{Q}, \epsilon > 0$, e um $N_0 \in \mathbb{N}$ tal que:

$$\forall n \geq N_0, \quad |s_n| > \epsilon$$

Isso garante, em particular, que $s_n \neq 0$ para $n \geq N_0$.

Construção da Sequência Inversa: Vamos construir uma nova sequência (r_n) que atuará como representante do inverso. Como os termos iniciais de uma sequência (antes de N_0) não afetam sua classe de equivalência, podemos definir (r_n) da seguinte forma:

$$r_n = \begin{cases} 0 & \text{se } n < N_0 \\ 1/s_n & \text{se } n \geq N_0 \end{cases}$$

(r_n) **é uma Sequência de Cauchy:** Devemos mostrar que $(r_n) \in \mathcal{C}(\mathbb{Q})$. Para $n, m \geq N_0$:

$$|r_n - r_m| = \left| \frac{1}{s_n} - \frac{1}{s_m} \right| = \left| \frac{s_m - s_n}{s_n s_m} \right| = \frac{|s_m - s_n|}{|s_n||s_m|}$$

Como $n, m \geq N_0$, sabemos que $|s_n| > \epsilon$ e $|s_m| > \epsilon$. Portanto, $|s_n s_m| > \epsilon^2$. Isso nos fornece:

$$|r_n - r_m| < \frac{|s_m - s_n|}{\epsilon^2}$$

Dado $\delta > 0$, como (s_n) é Cauchy, existe $N_c \geq N_0$ tal que $\forall n, m \geq N_c$, $|s_m - s_n| < \epsilon^2 \delta$. Para $n, m \geq N_c$, temos:

$$|r_n - r_m| < \frac{\epsilon^2 \delta}{\epsilon^2} = \delta$$

Isso prova que (r_n) é uma sequência de Cauchy. Seja $x^{-1} = [(r_n)] \in \mathbb{R}$.

Verificação do Inverso: Devemos mostrar que $x \cdot x^{-1} = 1_{\mathbb{R}}$. Calculamos a classe do produto:

$$x \cdot x^{-1} = [(s_n)] \cdot [(r_n)] = [(s_n \cdot r_n)]$$

A sequência produto $(s_n \cdot r_n)$ é:

$$s_n \cdot r_n = \begin{cases} s_n \cdot 0 = 0 & \text{se } n < N_0 \\ s_n \cdot (1/s_n) = 1 & \text{se } n \geq N_0 \end{cases}$$

A sequência produto é $(0, 0, \ldots, 0, 1, 1, 1, \ldots)$, onde os 1s começam no índice N_0.

Para mostrar que esta classe é $1_{\mathbb{R}}$, devemos mostrar que ela é equivalente à sequência $\mathbf{1} = (1, 1, \ldots)$, ou seja, que a diferença entre elas pertence a I:

$$\lim_{n\to\infty} ((s_n r_n) - 1) = 0$$

Para $n \geq N_0$, a diferença é $|(s_n r_n) - 1| = |1 - 1| = 0$. Dado $\epsilon > 0$, escolhendo $N = N_0$, temos $|(s_n r_n) - 1| = 0 < \epsilon$ para todo $n \geq N$. A sequência diferença converge para 0.

Portanto, $x \cdot x^{-1} = [(s_n r_n)] = [(1)] = 1_{\mathbb{R}}$. □

Corolário 4.6.0.1. A estrutura $(\mathbb{R}, +, \cdot)$ é um **corpo**.

Demonstração. Já estabelecemos que $(\mathbb{R}, +, \cdot)$ é um anel comutativo com unidade $1_{\mathbb{R}} \neq 0_{\mathbb{R}}$. A proposição anterior demonstra que todo elemento $x \neq 0_{\mathbb{R}}$ possui um inverso multiplicativo. Portanto, $\mathbb{R}$ satisfaz todos os axiomas de um corpo. □

4.7 $\mathbb{R}$ como um Corpo Ordenado Completo

4.7.1 Definição da Ordem em $\mathbb{R}$

A Proposição da Tricotomia mostrou que toda sequência de Cauchy ou converge para zero, ou é eventualmente positiva, ou é eventualmente negativa . Usamos esta divisão para definir o que significa um número real ser positivo ou negativo.

Definição 4.7.1 (Números Reais Positivos e Não-Negativos)**.** Seja $x \in \mathbb{R}$, representado pela classe de equivalência $[(s_n)]$. Conforme estabelecido na Proposição da Tricotomia das Sequências de Cauchy, a sequência (s_n) deve satisfazer exatamente uma de três condições. Usamos essas condições para definir os sinais em $\mathbb{R}$:

- Dizemos que x é **positivo**, e escrevemos $x > 0_{\mathbb{R}}$, se (s_n) é **eventualmente positiva**.
- Dizemos que x é **negativo**, e escrevemos $x < 0_{\mathbb{R}}$, se (s_n) é **eventualmente negativa**.
- Dizemos que x é **não-negativo**, e escrevemos $x \geq 0_{\mathbb{R}}$, se x não é negativo (ou seja, se (s_n) converge para zero ou é eventualmente positiva).

A relação de ordem é, então, definida comparando dois elementos através da sua diferença.

Definição 4.7.2 (Ordem em $\mathbb{R}$)**.** Sejam $x, y \in \mathbb{R}$. Dizemos que x é **menor ou igual a** y, e escrevemos $x \leq y$, se e somente se a diferença $y - x$ for um número real não-negativo.

$$x \leq y \iff (y - x) \geq 0_{\mathbb{R}}$$

4.7.2 Propriedades da Ordem

Devemos primeiro provar que esta definição independe dos representantes de sequência que escolhemos.

Proposição 4.7.1. A relação de ordem $\leq$ em $\mathbb{R}$ é bem-definida.

Demonstração. Precisamos mostrar que a definição de $x \leq y$ (que é $y - x \geq 0_{\mathbb{R}}$) não depende dos representantes específicos escolhidos para x e y.

Sejam $x = [(q_n)] = [(q'_n)]$ e $y = [(p_n)] = [(p'_n)]$. Isto significa que as sequências são equivalentes:

1. $(q_n) \sim (q'_n) \implies (q_n - q'_n) \in I \implies \lim_{n\to\infty}(q_n - q'_n) = 0$
2. $(p_n) \sim (p'_n) \implies (p_n - p'_n) \in I \implies \lim_{n\to\infty}(p_n - p'_n) = 0$

Devemos provar a equivalência:

$$y - x \geq 0_{\mathbb{R}} \iff y' - x' \geq 0_{\mathbb{R}}$$

Devido à simetria, basta provar uma direção. Vamos provar que $y - x \geq 0_{\mathbb{R}} \implies y' - x' \geq 0_{\mathbb{R}}$.

Seja $S = (p_n - q_n)$ o representante de $y - x$. Seja $S' = (p'_n - q'_n)$ o representante de $y' - x'$.

A hipótese $y - x \geq 0_{\mathbb{R}}$ significa que o número real representado por S é não-negativo. Em termos de limites racionais, isso implica que $\lim_{n\to\infty} S_n = L \geq 0$. Pela definição de limite, para qualquer $\delta > 0$, existe um N_1 tal que para todo $n \geq N_1$, a distância $|S_n - L| < \delta$. Em particular, isso significa que $S_n > L - \delta$. Como $L \geq 0$, temos que $S_n > 0 - \delta = -\delta$. Escolhendo $\delta = \epsilon/2$, obtemos a condição formal utilizada:

$$\forall \epsilon > 0, \exists N_1 \in \mathbb{N} \text{ tal que } \forall n \geq N_1, S_n > -\epsilon/2$$

Agora, analisamos a relação entre S e S'. Considere a sequência $S - S'$:

$$S_n - S'_n = (p_n - q_n) - (p'_n - q'_n) = (p_n - p'_n) - (q_n - q'_n)$$

Como $(p_n - p'_n) \in I$ e $(q_n - q'_n) \in I$, e I é um ideal, a diferença $(S - S')$ também pertence a I. Logo, $S \sim S'$, o que significa $\lim_{n\to\infty}(S_n - S'_n) = 0$.

Pela definição de limite, para $\epsilon/2$, existe $N_2 \in \mathbb{N}$ tal que:

$$\forall n \geq N_2, \quad |S_n - S'_n| < \epsilon/2$$

Esta desigualdade implica, entre outras coisas, que $S_n - S'_n < \epsilon/2$, que podemos rearranjar para:

$$S'_n > S_n - \epsilon/2$$

Agora, queremos provar que $y' - x' \geq 0_{\mathbb{R}}$, ou seja, que $\forall \epsilon > 0, \exists N$ tal que $S'_n > -\epsilon$.

Seja $\epsilon > 0$ um racional arbitrário. Escolhemos N_1 e N_2 como acima. Seja $N = \max(N_1, N_2)$. Para todo $n \geq N$, ambas as condições são válidas. Podemos combiná-las:

1. $S'_n > S_n - \epsilon/2$ (pela equivalência $S \sim S'$)
2. $S_n > -\epsilon/2$ (pela hipótese $y - x \geq 0$)

Portanto, para $n \geq N$:

$$S'_n > \left(-\frac{\epsilon}{2}\right) - \frac{\epsilon}{2} = -\epsilon$$

Isso prova que $\forall \epsilon > 0, \exists N$ tal que $n \geq N \implies S'_n > -\epsilon$. Esta é a definição de $S' \geq 0_{\mathbb{R}}$, ou $y' - x' \geq 0_{\mathbb{R}}$.

Como $y - x \geq 0_{\mathbb{R}} \implies y' - x' \geq 0_{\mathbb{R}}$, a definição de ordem é bem-definida. □

Proposição 4.7.2. O corpo $(\mathbb{R}, +, \cdot)$ com a relação $\leq$ é um **Corpo Totalmente Ordenado**.

Demonstração. Devemos provar que $\leq$ é uma relação de ordem total e que é compatível com as operações de corpo.

1. Ordem Total: Para provar que $(\mathbb{R}, \leq)$ é um conjunto totalmente ordenado, devemos verificar que a relação $\leq$ é reflexiva, antissimétrica, transitiva e total.

- **Reflexividade:** Devemos provar que $x \leq x$ para todo $x \in \mathbb{R}$. Pela definição de ordem, isso é equivalente a provar que $x - x \geq 0_{\mathbb{R}}$. Como $x - x = 0_{\mathbb{R}}$ a relação é reflexiva.
- **Antissimetria:** Devemos provar que se $x \leq y$ e $y \leq x$, então $x = y$. As hipóteses são $y - x \geq 0_{\mathbb{R}}$ e $x - y \geq 0_{\mathbb{R}}$. Seja $z = y - x$. Então, $x - y = -z$. As hipóteses se tornam $z \geq 0_{\mathbb{R}}$ e $-z \geq 0_{\mathbb{R}}$. Seja $z = [(d_n)]$ um representante de z.
  - Se $z > 0_{\mathbb{R}}$, seu representante (d_n) é eventualmente positivo. Então $(-d_n)$ é eventualmente negativo, o que implica $-z < 0_{\mathbb{R}}$. Isso contradiz a hipótese $-z \geq 0_{\mathbb{R}}$.
  - Se $z < 0_{\mathbb{R}}$, seu representante (d_n) é eventualmente negativo. Isso contradiz a hipótese $z \geq 0_{\mathbb{R}}$.

A única possibilidade que não leva a uma contradição é $z = 0_{\mathbb{R}}$. Se $z = y - x = 0_{\mathbb{R}}$, então $y = x$. A relação é antissimétrica.

- **Transitividade:** Devemos provar que se $x \leq y$ e $y \leq z$, então $x \leq z$.

  As hipóteses, por definição de ordem, são:

  1. $a = y - x \geq 0_{\mathbb{R}}$
  2. $b = z - y \geq 0_{\mathbb{R}}$

  Queremos provar que $x \leq z$, o que é equivalente a provar que a diferença $z - x$ é não-negativa.

  Usando a associatividade da adição em $\mathbb{R}$, podemos escrever a diferença como a soma das nossas hipóteses:

  $$z - x = (z - y) + (y - x) = b + a$$

  O problema se reduz a provar que a soma de dois números reais não-negativos é, ela própria, não-negativa.

  Sejam $a = [(a_n)]$ e $b = [(b_n)]$ os representantes de a e b. A soma $a + b$ é representada pela sequência $(a_n + b_n)$. Devemos mostrar que $a + b \geq 0_{\mathbb{R}}$, ou seja, que a sequência $(a_n + b_n)$ satisfaz a definição de não-negatividade.

  Seja $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, um racional arbitrário. Pela definição de não-negatividade, para o racional $\epsilon/2 > 0$, as nossas hipóteses nos garantem que:

  1. Como $a \geq 0_{\mathbb{R}}$, existe $N_a \in \mathbb{N}$ tal que $\forall n \geq N_a \implies a_n > -\frac{\epsilon}{2}$.
  2. Como $b \geq 0_{\mathbb{R}}$, existe $N_b \in \mathbb{N}$ tal que $\forall n \geq N_b \implies b_n > -\frac{\epsilon}{2}$.

  Seja $N = \max(N_a, N_b)$. Para qualquer $n \geq N$, ambas as condições acima são válidas. Somando as duas inequações (o que é permitido em $\mathbb{Q}$):

  $$a_n + b_n > \left(-\frac{\epsilon}{2}\right) + \left(-\frac{\epsilon}{2}\right) = -\epsilon$$

  Mostramos que para qualquer $\epsilon > 0$, existe N tal que $\forall n \geq N, a_n + b_n > -\epsilon$. Esta é precisamente a definição de que a sequência $(a_n + b_n)$ representa um número real não-negativo.

  Portanto, $z - x = a + b \geq 0_{\mathbb{R}}$, o que prova $x \leq z$. A relação é transitiva.

- **Totalidade (Tricotomia):** Para quaisquer $x, y \in \mathbb{R}$, exatamente um de $x < y$, $x = y$, ou $y < x$ é verdadeiro. Consideremos o elemento $z = y - x$. Pela Proposição da Tricotomia das Sequências de Cauchy, o representante $(p_n - q_n)$ de z deve satisfazer exatamente uma das três condições:

- **Caso 1:** $(p_n - q_n) \in I$. Isso implica $z = y - x = 0_{\mathbb{R}}$, ou $x = y$.
- **Caso 2:** $(p_n - q_n)$ é eventualmente positiva. Isso implica $z = y - x > 0_{\mathbb{R}}$, ou $x < y$.
- **Caso 3:** $(p_n - q_n)$ é eventualmente negativa. Isso implica $z = y - x < 0_{\mathbb{R}}$, ou $y < x$.

Como exatamente uma dessas condições deve ocorrer para z, a ordem em $\mathbb{R}$ é total.

2. Compatibilidade com a Adição: Devemos mostrar que $x \leq y \implies x+z \leq y+z$. Assumimos $x \leq y$, o que significa $y - x \geq 0_{\mathbb{R}}$. Queremos provar $x + z \leq y + z$, o que é equivalente a provar $(y + z) - (x + z) \geq 0_{\mathbb{R}}$. Usando as propriedades do grupo aditivo $\mathbb{R}$:

$$(y + z) - (x + z) = y + z - x - z = (y - x) + (z - z) = y - x$$

Como $y - x \geq 0_{\mathbb{R}}$ por hipótese, a condição está satisfeita.

3. Compatibilidade com a Multiplicação: Devemos mostrar que $x \leq y$ e $z \geq 0_{\mathbb{R}} \implies xz \leq yz$. Assumimos $y - x \geq 0_{\mathbb{R}}$ e $z \geq 0_{\mathbb{R}}$. Queremos provar $yz - xz \geq 0_{\mathbb{R}}$. Pela distributividade em $\mathbb{R}$:

$$yz - xz = (y - x)z$$

Sejam $a = y - x$, temos $a \geq 0_{\mathbb{R}}$. Devemos mostrar que $a \cdot z \geq 0_{\mathbb{R}}$. Sejam $a = [(a_n)]$ e $z = [(z_n)]$.

- Se $a = 0_{\mathbb{R}}$ ou $z = 0_{\mathbb{R}}$, então $a \cdot z = 0_{\mathbb{R}}$, e $0_{\mathbb{R}} \geq 0_{\mathbb{R}}$ é verdadeiro.
- Se $a > 0_{\mathbb{R}}$ e $z > 0_{\mathbb{R}}$, então (a_n) e (z_n) são eventualmente positivas.
  Isto é, $\exists N_a, \epsilon_a > 0$ tal que $n \geq N_a \implies a_n > \epsilon_a$.
  E $\exists N_z, \epsilon_z > 0$ tal que $n \geq N_z \implies z_n > \epsilon_z$.
  Seja $N = \max(N_a, N_z)$. Para $n \geq N$, o produto $a_n z_n > \epsilon_a \epsilon_z$.
  Seja $\epsilon' = \epsilon_a \epsilon_z$. Como $\epsilon' \in \mathbb{Q}$ e $\epsilon' > 0$, a sequência produto $(a_n z_n)$ é eventualmente positiva. Portanto, $a \cdot z = [(a_n z_n)] > 0_{\mathbb{R}}$.

Em ambos os casos, o produto de dois reais não-negativos é não-negativo. Assim, $(y - x)z \geq 0_{\mathbb{R}}$, e a compatibilidade da multiplicação é satisfeita.

Como $\mathbb{R}$ é um corpo, com uma relação de ordem total compatível com ambas as operações, $\mathbb{R}$ é um corpo ordenado. □

4.7.3 Propriedade Arquimediana

Proposição 4.7.3 (Propriedade Arquimediana)**.** O corpo ordenado $(\mathbb{R}, +, \cdot, \leq)$ é Arquimediano.

Demonstração. Sejam $x, y \in \mathbb{R}$ com $x > 0_{\mathbb{R}}$. Devemos encontrar um $n \in \mathbb{N}$ (identificado com sua imagem $\phi(n) = [(n, n, \dots)] \in \mathbb{R}$) tal que $n \cdot x > y$.

Sejam $x = [(s_k)]$ e $y = [(r_k)]$ os números reais representados por suas respectivas sequências de Cauchy em $\mathcal{C}(\mathbb{Q})$.

Como $x > 0_{\mathbb{R}}$, x não é nulo. Pela Proposição da Tricotomia, a sequência (s_k) deve ser eventualmente positiva. Isto é, existem um racional $\epsilon_s > 0$ e um índice $N_s \in \mathbb{N}$ tais que:

$$\forall k \geq N_s, \quad s_k > \epsilon_s$$

Como (r_k) é uma sequência de Cauchy, ela é limitada. Portanto, existe um racional $M > 0$ tal que $|r_k| \leq M$ para todo $k \in \mathbb{N}$. Isso implica que $r_k \leq M$ para todo k.

Temos agora dois números racionais fixos: $\epsilon_s > 0$ e M. Como $\mathbb{Q}$ é Arquimediano, sabemos que existe um $n \in \mathbb{N}$ tal que:

$$n \cdot \epsilon_s > M + 1$$

Vamos provar que este inteiro n satisfaz $n \cdot x > y$.
Isso é equivalente a provar que $n \cdot x - y > 0_{\mathbb{R}}$. O número real $n \cdot x - y$ é representado pela sequência $D = (n \cdot s_k - r_k)_{k \in \mathbb{N}}$. Para mostrar que $n \cdot x - y > 0_{\mathbb{R}}$, devemos mostrar que a sequência D é eventualmente positiva.

Seja $N = N_s$. Para todo $k \geq N$, temos:

- $s_k > \epsilon_s \implies n \cdot s_k > n \cdot \epsilon_s$ (pois $n > 0$)
- $r_k \leq M$

Combinando estes fatos:

$$n \cdot s_k - r_k > (n \cdot \epsilon_s) - r_k \geq (n \cdot \epsilon_s) - M$$

Usando $n \cdot \epsilon_s > M + 1$, temos:

$$n \cdot s_k - r_k > (M + 1) - M = 1$$

Seja $\epsilon' = 1 \in \mathbb{Q}$. Como $\epsilon' > 0$, encontramos um $N \in \mathbb{N}$ (a saber, N_s) tal que $\forall k \geq N$, o termo $d_k = n \cdot s_k - r_k > \epsilon'$.

Esta é exatamente a definição de Sequência Eventualmente Positiva. Portanto, $n \cdot x - y > 0_{\mathbb{R}}$, o que implica $n \cdot x > y$.

□

4.7.4 Completude de $\mathbb{R}$

Proposição 4.7.4 ($\mathbb{Q}$ é Denso em $\mathbb{R}$)**.** O corpo dos racionais $\mathbb{Q}$ é denso em $\mathbb{R}$. Isto é, para quaisquer dois números reais $x, y \in \mathbb{R}$ com $x < y$, existe um número racional $q \in \mathbb{Q}$ tal que $x < q < y$.

Demonstração. Sejam $x, y \in \mathbb{R}$ com $x < y$. A diferença $y - x$ é um número real positivo, $y - x > 0$.

Como $\mathbb{R}$ é um corpo Arquimediano, dado $y - x > 0$, deve existir um $n \in \mathbb{N}^*$ (que identificamos com sua imagem $\phi(n)$ em $\mathbb{R}$) tal que:

$$n \cdot (y - x) > 1$$

Isso implica que $ny - nx > 1$, ou $ny > nx + 1$.

Agora, considere o elemento $nx \in \mathbb{R}$. Pela propriedade Arquimediana, deve existir um inteiro $m \in \mathbb{Z}$ tal que $m > nx$.

Pelo Princípio da Boa Ordem (aplicado ao conjunto de inteiros maiores que nx), podemos escolher m como sendo o *menor* inteiro que satisfaz $m > nx$. Se m é o menor inteiro, então o inteiro anterior, $m - 1$, não pode satisfazer a condição, ou seja:

$$m - 1 \leq nx$$

Agora temos duas desigualdades para m:

1. $nx < m$ (pela nossa escolha de m)
2. $m \leq nx + 1$ (adicionando 1 a $m - 1 \leq nx$)

Combinando estas inequações com a que obtivemos no início ($nx + 1 < ny$), criamos a seguinte cadeia:

$$nx < m \leq nx + 1 < ny$$

Isso nos mostra, em particular, que $nx < m < ny$.

Como $n \in \mathbb{N}$, seu inverso multiplicativo $\frac{1}{n}$ existe em $\mathbb{R}$ e é positivo. Podemos multiplicar a inequação $nx < m < ny$ por $\frac{1}{n}$ sem alterar a direção da ordem:

$$x < \frac{m}{n} < y$$

Seja $q = \frac{m}{n}$. Como $m \in \mathbb{Z}$ e $n \in \mathbb{N}^*$, o elemento q é, por definição, um número racional (identificado com sua classe $\phi(q) \in \mathbb{R}$).

Demonstramos assim a existência de um $q \in \mathbb{Q}$ estritamente entre x e y. □

Teorema 4.7.1 (Completude de $\mathbb{R}$)**.** O corpo ordenado $(\mathbb{R}, +, \cdot, \leq)$ é completo. Isto é, toda sequência de Cauchy de números reais converge para um limite em $\mathbb{R}$.

Demonstração. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência de Cauchy em $\mathbb{R}$. Queremos provar que existe um $L \in \mathbb{R}$ tal que $\lim_{n\to\infty} x_n = L$. A prova consiste em construir um candidato para L usando a densidade de $\mathbb{Q}$ e depois mostrar que (x_n) converge para ele.

Construção do candidato a limite L

Para cada $n \in \mathbb{N}$, definimos o valor positivo $\delta_n = \frac{1}{n+1} \in \mathbb{R}$. Conforme demonstrado anteriormente, o conjunto dos números racionais é denso nos reais. Isso significa que, para quaisquer dois números reais a e b tais que $a < b$, existe um racional q tal que $a < \phi(q) < b$.

Tomando $a = x_n - \delta_n$ e $b = x_n + \delta_n$, a propriedade de densidade garante a existência de um $q_n \in \mathbb{Q}$ tal que:

$$x_n - \frac{1}{n+1} < \phi(q_n) < x_n + \frac{1}{n+1}$$

onde $\phi(q_n)$ é o mergulho de q_n em $\mathbb{R}$, ou seja, a classe da sequência constante $(q_n, q_n, \dots)$.

Subtraindo x_n de todos os membros da desigualdade acima, obtemos a seguinte expressão equivalente:

$$-\frac{1}{n+1} < \phi(q_n) - x_n < \frac{1}{n+1}$$

Esta dupla desigualdade, implica diretamente que:

$$|\phi(q_n) - x_n| < \frac{1}{n+1}$$

Como a distância é simétrica, temos $|x_n - \phi(q_n)| < \frac{1}{n+1}$. Dessa forma, construímos uma sequência de racionais $(q_n)_{n\in\mathbb{N}}$ cujos valores estão arbitrariamente próximos dos termos da sequência de Cauchy original.

(q_n) é uma sequência de Cauchy em $\mathbb{Q}$

Vamos mostrar que esta nova sequência de racionais, $(q_n)_{n\in\mathbb{N}}$, é uma sequência de Cauchy em $\mathbb{Q}$. Para isso, analisamos a distância $|q_n - q_m|$ (em $\mathbb{Q}$), que é igual à distância $|\phi(q_n) - \phi(q_m)|$ (em $\mathbb{R}$). Usamos a Desigualdade Triangular em $\mathbb{R}$:

$$\begin{aligned} |\phi(q_n) - \phi(q_m)| &= |\phi(q_n) - x_n + x_n - x_m + x_m - \phi(q_m)| \\ &\leq |\phi(q_n) - x_n| + |x_n - x_m| + |x_m - \phi(q_m)| \end{aligned}$$

Substituindo as aproximações da Etapa 1:

$$|\phi(q_n) - \phi(q_m)| < \frac{1}{n+1} + |x_n - x_m| + \frac{1}{m+1}$$

Seja $\epsilon \in \mathbb{Q}, \epsilon > 0$.

- Como (x_n) é Cauchy (em $\mathbb{R}$), $\exists N_1$ tal que $n, m \geq N_1 \implies |x_n - x_m| < \epsilon/3$.
- $\exists N_2$ tal que $k \geq N_2 \implies \frac{1}{k+1} < \epsilon/3$.

Seja $N = \max(N_1, N_2)$. Para $n, m \geq N$, temos $\frac{1}{n+1} < \epsilon/3$ e $\frac{1}{m+1} < \epsilon/3$. Portanto:

$$|q_n - q_m| = |\phi(q_n) - \phi(q_m)| < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon$$

Logo, (q_n) é uma sequência de Cauchy de números racionais, $(q_n) \in \mathcal{C}(\mathbb{Q})$.

Definição do Limite L

Pela nossa definição de $\mathbb{R}$, esta sequência de Cauchy (q_n) define um número real. Definimos L como este número:

$$L := [(q_n)_{n\in\mathbb{N}}] \in \mathbb{R}$$

Prova da Convergência $x_n \to L$

Resta provar que a sequência original (x_n) converge para este L. Devemos mostrar que $\lim_{n\to\infty}(x_n - L) = 0_{\mathbb{R}}$. Usamos a Desigualdade Triangular novamente:

$$|x_n - L| = |(x_n - \phi(q_n)) + (\phi(q_n) - L)| \leq |x_n - \phi(q_n)| + |\phi(q_n) - L|$$

Analisamos os dois termos para n suficientemente grande:

- $|x_n - \phi(q_n)|$: Pela nossa construção, $|x_n - \phi(q_n)| < \frac{1}{n+1}$. A Propriedade Arquimediana garante que, para qualquer $\epsilon > 0$, podemos encontrar um inteiro N tal que $N \cdot x > y$. Aplicando a propriedade a $x = 1$ e $y = 1/\epsilon$, temos $N > 1/\epsilon$, o que implica que para todo $n \geq N$, $\frac{1}{n+1} < \epsilon$. Esta é a definição de que $\lim_{n\to\infty} \frac{1}{n+1} = 0$.
- $|\phi(q_n) - L|$: Este termo representa a distância em $\mathbb{R}$ entre o n-ésimo termo da sequência (q_k) (mergulhado como a classe constante $\phi(q_n)$) e o limite L da própria sequência (q_k). Portanto, $\lim_{n\to\infty}(\phi(q_n) - L) = 0_{\mathbb{R}}$.

Dado $\epsilon > 0$:

- $\exists N_1$ tal que $n \geq N_1 \implies |x_n - \phi(q_n)| < \epsilon/2$.
- $\exists N_2$ tal que $n \geq N_2 \implies |\phi(q_n) - L| < \epsilon/2$.

Seja $N_f = \max(N_1, N_2)$. Para $n \geq N_f$:

$$|x_n - L| \leq |x_n - \phi(q_n)| + |\phi(q_n) - L| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$$

Isso prova que $\lim_{n\to\infty} x_n = L$.

Portanto, toda sequência de Cauchy em $\mathbb{R}$ converge para um limite $L \in \mathbb{R}$. □

Esta propriedade de completude, que garante que $\mathbb{R}$ não possui buracos, é o que o distingue fundamentalmente de $\mathbb{Q}$. Juntamente com as propriedades de corpo ordenado e Arquimediano, a completude define $\mathbb{R}$ de forma única: qualquer corpo que satisfaça todas estas propriedades é, necessariamente, isomórfico a $\mathbb{R}$.

4.7.5 Unicidade do Corpo Ordenado Arquimediano Completo

Provamos que $\mathbb{R}$ é um corpo ordenado arquimediano completo. A notabilidade desta estrutura é que ela é a única que satisfaz estas propriedades. Qualquer outra estrutura que satisfaça estas condições será, necessariamente, idêntica a $\mathbb{R}$ em termos algébricos e de ordem.

Proposição 4.7.5. Todo corpo ordenado completo $(K, \oplus, \odot, \preceq)$ contém um subcorpo $\mathbb{Q}_K$ que é isomórfico ao corpo dos números racionais $(\mathbb{Q}, +, \cdot, \leq)$.

Demonstração. Seja $(K, \oplus, \odot, \preceq)$ um corpo ordenado completo.

Como K é um corpo, ele contém os elementos 0_K (identidade aditiva) e 1_K (identidade multiplicativa). Podemos definir uma função $f_{\mathbb{Z}} : \mathbb{Z} \to K$ que mapeia os inteiros para seus análogos em K, baseando-se na estrutura aditiva de K:

- $f_{\mathbb{Z}}(0) = 0_K$
- $f_{\mathbb{Z}}(n) = \underbrace{1_K \oplus \cdots \oplus 1_K}_{n \text{ vezes}}$, para $n > 0$.
- $f_{\mathbb{Z}}(n) = -f_{\mathbb{Z}}(-n)$, para $n < 0$.

Seja $\mathbb{Z}_K = \mathrm{Im}(f_{\mathbb{Z}}) = \{f_{\mathbb{Z}}(n) \mid n \in \mathbb{Z}\}$ a imagem desta função.

Vamos provar que $f_{\mathbb{Z}}$ é um **isomorfismo de anéis ordenados** entre $(\mathbb{Z}, +, \cdot, \leq)$ e $(\mathbb{Z}_K, \oplus, \odot, \preceq)$.

$f_{\mathbb{Z}}$ preserva a Adição:

A prova será feita por casos, com base nos sinais de n e m.

- **Caso 1: $n = 0$ ou $m = 0$.** Se $n = 0$, $f_{\mathbb{Z}}(0 + m) = f_{\mathbb{Z}}(m)$. O outro lado é $f_{\mathbb{Z}}(0) \oplus f_{\mathbb{Z}}(m) = 0_K \oplus f_{\mathbb{Z}}(m) = f_{\mathbb{Z}}(m)$. Para $m = 0$ o raciocínio é análogo.
- **Caso 2: $n > 0$ e $m > 0$.** Por definição, $f_{\mathbb{Z}}(n + m)$ é a soma de $n + m$ termos 1_K.

$$f_{\mathbb{Z}}(n + m) = \underbrace{1_K \oplus \cdots \oplus 1_K}_{n+m \text{ vezes}}$$

Pela associatividade da operação $\oplus$ em K, podemos separar a soma:

$$f_{\mathbb{Z}}(n+m) = \left(\underbrace{1_K \oplus \cdots \oplus 1_K}_{n \text{ vezes}}\right) \oplus \left(\underbrace{1_K \oplus \cdots \oplus 1_K}_{m \text{ vezes}}\right)$$

O que é, por definição, $f_{\mathbb{Z}}(n) \oplus f_{\mathbb{Z}}(m)$.

- **Caso 3:** $n < 0$ **e** $m < 0$**.** Sejam $n = -n'$ e $m = -m'$, onde $n', m' > 0$.

$$f_{\mathbb{Z}}(n+m) = f_{\mathbb{Z}}(-(n'+m')) = -f_{\mathbb{Z}}(n'+m')$$

Pelo Caso 1, $f_{\mathbb{Z}}(n'+m') = f_{\mathbb{Z}}(n') \oplus f_{\mathbb{Z}}(m')$. Substituindo, e usando que $-(a+b) = (-a)+(-b)$:

$$f_{\mathbb{Z}}(n+m) = -(f_{\mathbb{Z}}(n') \oplus f_{\mathbb{Z}}(m')) = (-f_{\mathbb{Z}}(n')) \oplus (-f_{\mathbb{Z}}(m'))$$

Por definição, $f_{\mathbb{Z}}(n) = -f_{\mathbb{Z}}(n')$ e $f_{\mathbb{Z}}(m) = -f_{\mathbb{Z}}(m')$. Logo, $f_{\mathbb{Z}}(n+m) = f_{\mathbb{Z}}(n) \oplus f_{\mathbb{Z}}(m)$.

- **Caso 4:** $n > 0$ **e** $m < 0$**.**

Se $n > 0$ e $m < 0$, seja $m = -m'$ (com $m' > 0$). Queremos provar $f_{\mathbb{Z}}(n-m') = f_{\mathbb{Z}}(n) \oplus f_{\mathbb{Z}}(-m')$.

  - Se $n > m'$, então $n - m' = k > 0$. Temos $n = m' + k$. Note que $f_{\mathbb{Z}}(n) = f_{\mathbb{Z}}(m'+k) = f_{\mathbb{Z}}(m') \oplus f_{\mathbb{Z}}(k)$ (pelo Caso 1). Portanto, $f_{\mathbb{Z}}(k) = f_{\mathbb{Z}}(n) - f_{\mathbb{Z}}(m')$ e $f_{\mathbb{Z}}(n-m') = f_{\mathbb{Z}}(n) \oplus (-f_{\mathbb{Z}}(m')) = f_{\mathbb{Z}}(n) \oplus f_{\mathbb{Z}}(-m')$.
  - Se $n < m'$, $n - m' = -k < 0$ (onde $k = m' - n > 0$). Note que $f_{\mathbb{Z}}(m') = f_{\mathbb{Z}}(n+k) = f_{\mathbb{Z}}(n) \oplus f_{\mathbb{Z}}(k)$ e $f_{\mathbb{Z}}(n) - f_{\mathbb{Z}}(m') = -f_{\mathbb{Z}}(k)$. Por outro lado, $f_{\mathbb{Z}}(n-m') = f_{\mathbb{Z}}(-k) = -f_{\mathbb{Z}}(k)$. A igualdade se verifica.
  - Se $n = m'$, $n - m' = 0$. Note que $f_{\mathbb{Z}}(n-m') = f_{\mathbb{Z}}(0) = 0_K$ e $f_{\mathbb{Z}}(n) \oplus f_{\mathbb{Z}}(-n) = 0_K$. A igualdade se verifica.

O raciocínio é análogo para $n < 0$ e $m > 0$

Em todos os casos, a adição é preservada.

$f_{\mathbb{Z}}$ **preserva a Multiplicação:**

- **Caso 1:** $n = 0$ **ou** $m = 0$**.** Note que $f_{\mathbb{Z}}(n \cdot 0) = f_{\mathbb{Z}}(0) = 0_K$ e $f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(0) = f_{\mathbb{Z}}(n) \odot 0_K = 0_K$. A igualdade é válida. Para $m = 0$ o raciocínio é análogo.

- **Caso 2:** $n > 0$ **e** $m > 0$**.**

$$f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(m) = \left(\underbrace{1_K \oplus \cdots \oplus 1_K}_{n \text{ vezes}}\right) \odot \left(\underbrace{1_K \oplus \cdots \oplus 1_K}_{m \text{ vezes}}\right)$$

Pela distributividade em K, aplicamos o primeiro termo n vezes ao segundo:

$$= \underbrace{\left(\left(\underbrace{1_K \oplus \cdots \oplus 1_K}_{m \text{ vezes}}\right) \oplus \cdots \oplus \left(\underbrace{1_K \oplus \cdots \oplus 1_K}_{m \text{ vezes}}\right)\right)}_{n \text{ vezes}}$$

Pela associatividade da adição $\oplus$, isso é uma soma de $n \cdot m$ termos 1_K.

$$= f_{\mathbb{Z}}(n \cdot m)$$

- **Caso 3:** $n < 0$ **e** $m < 0$**.** Sejam $n = -n'$ e $m = -m'$, com $n', m' > 0$. Note que $f_{\mathbb{Z}}(n \cdot m) = f_{\mathbb{Z}}((-n') \cdot (-m')) = f_{\mathbb{Z}}(n'm')$. Pelo Caso 1, $f_{\mathbb{Z}}(n'm') = f_{\mathbb{Z}}(n') \odot f_{\mathbb{Z}}(m')$.

  Por outro lado: $f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(m) = f_{\mathbb{Z}}(-n') \odot f_{\mathbb{Z}}(-m') = (-f_{\mathbb{Z}}(n')) \odot (-f_{\mathbb{Z}}(m'))$. Em qualquer anel, $(-a) \cdot (-b) = a \cdot b$, logo: $(-f_{\mathbb{Z}}(n')) \odot (-f_{\mathbb{Z}}(m')) = f_{\mathbb{Z}}(n') \odot f_{\mathbb{Z}}(m')$. As duas expressões são idênticas.

- **Caso 4:** $n > 0, m < 0$**).** Seja $m = -m'$, com $m' > 0$. Note que $f_{\mathbb{Z}}(n \cdot m) = f_{\mathbb{Z}}(n \cdot (-m')) = f_{\mathbb{Z}}(-nm') = -f_{\mathbb{Z}}(nm')$. Pelo Caso 1, $f_{\mathbb{Z}}(nm') = f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(m')$. Portanto, $f_{\mathbb{Z}}(n \cdot m) = -(f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(m'))$.

  Por outro lado: $f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(m) = f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(-m') = f_{\mathbb{Z}}(n) \odot (-f_{\mathbb{Z}}(m'))$. Em qualquer anel, $a \cdot (-b) = -(a \cdot b)$, logo: $f_{\mathbb{Z}}(n) \odot (-f_{\mathbb{Z}}(m')) = -(f_{\mathbb{Z}}(n) \odot f_{\mathbb{Z}}(m'))$. As duas expressões são idênticas.
  O raciocínio é análogo para $n < 0$ e $m > 0$

Em todos os casos, a multiplicação é preservada.

$f_{\mathbb{Z}}$ **é Injetiva:** Devemos provar que o núcleo do homomorfismo é trivial, ou seja, $\ker(f_{\mathbb{Z}}) = \{n \in \mathbb{Z} \mid f_{\mathbb{Z}}(n) = 0_K\} = \{0\}$. Como K é um corpo ordenado, $1_K \succ 0_K$. Pela compatibilidade da ordem com a adição (somando 1_K repetidamente):

$$f_{\mathbb{Z}}(1) = 1_K \succ 0_K$$

$$f_{\mathbb{Z}}(2) = 1_K \oplus 1_K \succ 1_K \succ 0_K$$

Por indução, para qualquer $n > 0$, temos $f_{\mathbb{Z}}(n) \succ 0_K$. Isso significa que nenhum inteiro

positivo está no núcleo. Se $n < 0$, então $-n > 0$, o que implica $f_{\mathbb{Z}}(-n) \succ 0_K$. O inverso aditivo, $f_{\mathbb{Z}}(n) = -f_{\mathbb{Z}}(-n)$, deve ser estritamente menor que 0_K ($f_{\mathbb{Z}}(n) \prec 0_K$). Isso significa que nenhum inteiro negativo está no núcleo. O único elemento restante é $n = 0$, para o qual $f_{\mathbb{Z}}(0) = 0_K$. Portanto, $\ker(f_{\mathbb{Z}}) = \{0\}$, e a função $f_{\mathbb{Z}}$ é injetiva.

$f_{\mathbb{Z}}$ **Preserva a Ordem:** Devemos mostrar que $n \leq m \implies f_{\mathbb{Z}}(n) \preceq f_{\mathbb{Z}}(m)$. Esta implicação é equivalente a mostrar que $m - n \geq 0 \implies f_{\mathbb{Z}}(m - n) \succeq 0_K$.

Seja $k = m - n$. A hipótese é $k \geq 0$.

- Se $k = 0$, $f_{\mathbb{Z}}(k) = f_{\mathbb{Z}}(0) = 0_K$. A condição $0_K \succeq 0_K$ é válida.
- Se $k > 0$, como provado na injetividade, $f_{\mathbb{Z}}(k) \succ 0_K$. A condição $f_{\mathbb{Z}}(k) \succeq 0_K$ é válida.

Como $f_{\mathbb{Z}}$ é um homomorfismo, $f_{\mathbb{Z}}(m - n) = f_{\mathbb{Z}}(m) \oplus f_{\mathbb{Z}}(-n) = f_{\mathbb{Z}}(m) \oplus (-f_{\mathbb{Z}}(n)) = f_{\mathbb{Z}}(m) \ominus f_{\mathbb{Z}}(n)$. Portanto, $f_{\mathbb{Z}}(m) \ominus f_{\mathbb{Z}}(n) \succeq 0_K$, o que implica $f_{\mathbb{Z}}(m) \succeq f_{\mathbb{Z}}(n)$.

Como $f_{\mathbb{Z}}$ é um homomorfismo injetivo que preserva a ordem, ele é um isomorfismo de anéis ordenados entre $\mathbb{Z}$ e sua imagem $\mathbb{Z}_K$. Isso nos permite identificar $\mathbb{Z}$ com $\mathbb{Z}_K$ sem ambiguidade.

Agora, definimos o subcorpo $\mathbb{Q}_K \subset K$ como o corpo de frações de $\mathbb{Z}_K$:

$$\mathbb{Q}_K = \{a_K \odot (b_K)^{-1} \mid a_K, b_K \in \mathbb{Z}_K, b_K \neq 0_K\}$$

Agora, construímos a função $f : \mathbb{Q} \to \mathbb{Q}_K$ que estende $f_{\mathbb{Z}}$: Para qualquer $q = \frac{a}{b} \in \mathbb{Q}$ (onde $a, b \in \mathbb{Z}, b \neq 0$):

$$f\left(\frac{a}{b}\right) := f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1}$$

Devemos provar que f é um isomorfismo de corpos ordenados.

f **é bem-definida:** Devemos mostrar que se $\frac{a}{b} = \frac{c}{d}$ em $\mathbb{Q}$, então $f(\frac{a}{b}) = f(\frac{c}{d})$ em K. A hipótese $\frac{a}{b} = \frac{c}{d}$ implica $a \cdot d = b \cdot c$ em $\mathbb{Z}$. Aplicamos o isomorfismo $f_{\mathbb{Z}}$ a ambos os lados:

$$f_{\mathbb{Z}}(a \cdot d) = f_{\mathbb{Z}}(b \cdot c)$$

$$f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d) = f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(c)$$

Como $b, d \neq 0$, seus isomorfos $f_{\mathbb{Z}}(b)$ e $f_{\mathbb{Z}}(d)$ são não-nulos em K e, portanto, possuem inversos multiplicativos $(f_{\mathbb{Z}}(b))^{-1}$ e $(f_{\mathbb{Z}}(d))^{-1}$. Multiplicamos ambos os lados da equação por estes inversos:

$$(f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d)) \odot (f_{\mathbb{Z}}(d))^{-1} \odot (f_{\mathbb{Z}}(b))^{-1} = (f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(c)) \odot (f_{\mathbb{Z}}(d))^{-1} \odot (f_{\mathbb{Z}}(b))^{-1}$$

Usando a associatividade e comutatividade de $\odot$ em K:

$$(f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1}) \odot (f_{\mathbb{Z}}(d) \odot (f_{\mathbb{Z}}(d))^{-1}) = (f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}) \odot (f_{\mathbb{Z}}(b) \odot (f_{\mathbb{Z}}(b))^{-1})$$

$$(f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1}) \odot 1_K = (f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}) \odot 1_K$$

$$f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} = f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}$$

Pela definição de f, isso é $f(\frac{a}{b}) = f(\frac{c}{d})$. A função f é bem-definida.

f **preserva a adição:** Devemos provar que $f(\frac{a}{b} + \frac{c}{d}) = f(\frac{a}{b}) \oplus f(\frac{c}{d})$.

$$\begin{aligned} f\left(\frac{a}{b} + \frac{c}{d}\right) &= f\left(\frac{ad+bc}{bd}\right) \\ &= f_{\mathbb{Z}}(ad+bc) \odot (f_{\mathbb{Z}}(bd))^{-1} \\ &= (f_{\mathbb{Z}}(ad) \oplus f_{\mathbb{Z}}(bc)) \odot (f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(d))^{-1} \\ &= (f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d) \oplus f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(c)) \odot (f_{\mathbb{Z}}(b))^{-1} \odot (f_{\mathbb{Z}}(d))^{-1} \end{aligned}$$

Agora, calculamos o outro lado, $f(\frac{a}{b}) \oplus f(\frac{c}{d})$:

$$\begin{aligned} f\left(\frac{a}{b}\right) \oplus f\left(\frac{c}{d}\right) &= [f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1}] \oplus [f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}] \\ &= [f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} \odot (f_{\mathbb{Z}}(d) \odot (f_{\mathbb{Z}}(d))^{-1})] \oplus \\ &\quad [f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1} \odot (f_{\mathbb{Z}}(b) \odot (f_{\mathbb{Z}}(b))^{-1})] \\ &= [f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d) \odot (f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(d))^{-1}] \oplus \\ &\quad [f_{\mathbb{Z}}(c) \odot f_{\mathbb{Z}}(b) \odot (f_{\mathbb{Z}}(d) \odot f_{\mathbb{Z}}(b))^{-1}] \\ &= [(f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d)) \oplus (f_{\mathbb{Z}}(c) \odot f_{\mathbb{Z}}(b))] \odot (f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(d))^{-1} \end{aligned}$$

Usando a comutatividade de $\oplus$ e $\odot$ em K, as duas expressões são idênticas.

f **preserva a multiplicação:** Devemos provar que $f(\frac{a}{b} \cdot \frac{c}{d}) = f(\frac{a}{b}) \odot f(\frac{c}{d})$.

$$\begin{aligned} f\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= f\left(\frac{ac}{bd}\right) \\ &= f_{\mathbb{Z}}(ac) \odot (f_{\mathbb{Z}}(bd))^{-1} \\ &= (f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(c)) \odot (f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(d))^{-1} \\ &= (f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(c)) \odot (f_{\mathbb{Z}}(b))^{-1} \odot (f_{\mathbb{Z}}(d))^{-1} \end{aligned}$$

Calculando o outro lado:

$$\begin{aligned} f\left(\frac{a}{b}\right) \odot f\left(\frac{c}{d}\right) &= [f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1}] \odot [f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}] \\ &= (f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(c)) \odot (f_{\mathbb{Z}}(b))^{-1} \odot (f_{\mathbb{Z}}(d))^{-1} \end{aligned}$$

As duas expressões são idênticas.

A preservação da unidade é direta: $f(1/1) = f_{\mathbb{Z}}(1) \odot (f_{\mathbb{Z}}(1))^{-1} = 1_K$.

f é injetiva: Provamos que o núcleo é trivial: $\ker(f) = \{q \in \mathbb{Q} \mid f(q) = 0_K\}$.

$$f\left(\frac{a}{b}\right) = 0_K \implies f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} = 0_K$$

Como $b \neq 0$, $f_{\mathbb{Z}}(b) \neq 0_K$, e seu inverso $(f_{\mathbb{Z}}(b))^{-1}$ também é não-nulo. Como K é um corpo (e, portanto, um domínio de integridade), o produto de dois elementos não nulos não pode ser 0_K. A única possibilidade para $f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} = 0_K$ é que $f_{\mathbb{Z}}(a) = 0_K$. Como $f_{\mathbb{Z}}$ é um isomorfismo, $f_{\mathbb{Z}}(a) = 0_K \implies a = 0$. Se $a = 0$, então $q = \frac{0}{b} = 0_{\mathbb{Q}}$. Logo, $\ker(f) = \{0_{\mathbb{Q}}\}$, e f é injetiva.

f é sobrejetiva (em $\mathbb{Q}_K$): Seja y um elemento arbitrário de $\mathbb{Q}_K$. Por definição de $\mathbb{Q}_K$, $y = a_K \odot (b_K)^{-1}$ para alguns $a_K, b_K \in \mathbb{Z}_K$ ($b_K \neq 0_K$). Como $f_{\mathbb{Z}}$ é um isomorfismo, ele é bijetivo. Portanto, existem únicos $a, b \in \mathbb{Z}$ ($b \neq 0$) tais que $f_{\mathbb{Z}}(a) = a_K$ e $f_{\mathbb{Z}}(b) = b_K$. Considere o elemento $x = \frac{a}{b} \in \mathbb{Q}$.

$$f(x) = f\left(\frac{a}{b}\right) = f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} = a_K \odot (b_K)^{-1} = y$$

Como todo $y \in \mathbb{Q}_K$ é imagem de algum $x \in \mathbb{Q}$, f é sobrejetiva.

f preserva a ordem: Devemos mostrar que $q_1 \leq q_2 \implies f(q_1) \preceq f(q_2)$. Sejam $q_1 = \frac{a}{b}, q_2 = \frac{c}{d} \in \mathbb{Q}$, sabemos que $b > 0$ e $d > 0$. A hipótese $q_1 \leq q_2$ implica $a \cdot d \leq b \cdot c$ em $\mathbb{Z}$. Como $f_{\mathbb{Z}}$ é um isomorfismo de anéis ordenados, ele preserva a ordem:

$$f_{\mathbb{Z}}(ad) \preceq f_{\mathbb{Z}}(bc) \implies f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d) \preceq f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(c)$$

Queremos provar que $f(\frac{a}{b}) \preceq f(\frac{c}{d})$, ou seja:

$$f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} \preceq f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}$$

Como $b > 0$ e $d > 0$, seus isomorfos $f_{\mathbb{Z}}(b) \succ 0_K$ e $f_{\mathbb{Z}}(d) \succ 0_K$. Em um corpo ordenado, o inverso de um elemento positivo é positivo, então $(f_{\mathbb{Z}}(b))^{-1} \succ 0_K$ e $(f_{\mathbb{Z}}(d))^{-1} \succ 0_K$. Partindo da inequação $f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d) \preceq f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(c)$, multiplicamos ambos os lados pelos

inversos:

$$(f_{\mathbb{Z}}(a) \odot f_{\mathbb{Z}}(d)) \odot (f_{\mathbb{Z}}(d))^{-1} \odot (f_{\mathbb{Z}}(b))^{-1} \preceq (f_{\mathbb{Z}}(b) \odot f_{\mathbb{Z}}(c)) \odot (f_{\mathbb{Z}}(d))^{-1} \odot (f_{\mathbb{Z}}(b))^{-1}$$

Simplificando com associatividade e comutatividade:

$$f_{\mathbb{Z}}(a) \odot (f_{\mathbb{Z}}(b))^{-1} \preceq f_{\mathbb{Z}}(c) \odot (f_{\mathbb{Z}}(d))^{-1}$$

Equivalentemente,

$$f\left(\frac{a}{b}\right) \preceq f\left(\frac{c}{d}\right)$$

A ordem é preservada.

Conclusão: Como f é um homomorfismo bijetivo que preserva a ordem, é um isomorfismo de corpos ordenados entre $\mathbb{Q}$ e $\mathbb{Q}_K$. □

Teorema 4.7.2 (Unicidade de $\mathbb{R}$)**.** Qualquer corpo ordenado arquimediano completo $(K, \oplus, \odot, \preceq)$ é isomórfico ao corpo dos números reais $(\mathbb{R}, +, \cdot, \leq)$.

Demonstração. Seja $(K, \oplus, \odot, \preceq)$ um corpo ordenado completo.

O Subcorpo Racional de K

Como foi demonstrado na proposição anterior, todo corpo ordenado completo K contém um subcorpo, que denotamos $\mathbb{Q}_K$, que é isomórfico ao corpo dos números racionais $(\mathbb{Q}, +, \cdot, \leq)$.

Seja $f : \mathbb{Q} \to \mathbb{Q}_K$ este isomorfismo de corpos ordenados.

Construção do Isomorfismo $\Psi : \mathbb{R} \to K$

Devemos construir uma função que mapeie o corpo dos reais $\mathbb{R}$ para o corpo K.

Seja $x \in \mathbb{R}$. Pela nossa construção dos números reais, x é uma classe de equivalência de sequências de Cauchy de números racionais. Seja (q_n) uma sequência de Cauchy em $\mathbb{Q}$ tal que $x = [(q_n)]$.

Aplicamos o isomorfismo f a cada termo da sequência (q_n) para criar uma nova sequência $(f(q_n))$ em $\mathbb{Q}_K$. Como f é um isomorfismo de corpos ordenados, ele preserva a distância. Assim, como (q_n) é uma sequência de Cauchy em $\mathbb{Q}$, a sequência imagem $(f(q_n))$ é uma sequência de Cauchy em $\mathbb{Q}_K$ (e, portanto, em K).

Por hipótese, K é um corpo ordenado **completo**. A propriedade de completude garante que a sequência $(f(q_n))$ converge para um limite único em K.

Definimos a função $\Psi : \mathbb{R} \to K$ da seguinte forma:

$$\Psi(x) = \Psi([(q_n)]) := \lim_{n\to\infty} (f(q_n))$$

Ψ é bem-definida

Devemos mostrar que o limite $k \in K$ não depende da sequência de Cauchy (q_n) escolhida para representar x. Suponha que $x = [(q_n)] = [(p_n)]$. Por definição de equivalência em $\mathbb{R}$, isso significa que $(q_n) \sim (p_n)$, ou seja, $\lim_{n\to\infty}(q_n - p_n) = 0$.

Queremos mostrar que $\Psi([(q_n)]) = \Psi([(p_n)])$, o que é o mesmo que $\lim(f(q_n)) = \lim(f(p_n))$. Isso é equivalente a provar que a diferença dos limites é 0_K:

$$\lim_{n\to\infty}(f(q_n)) \ominus \lim_{n\to\infty}(f(p_n)) = \lim_{n\to\infty}(f(q_n) \ominus f(p_n))$$

Como f é um homomorfismo de grupos aditivos:

$$= \lim_{n\to\infty}(f(q_n - p_n))$$

Como f é um isomorfismo de corpos ordenados, ele preserva a ordem e a métrica. Uma sequência (d_n) converge para 0 em $\mathbb{Q}$ se, e somente se, a sequência $(f(d_n))$ converge para 0_K em K. Dado que $\lim_{n\to\infty}(q_n - p_n) = 0$, segue que $\lim_{n\to\infty} f(q_n - p_n) = f(0) = 0_K$. Portanto, $\lim(f(q_n)) = \lim(f(p_n))$, e a função Ψ está bem-definida.

Ψ é um Homomorfismo de Corpos

Sejam $x = [(q_n)]$ e $y = [(p_n)]$ dois números reais.

- **Adição:**

$$\begin{aligned}
\Psi(x+y) &= \Psi([(q_n + p_n)]) && \text{(Def. de } + \text{ em } \mathbb{R}) \\
&= \lim_{n\to\infty}(f(q_n + p_n)) && \text{(Def. de } \Psi) \\
&= \lim_{n\to\infty}(f(q_n) \oplus f(p_n)) && \text{(f preserva } \oplus) \\
&= \lim_{n\to\infty}(f(q_n)) \oplus \lim_{n\to\infty}(f(p_n)) && \text{(Limite da soma em } K) \\
&= \Psi(x) \oplus \Psi(y)
\end{aligned}$$

- **Multiplicação:**

$$\begin{aligned}
\Psi(x\cdot y) &= \Psi([(q_n \cdot p_n)]) && \text{(Def. de } \cdot \text{ em } \mathbb{R}) \\
&= \lim_{n\to\infty}(f(q_n \cdot p_n)) && \text{(Def. de } \Psi) \\
&= \lim_{n\to\infty}(f(q_n) \odot f(p_n)) && \text{(f preserva } \odot) \\
&= \lim_{n\to\infty}(f(q_n)) \odot \lim_{n\to\infty}(f(p_n)) && \text{(Limite do produto em } K) \\
&= \Psi(x) \odot \Psi(y)
\end{aligned}$$

(A preservação da unidade, $\Psi(1_{\mathbb{R}}) = \Psi([(1,1,\dots)]) = \lim(f(1,1,\dots)) =$

$\lim(1_K, 1_K, \dots) = 1_K$, segue da mesma forma). Portanto, Ψ é um homomorfismo de corpos.

Ψ é Injetiva

Provamos que o núcleo de Ψ é trivial, $\ker(\Psi) = \{0_\mathbb{R}\}$. Seja $x \in \ker(\Psi)$, o que significa $\Psi(x) = 0_K$. Se $x = [(q_n)]$, então $\Psi(x) = \lim_{n\to\infty}(f(q_n)) = 0_K$. Como f é um isomorfismo, a sequência $(f(q_n))$ em $\mathbb{Q}_K$ converge para 0_K se, e somente se, a sequência (q_n) em $\mathbb{Q}$ converge para $0_\mathbb{Q}$. A condição $\lim_{n\to\infty}(q_n) = 0$ é a definição de que $(q_n) \sim (0, 0, \dots)$. Portanto, $x = [(q_n)] = [(0, 0, \dots)] = 0_\mathbb{R}$. Como $\ker(\Psi) = \{0_\mathbb{R}\}$, Ψ é injetiva.

Ψ é Sobrejetiva

Seja k um elemento arbitrário de K. Como K é um corpo ordenado completo, o subcorpo $\mathbb{Q}_K$ é denso em K. Isso significa que k é o limite de alguma sequência de Cauchy (k_n) onde $k_n \in \mathbb{Q}_K$.

Como $f : \mathbb{Q} \to \mathbb{Q}_K$ é um isomorfismo, podemos construir a sequência (q_n) em $\mathbb{Q}$ tal que $q_n = f^{-1}(k_n)$. Como f^{-1} também preserva a métrica, a sequência (q_n) é de Cauchy em $\mathbb{Q}$. Portanto, $x = [(q_n)]$ é um número real bem-definido.

Agora, aplicamos Ψ a este x:

$$\Psi(x) = \Psi([(q_n)]) = \lim_{n\to\infty}(f(q_n)) = \lim_{n\to\infty}(f(f^{-1}(k_n))) = \lim_{n\to\infty}(k_n) = k$$

Como para todo $k \in K$ encontramos um $x \in \mathbb{R}$ tal que $\Psi(x) = k$, a função Ψ é sobrejetiva.

Ψ Preserva a Ordem

Devemos mostrar que $x \leq y \implies \Psi(x) \preceq \Psi(y)$. Isso é equivalente a provar que $z \geq 0_\mathbb{R} \implies \Psi(z) \succeq 0_K$. Seja $z = [(q_n)] \geq 0_\mathbb{R}$. Conforme definido anteriormente, isso significa que $\forall \epsilon > 0, \exists N, \forall n \geq N, q_n > -\epsilon$. Seja $(k_n) = (f(q_n))$ a sequência correspondente em K. Como f preserva a ordem, $\forall \epsilon_K \succ 0_K$ (onde $\epsilon_K = f(\epsilon)$), $\exists N$ tal que $n \geq N \implies k_n \succ -\epsilon_K$. Isso significa que o limite $k = \lim_{n\to\infty}(k_n) = \Psi(z)$ não pode ser estritamente negativo (pois, se fosse, estaria abaixo de $-\epsilon_K$ para algum ϵ_K, o que contradiria a condição dos termos k_n). Portanto, $\Psi(z) \succeq 0_K$. A ordem é preservada.

Conclusão: A função Ψ é um homomorfismo bijetivo que preserva a ordem. Portanto, Ψ é um isomorfismo de corpos ordenados. Isso prova que qualquer corpo ordenado arquimediano completo K é isomórfico a $\mathbb{R}$. □

A exigência de que o corpo K seja arquimediano é fundamental para garantir a densidade do subcorpo racional $\mathbb{Q}_K$ em K. A propriedade arquimediana assegura que não existem elementos em K que sejam infinitamente grandes ou infinitamente pequenos (infinitésimos) em relação à unidade. Sem essa propriedade, os números

racionais não estariam espalhados por todo o corpo K, e existiriam elementos em K que não poderiam ser aproximados arbitrariamente por sequências de racionais. Consequentemente, a função Ψ construída na demonstração não seria sobrejetiva, pois esses elementos não-arquimedianos não seriam limites de sequências de Cauchy de $\mathbb{Q}_K$.

Capítulo 5

Complexos

No capítulo anterior, estabelecemos que o corpo dos números reais $(\mathbb{R}, +, \cdot, \leq)$ é um corpo ordenado arquimediano completo, resolvendo a deficiência de incompletude de $\mathbb{Q}$. No entanto, a estrutura de $\mathbb{R}$ ainda é algebricamente incompleta. A motivação para a construção dos números complexos surge da incapacidade de $\mathbb{R}$ em fornecer soluções para equações polinomiais simples. Um exemplo fundamental é a equação:

$$x^2 + 1 = 0 \quad \text{ou} \quad x^2 = -1$$

Como o quadrado de qualquer número real não-nulo é positivo, não existe $x \in \mathbb{R}$ que satisfaça esta equação. Nosso objetivo é, portanto, construir um novo corpo, $\mathbb{C}$, que contenha $\mathbb{R}$ e que forneça uma solução para esta equação.

5.1 Construção de $\mathbb{C}$ como $\mathbb{R} \times \mathbb{R}$

Em analogia às construções anteriores, definimos o novo conjunto a partir de pares ordenados do conjunto anterior.

Definição 5.1.1 (O Conjunto dos Números Complexos)**.** O conjunto dos números complexos, denotado por $\mathbb{C}$, é o conjunto de todos os pares ordenados de números reais:

$$\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a \in \mathbb{R}, b \in \mathbb{R}\}$$

Dois números complexos (a, b) e (c, d) são ditos **iguais** se, e somente se, suas componentes são iguais:

$$(a, b) = (c, d) \iff a = c \wedge b = d$$

5.1.1 Operações em $\mathbb{C}$

Definimos duas operações binárias sobre o conjunto $\mathbb{C}$.

Definição 5.1.2 (Adição de Complexos)**.** Sejam $z_1 = (a, b)$ e $z_2 = (c, d)$ dois números complexos. A **soma** $z_1 + z_2$ é definida como a adição componente a componente:

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

Definição 5.1.3 (Multiplicação de Complexos)**.** Sejam $z_1 = (a, b)$ e $z_2 = (c, d)$ dois números complexos. O **produto** $z_1 \cdot z_2$ é definido por:

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

5.2 A Estrutura de Corpo em $\mathbb{C}$

Verificamos que $(\mathbb{C}, +, \cdot)$ satisfaz os axiomas de um corpo.

5.2.1 O Grupo Aditivo $(\mathbb{C}, +)$

Proposição 5.2.1. A estrutura $(\mathbb{C}, +)$ é um **grupo abeliano**.

Demonstração. A prova baseia-se nas propriedades do grupo abeliano $(\mathbb{R}, +)$. Sejam $z_1 = (a, b)$, $z_2 = (c, d)$ e $z_3 = (e, f)$ em $\mathbb{C}$.

1. **Associatividade:**

$$\begin{aligned}(z_1 + z_2) + z_3 &= ((a + c), (b + d)) + (e, f) = ((a + c) + e, (b + d) + f) \\ &= (a + (c + e), b + (d + f)) = (a, b) + ((c + e), (d + f)) \\ &= z_1 + (z_2 + z_3)\end{aligned}$$

2. **Comutatividade:**

$$z_1 + z_2 = (a + c, b + d) = (c + a, d + b) = z_2 + z_1$$

3. **Elemento Identidade:** O par $(0, 0) \in \mathbb{C}$ é a identidade aditiva (denotada $0_{\mathbb{C}}$), pois:
$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$$

4. **Elemento Inverso:** Para todo $(a, b) \in \mathbb{C}$, existe um inverso $(-a, -b) \in \mathbb{C}$, pois:

$$(a, b) + (-a, -b) = (a - a, b - b) = (0, 0) = 0_{\mathbb{C}}$$

□

5.2.2 O Grupo Multiplicativo $(\mathbb{C}^*, \cdot)$

Seja $\mathbb{C}^* = \mathbb{C} \setminus \{(0,0)\}$.

Proposição 5.2.2. A estrutura $(\mathbb{C}^*, \cdot)$ é um **grupo abeliano**.

Demonstração. Sejam $z_1 = (a,b)$, $z_2 = (c,d)$ e $z_3 = (e,f)$ em $\mathbb{C}^*$.

1. **Associatividade:**

$$\begin{aligned}(z_1 \cdot z_2) \cdot z_3 &= (ac - bd, ad + bc) \cdot (e,f) \\ &= ((ac-bd)e - (ad+bc)f, (ac-bd)f + (ad+bc)e) \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce)\end{aligned}$$

$$\begin{aligned}z_1 \cdot (z_2 \cdot z_3) &= (a,b) \cdot (ce - df, cf + de) \\ &= (a(ce-df) - b(cf+de), a(cf+de) + b(ce-df)) \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf)\end{aligned}$$

   As expressões são idênticas.

2. **Comutatividade:**

$$\begin{aligned}z_1 \cdot z_2 &= (ac - bd, ad + bc) \\ z_2 \cdot z_1 &= (ca - db, cb + da) = (ac - bd, ad + bc)\end{aligned}$$

3. **Elemento Identidade:** O par $(1,0) \in \mathbb{C}^*$ é a identidade multiplicativa (denotada $1_{\mathbb{C}}$), pois:
$$(a,b) \cdot (1,0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a,b)$$

4. **Elemento Inverso:** Seja $z = (a,b) \in \mathbb{C}^*$. Procuramos $z^{-1} = (x,y)$ tal que $(a,b) \cdot (x,y) = (1,0)$.
$$(ax - by, ay + bx) = (1,0)$$

   Isso gera um sistema de equações em $\mathbb{R}$:

$$\begin{aligned}ax - by &= 1 \\ bx + ay &= 0\end{aligned}$$

   Como $(a,b) \neq (0,0)$, temos que $a^2 + b^2 \neq 0$. Resolveremos o sistema da seguinte maneira:

- **Para encontrar x:** Multiplicamos a equação (I) por a, a equação (II) por b e somamos as duas equações resultantes:

$$\begin{aligned}(a^2x - aby) + (b^2x + aby) &= (a \cdot 1) + (b \cdot 0)\\ (a^2 + b^2)x &= a\\ x &= \frac{a}{a^2 + b^2}\end{aligned}$$

- **Para encontrar y:** Multiplicamos a equação (I) por $-b$, a equação (II) por a e somamos as equações resultantes:

$$\begin{aligned}(-abx + b^2y) + (abx + a^2y) &= (-b \cdot 1) + (a \cdot 0)\\ (b^2 + a^2)y &= -b\\ y &= \frac{-b}{a^2 + b^2}\end{aligned}$$

Portanto, todo elemento não nulo (a, b) possui um inverso multiplicativo único:

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right)$$

5. **Fechamento:** Precisamos garantir que se $z_1, z_2 \in \mathbb{C}^*$, então $z_1 \cdot z_2 \in \mathbb{C}^*$ (ou seja, $z_1 \cdot z_2 \neq 0$). Suponha, por contradição, que $z_1 \neq 0$ e $z_2 \neq 0$, mas que $z_1 \cdot z_2 = 0$. Pelo item anterior, sabemos que existe z_1^{-1}. Multiplicando a equação por z_1^{-1} à esquerda:

$$\begin{aligned}z_1^{-1} \cdot (z_1 \cdot z_2) &= z_1^{-1} \cdot 0\\ (z_1^{-1} \cdot z_1) \cdot z_2 &= 0\\ 1 \cdot z_2 &= 0\\ z_2 &= 0\end{aligned}$$

Isso contradiz a hipótese de que $z_2 \in \mathbb{C}^*$. Portanto, o produto de dois números complexos não nulos é necessariamente não nulo. O conjunto é fechado.

□

5.2.3 Distributividade e Estrutura de Corpo

Proposição 5.2.3. A multiplicação em $\mathbb{C}$ distribui sobre a adição.

Demonstração. Sejam $z_1 = (a, b)$, $z_2 = (c, d)$ e $z_3 = (e, f)$.

$$\begin{aligned} z_1 \cdot (z_2 + z_3) &= (a, b) \cdot (c + e, d + f) \\ &= (a(c + e) - b(d + f), a(d + f) + b(c + e)) \\ &= (ac + ae - bd - bf, ad + af + bc + be) \end{aligned}$$

$$\begin{aligned} (z_1 \cdot z_2) + (z_1 \cdot z_3) &= (ac - bd, ad + bc) + (ae - bf, af + be) \\ &= ((ac - bd) + (ae - bf), (ad + bc) + (af + be)) \\ &= (ac - bd + ae - bf, ad + bc + af + be) \end{aligned}$$

As expressões são idênticas. □

Corolário 5.2.0.1. A estrutura $(\mathbb{C}, +, \cdot)$ é um **corpo**.

Demonstração. Conforme demonstrado, $(\mathbb{C}, +)$ é um grupo abeliano, $(\mathbb{C}^*, \cdot)$ é um grupo abeliano, e a multiplicação é distributiva sobre a adição. Portanto, $\mathbb{C}$ satisfaz todos os axiomas de um corpo. □

5.3 A Inserção de $\mathbb{R}$ em $\mathbb{C}$

Assim como identificamos $\mathbb{Z}$ dentro de $\mathbb{Q}$ e $\mathbb{Q}$ dentro de $\mathbb{R}$, devemos agora mostrar que $\mathbb{C}$ contém uma cópia de $\mathbb{R}$.

Proposição 5.3.1. A função $f : \mathbb{R} \to \mathbb{C}$ definida por $f(x) = (x, 0)$ é um homomorfismo injetivo de corpos.

Demonstração. Sejam $x, y \in \mathbb{R}$.

- **Preservação da Adição:**

$$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$$

- **Preservação da Multiplicação:**

$$f(x \cdot y) = (xy, 0)$$

Por outro lado,

$$f(x) \cdot f(y) = (x, 0) \cdot (y, 0) = (x \cdot y - 0 \cdot 0, x \cdot 0 + 0 \cdot y) = (xy, 0)$$

- **Injetividade:** $\ker(f) = \{x \in \mathbb{R} \mid f(x) = 0_{\mathbb{C}}\}$.

$$f(x) = (x, 0) = (0, 0) \implies x = 0$$

Como o núcleo é trivial ($\{0\}$), a função é injetiva.

□

Este isomorfismo entre $\mathbb{R}$ e o subconjunto (e subcorpo) $\mathbb{R} \times \{0\}$ de $\mathbb{C}$ nos permite identificar o número real x com o número complexo $(x, 0)$.

5.4 A Unidade Imaginária e a Forma Algébrica

5.4.1 A Definição de i

Com a estrutura de corpo estabelecida, podemos agora investigar a solução da equação que motivou esta construção.

Definição 5.4.1 (Unidade Imaginária)**.** A **unidade imaginária**, denotada por i, é o número complexo definido pelo par ordenado $(0, 1)$.

$$i := (0, 1)$$

Proposição 5.4.1 (Propriedade Fundamental de i)**.** O quadrado da unidade imaginária é o número real -1.

$$i^2 = -1$$

Demonstração. Usando a definição de multiplicação em $\mathbb{C}$:

$$i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$$

Através da identificação de $\mathbb{R}$ com o subcorpo $\mathbb{R} \times \{0\}$, o par $(-1, 0)$ é a representação do número real -1. □

5.4.2 Forma Algébrica (Notação $a + bi$)

A notação de par ordenado (a, b) pode ser simplificada usando a unidade imaginária i. Seja $z = (a, b)$ um número complexo. Usando a definição de adição e multiplicação, podemos decompor z:

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

O termo $(0, b)$ pode ser reescrito como um produto:

$$(b, 0) \cdot (0, 1) = (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (0, b)$$

Combinando estes passos e usando a identificação $x \equiv (x, 0)$ e $i \equiv (0, 1)$:

$$z = (a, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + b \cdot i$$

Definição 5.4.2 (Forma Algébrica)**.** A **forma algébrica** de um número complexo $z = (a, b)$ é:

$$z = a + bi$$

Onde $a = \mathrm{Re}(z)$ é a **parte real** e $b = \mathrm{Im}(z)$ é a **parte imaginária**.

5.5 Conjugação, Módulo e Forma Polar a Inexistência de Ordem

5.5.1 Conjugado Complexo

Definição 5.5.1 (Conjugado)**.** Seja $z = a + bi$ um número complexo. O **conjugado** de z, denotado por $\overline{z}$, é definido como:

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

Proposição 5.5.1. Sejam $z, w \in \mathbb{C}$. As seguintes propriedades são válidas:

1. $\overline{z + w} = \overline{z} + \overline{w}$
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
3. $z + \overline{z} = 2 \cdot \mathrm{Re}(z)$
4. $z - \overline{z} = 2i \cdot \mathrm{Im}(z)$
5. $\overline{\overline{z}} = z$

Demonstração. Sejam $z = a + bi$ e $w = c + di$ dois números complexos, onde $a, b, c, d \in \mathbb{R}$.

1. **Prova de $\overline{z + w} = \overline{z} + \overline{w}$:** Calculamos o lado esquerdo (LE):

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

$$(LE) = \overline{z + w} = (a + c) - (b + d)i$$

Calculamos o lado direito (LD):

$$\overline{z} = a - bi \quad \text{e} \quad \overline{w} = c - di$$

$$(LD) = \overline{z} + \overline{w} = (a - bi) + (c - di) = (a + c) + (-b - d)i = (a + c) - (b + d)i$$

Como $LE = LD$, a propriedade é válida.

2. **Prova de $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$:** Calculamos o lado esquerdo (LE):

$$z \cdot w = (ac - bd) + (ad + bc)i$$

$$(LE) = \overline{z \cdot w} = (ac - bd) - (ad + bc)i$$

Calculamos o lado direito (LD):

$$\overline{z} \cdot \overline{w} = (a - bi) \cdot (c - di)$$

Aplicando a definição de multiplicação:

$$(LD) = (a(c) - (-b)(-d)) + (a(-d) + (-b)c)i$$

$$(LD) = (ac - bd) + (-ad - bc)i = (ac - bd) - (ad + bc)i$$

Como $LE = LD$, a propriedade é válida.

3. **Prova de $z + \overline{z} = 2 \cdot \mathbf{Re}(z)$:** Seja $z = a + bi$. Então $\text{Re}(z) = a$ e $\overline{z} = a - bi$.

$$z + \overline{z} = (a + bi) + (a - bi) = (a + a) + (b - b)i = 2a + 0i = 2a$$

Como $2 \cdot \text{Re}(z) = 2a$, a igualdade é verificada.

4. **Prova de $z - \overline{z} = 2i \cdot \mathbf{Im}(z)$:** Seja $z = a + bi$. Então $\text{Im}(z) = b$ e $\overline{z} = a - bi$.

$$z - \overline{z} = (a + bi) - (a - bi) = (a - a) + (b - (-b))i = 0 + 2bi = 2bi$$

Como $2i \cdot \text{Im}(z) = 2i \cdot b = 2bi$, a igualdade é verificada.

5. **Prova de $\overline{\overline{z}} = z$:** Seja $z = a + bi$.

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

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

Portanto, $\overline{\overline{z}} = z$.

□

Observação: As duas primeiras propriedades demonstradas ($\overline{z + w} = \overline{z} + \overline{w}$ e $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$) revelam que a conjugação preserva as operações de adição e multiplicação. Algebricamente, isso implica que uma função $f : \mathbb{C} \to \mathbb{C}$ definida por $f(z) = \overline{z}$ é um **homomorfismo de corpos**. Sob o ponto de vista geométrico, ao associar cada complexo

$z = a+bi$ ao seu conjugado $\overline{z} = a-bi$, estamos mapeando o ponto (a, b) no ponto $(a, -b)$. Visualmente, no Plano Complexo, isso corresponde a uma **reflexão** em torno do eixo real.

Proposição 5.5.2. Seja $z \in \mathbb{C}$. O número z é um número real se, e somente se, ele é igual ao seu conjugado.

$$z \in \mathbb{R} \iff z = \overline{z}$$

Demonstração. ($\Rightarrow$) Suponha que $z \in \mathbb{R}$. Podemos escrever z na forma algébrica como $z = a + 0i$. O conjugado de z é $\overline{z} = a - 0i$. Como $a + 0i = a - 0i = a$, temos que $z = \overline{z}$.

($\Leftarrow$) Suponha que $z = \overline{z}$. Seja $z = a + bi$. A hipótese nos diz que:

$$a + bi = a - bi$$

Subtraindo a de ambos os lados, obtemos:

$$bi = -bi$$

Somando bi a ambos os lados:

$$2bi = 0$$

Como estamos em um corpo e $2 \neq 0$ e $i \neq 0$, a lei do cancelamento implica necessariamente que $b = 0$. Como a parte imaginária de z é nula, concluímos que $z = a \in \mathbb{R}$. □

5.5.2 Módulo

Definição 5.5.2 (Módulo)**.** O **módulo** (ou valor absoluto) de um número complexo $z = a + bi$ é o número real não-negativo $|z|$ definido por:

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

Proposição 5.5.3. Para qualquer $z \in \mathbb{C}$, $z \cdot \overline{z} = |z|^2$.

Demonstração. Seja $z = a + bi$. Então $\overline{z} = a - bi$.

$$z \cdot \overline{z} = (a + bi)(a - bi) = a^2 - (abi) + (bia) - (bi)(bi) = a^2 - (bi)^2 = a^2 - b^2i^2$$

Como $i^2 = -1$:

$$z \cdot \overline{z} = a^2 - b^2(-1) = a^2 + b^2 = |z|^2$$

□

Pode-se obter, através da definição de módulo, outra forma de forma de demonstrar o fechamento de $\mathbb{C}^*$:

Corolário 5.5.0.1 (Fechamento de $\mathbb{C}^*$)**.** Se $z, w \in \mathbb{C}^*$ (são não-nulos), então $z \cdot w \neq 0$.

Demonstração. Se $z \neq 0$, então $|z| > 0$. Se $w \neq 0$, então $|w| > 0$.

Primeiro, demonstraremos a propriedade multiplicativa do módulo: $|z \cdot w| = |z| \cdot |w|$. Utilizando a propriedade $|u|^2 = u \cdot \overline{u}$, a propriedade do conjugado do produto, $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$, e a comutatividade da multiplicação em $\mathbb{C}$, temos:

$$|z \cdot w|^2 = (z \cdot w) \cdot \overline{(z \cdot w)} = (z \cdot w) \cdot (\overline{z} \cdot \overline{w}) = (z \cdot \overline{z}) \cdot (w \cdot \overline{w}) = |z|^2 \cdot |w|^2$$

Como os módulos são números reais não-negativos, podemos extrair a raiz quadrada de ambos os lados, concluindo que $|z \cdot w| = |z| \cdot |w|$.

Retornando à prova do corolário: como $|z| > 0$ e $|w| > 0$, segue que o produto $|z \cdot w| > 0$. Se o módulo de $z \cdot w$ não é zero, o próprio número complexo $z \cdot w$ não pode ser $0_{\mathbb{C}}$. Isto prova que não existem divisores de zero em $\mathbb{C}^*$, confirmando que $\mathbb{C}$ é um domínio de integridade. □

5.5.3 Forma Polar (ou Trigonométrica)

A representação algébrica $z = a+bi$ associa cada número complexo a um par ordenado (a, b), que pode ser visualizado como um ponto P no plano cartesiano.

Podemos descrever a posição deste ponto P não apenas por suas coordenadas cartesianas (a, b), mas por suas coordenadas polares: a distância até a origem e o ângulo formado com o eixo real positivo.

- A distância de P à origem é dada pelo **módulo** $|z| = \sqrt{a^2 + b^2}$, que já definimos.
- O ângulo θ formado pelo segmento OP com o semi-eixo real positivo é chamado de **argumento** de z.

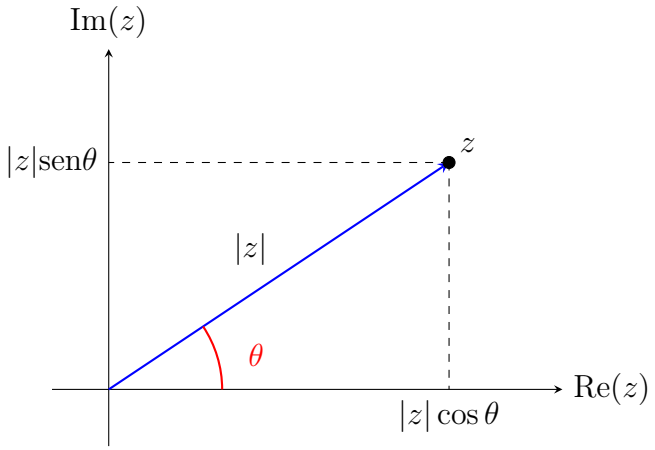
A partir das relações trigonométricas no triângulo retângulo formado pelas coordenadas, temos:

$$a = |z| \cos\theta \quad \text{e} \quad b = |z| \text{sen}\theta$$

Definição 5.5.3 (Forma Polar)**.** Seja $z \in \mathbb{C}$ um número complexo não nulo. A **forma polar** (ou trigonométrica) de z é dada por:

$$z = |z|(\cos\theta + i\text{sen}\theta)$$

Onde θ é um argumento de z. Embora θ possa assumir infinitos valores (diferindo por múltiplos de 2π), geralmente trabalhamos com o **argumento principal**, denotado por $\arg(z)$, tal que $-\pi < \arg(z) \leq \pi$ (ou $0 \leq \arg(z) < 2\pi$, dependendo da convenção).



A grande vantagem da forma polar reside na simplificação das operações de multiplicação e divisão. Geometricamente, multiplicar números complexos corresponde a multiplicar seus tamanhos (módulos) e somar seus ângulos (argumentos).

Proposição 5.5.4 (Multiplicação na Forma Polar)**.** Sejam $z_1 = r_1(\cos\theta_1 + i\text{sen}\theta_1)$ e $z_2 = r_2(\cos\theta_2 + i\text{sen}\theta_2)$ dois números complexos. Então:

$$z_1 \cdot z_2 = r_1 r_2[\cos(\theta_1 + \theta_2) + i\text{sen}(\theta_1 + \theta_2)]$$

Demonstração. Realizamos a multiplicação distributiva e agrupamos as partes real e imaginária:

$$\begin{aligned} z_1 \cdot z_2 &= [r_1(\cos\theta_1 + i\text{sen}\theta_1)] \cdot [r_2(\cos\theta_2 + i\text{sen}\theta_2)] \\ &= r_1 r_2[(\cos\theta_1\cos\theta_2 - \text{sen}\theta_1\text{sen}\theta_2) + i(\text{sen}\theta_1\cos\theta_2 + \cos\theta_1\text{sen}\theta_2)] \end{aligned}$$

Utilizando as fórmulas trigonométricas de adição de arcos para o cosseno e para o seno:

- $\cos(\theta_1 + \theta_2) = \cos\theta_1\cos\theta_2 - \text{sen}\theta_1\text{sen}\theta_2$
- $\text{sen}(\theta_1 + \theta_2) = \text{sen}\theta_1\cos\theta_2 + \cos\theta_1\text{sen}\theta_2$

Substituindo estas identidades na expressão, obtemos:

$$z_1 \cdot z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i\text{sen}(\theta_1 + \theta_2))$$

□

Interpretação Geométrica: O resultado obtido revela que a multiplicação de números complexos não é apenas uma operação algébrica, mas uma transformação geométrica. Ao multiplicarmos um número complexo w por um número z (onde z possui módulo $|z|$ e argumento θ), o vetor que representa w sofre duas alterações simultâneas:

1. Seu comprimento é multiplicado por $|z|$, resultando em uma **dilatação** (se $|z| > 1$) ou **contração** (se $|z| < 1$);

2. Sua direção é alterada, sofrendo uma **rotação** no sentido anti-horário igual ao ângulo θ (o argumento de z).

Dessa forma, quando visto no plano complexo, $z \cdot w$ possui comprimento igual a $r|w|$ e argumento igual a $\arg(w) + \theta$.

Corolário 5.5.0.2 (Divisão na Forma Polar)**.** Sejam $z_1, z_2 \in \mathbb{C}$ com $z_2 \neq 0$, representados na forma polar como acima. Então:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i\text{sen}(\theta_1 - \theta_2)]$$

Proposição 5.5.5 (Fórmula de De Moivre)**.** Seja $z = |z|(\cos\alpha + i\text{sen}\alpha)$ um número complexo na forma polar. Para todo $n \geq 1$, temos:

$$z^n = |z|^n(\cos(n\alpha) + i\text{sen}(n\alpha))$$

Demonstração. A prova é feita por indução sobre n. **Base ($n = 1$):** $z^1 = |z|^1(\cos(1\alpha) + i\text{sen}(1\alpha))$, o que é trivialmente verdadeiro.

Passo Indutivo: Suponha que a fórmula vale para um $n \geq 1$, ou seja, $z^n = |z|^n(\cos(n\alpha) + i\text{sen}(n\alpha))$. Vamos provar para $n + 1$:

$$\begin{aligned} z^{n+1} &= z^n \cdot z \\ &= [|z|^n(\cos(n\alpha) + i\text{sen}(n\alpha))] \cdot [|z|(\cos\alpha + i\text{sen}\alpha)] \\ &= |z|^{n+1}[(\cos(n\alpha)\cos\alpha - \text{sen}(n\alpha)\text{sen}\alpha) + i(\text{sen}(n\alpha)\cos\alpha + \cos(n\alpha)\text{sen}\alpha)] \end{aligned}$$

Utilizando as fórmulas trigonométricas da soma dos arcos:

$$\cos(n\alpha + \alpha) = \cos(n\alpha)\cos\alpha - \text{sen}(n\alpha)\text{sen}\alpha$$

$$\text{sen}(n\alpha + \alpha) = \text{sen}(n\alpha)\cos\alpha + \cos(n\alpha)\text{sen}\alpha$$

Substituindo, obtemos:

$$z^{n+1} = |z|^{n+1}(\cos((n+1)\alpha) + i\text{sen}((n+1)\alpha))$$

O que conclui a indução. □

Como consequência direta, podemos determinar as raízes de um número complexo.

Corolário 5.5.0.3 (Raízes n-ésimas e Raiz Quadrada)**.** Dado $z = |z|(\cos\alpha + i\text{sen}\alpha)$, os

números complexos definidos por:

$$\omega_k = \sqrt[n]{|z|}\left(\cos\left(\frac{\alpha+2\pi k}{n}\right)+i\text{sen}\left(\frac{\alpha+2\pi k}{n}\right)\right)$$

com $k \in \{0,1,\ldots,n-1\}$, satisfazem a equação $X^n = z$.

Prova: Elevando ω_k a n e aplicando a Fórmula de De Moivre:

$$\begin{aligned}(\omega_k)^n &= \left(\sqrt[n]{|z|}\right)^n\left(\cos\left(n\cdot\frac{\alpha+2\pi k}{n}\right)+i\text{sen}\left(n\cdot\frac{\alpha+2\pi k}{n}\right)\right)\\ &= |z|\left(\cos(\alpha+2\pi k)+i\text{sen}(\alpha+2\pi k)\right)\\ &= |z|(\cos\alpha+i\text{sen}\alpha) = z\end{aligned}$$

Em particular, para $n = 2$, isso prova que todo número complexo possui raiz quadrada em $\mathbb{C}$.

5.6 A Impossibilidade de Ordenar $\mathbb{C}$

Proposição 5.6.1. Não é possível definir uma relação de ordem total $\leq$ sobre $\mathbb{C}$ que o torne um corpo ordenado.

Demonstração. A prova é feita por contradição. Suponha que tal relação de ordem $\leq$ exista. Por definição de corpo ordenado, esta relação deve satisfazer:

1. **Tricotomia:** Para todo $z \in \mathbb{C}$, exatamente uma das condições é válida: $z > 0$, $z < 0$, ou $z = 0$.
2. **Compatibilidade:** Se $a > 0$ e $b > 0$, então $a \cdot b > 0$.

Consideremos o elemento $i = (0,1)$. Pela Tricotomia, $i \neq 0$ (pois $i = (0,1) \neq (0,0)$). Portanto, $i > 0$ ou $i < 0$.

- **Caso 1: Suponha $i > 0$.** Pela propriedade de compatibilidade, o produto de dois elementos positivos deve ser positivo.

$$i \cdot i > 0$$

$$i^2 > 0$$

Mas já provamos que $i^2 = -1$. Isso implicaria que $-1 > 0$. Se somarmos 1 a ambos os lados (pela compatibilidade da adição):

$$-1+1 > 0+1 \implies 0 > 1$$

Isso contradiz o fato de que $1 > 0$ (pois $1 = 1^2$, e o quadrado de qualquer elemento não-nulo em um corpo ordenado é positivo).

- **Caso 2: Suponha $i < 0$.** Se $i < 0$, então seu inverso aditivo $-i$ deve ser positivo: $-i > 0$. Pela propriedade de compatibilidade, o produto de dois elementos positivos deve ser positivo:

$$(-i) \cdot (-i) > 0$$

Usando as propriedades de anel, $(-i)(-i) = i^2$.

$$i^2 > 0$$

Isso nos leva exatamente à mesma contradição do Caso 1 ($i^2 = -1 > 0$).

Como ambas as possibilidades levam a uma contradição, a suposição inicial de que uma relação de ordem compatível existe deve ser falsa. □

Capítulo 6

Teorema Fundamental da Álgebra

A construção do corpo dos números complexos $\mathbb{C}$ foi motivada pela necessidade de resolver a equação $x^2 + 1 = 0$. No entanto, uma pergunta natural surge: será que $\mathbb{C}$ é suficiente para resolver qualquer equação polinomial? Ou precisaríamos criar um novo conjunto numérico para resolver $x^5 + 2x - 1 = 0$?

Neste capítulo, formalizaremos o conceito de polinômios e utilizaremos o Teorema Fundamental das Funções Simétricas para demonstrar o Teorema Fundamental da Álgebra, garantindo que $\mathbb{C}$ é algebricamente fechado e encerra nossa cadeia de extensões numéricas.

6.1 O Anel de Polinômios

Começamos definindo formalmente o objeto de nosso estudo sobre um corpo arbitrário $\mathbb{K}$ (que em nosso contexto será $\mathbb{R}$ ou $\mathbb{C}$).

Definição 6.1.1 (Polinômio)**.** Seja $\mathbb{K}$ um corpo. Um **polinômio** na indeterminada (ou variável) x com coeficientes em $\mathbb{K}$ é uma sequência infinita de elementos de $\mathbb{K}$, denotada por $(a_0, a_1, a_2, \dots)$, na qual apenas um número finito de termos é não-nulo. Usualmente, representamos este polinômio pela expressão formal:

$$P(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

O conjunto de todos os polinômios com coeficientes em $\mathbb{K}$ é denotado por $\mathbb{K}[x]$.

- O coeficiente a_n é chamado de **coeficiente líder**.
- O coeficiente a_0 é chamado de **termo independente**.
- Se o coeficiente líder for igual à unidade do corpo (ou seja, $a_n = 1$), o polinômio é chamado de **mônico**.

Observação: É importante notar que esta definição pode ser generalizada naturalmente para o caso em que os coeficientes pertencem a um anel comutativo com unidade (não necessariamente um corpo). Faremos uso desta generalização posteriormente no texto.

Definição 6.1.2 (Grau)**.** Seja $P(x) = \sum_{i=0}^{\infty} a_i x^i$ um polinômio não-nulo. O **grau** de P, denotado por ∂P ou $\deg(P)$, é o maior índice n tal que $a_n \neq 0$. Se $P(x)$ é o polinômio nulo, definimos seu grau como $-\infty$.

6.1.1 Operações em $\mathbb{K}[x]$

Sejam $P(x) = \sum_{i=0}^{n} a_i x^i$ e $Q(x) = \sum_{j=0}^{m} b_j x^j$.

- **Adição:** A soma é realizada termo a termo. Somamos os coeficientes que acompanham a mesma potência de x.

$$(P+Q)(x) = \sum_{k=0}^{\max(n,m)} (a_k + b_k)x^k$$

  O grau do polinômio soma será menor ou igual ao máximo dos graus de P e Q, dependendo se os coeficientes líderes se cancelam ou não.

- **Multiplicação:** O produto baseia-se na propriedade distributiva e na regra de potências $x^i \cdot x^j = x^{i+j}$. O coeficiente c_k do termo x^k no produto é obtido pela soma de todos os produtos $a_i b_j$ onde $i + j = k$:

$$P(x) \cdot Q(x) = \sum_{k=0}^{n+m} c_k x^k, \quad \text{onde } c_k = \sum_{p=0}^{k} a_p b_{k-p}$$

  O termo de maior grau possível no produto surge da multiplicação dos termos líderes de P e Q, ou seja, $(a_n x^n) \cdot (b_m x^m) = (a_n b_m)x^{n+m}$. Como estamos trabalhando em um corpo $\mathbb{K}$, não existem divisores de zero. Logo, como $a_n \neq 0$ e $b_m \neq 0$, o produto $a_n b_m$ é necessariamente diferente de zero. Isso garante que o grau do polinômio produto é exatamente a soma dos graus dos fatores:

$$\deg(P \cdot Q) = \deg(P) + \deg(Q)$$

Proposição 6.1.1. Seja $\mathbb{K}$ um corpo. O conjunto dos polinômios $\mathbb{K}[x]$, munido das operações de adição e multiplicação definidas anteriormente, é um **anel comutativo com unidade**.

Demonstração. Para provar que $(\mathbb{K}[x], +, \cdot)$ é um anel comutativo com unidade, devemos verificar se satisfaz os axiomas de anel. Sejam $P(x) = \sum_{i=0}^{\infty} a_i x^i$, $Q(x) = \sum_{j=0}^{\infty} b_j x^j$ e $R(x) = \sum_{k=0}^{\infty} c_k x^k$ polinômios em $\mathbb{K}[x]$.

1. **Propriedades do Grupo Aditivo** $(\mathbb{K}[x], +)$**:** A adição em $\mathbb{K}[x]$ é definida termo a termo. Como a adição em $\mathbb{K}$ é associativa e comutativa, essas propriedades são herdadas diretamente pelos polinômios.

   - *Elemento Neutro Aditivo:* O polinômio nulo $0(x)$, onde todos os coeficientes são 0, atua como elemento neutro, pois $(a_i + 0) = a_i$.
   - *Inverso Aditivo:* Para cada $P(x)$, existe $-P(x) = \sum(-a_i)x^i$ tal que $P(x) + (-P(x)) = 0$.

   Portanto, $(\mathbb{K}[x], +)$ é um grupo abeliano.

2. **Associatividade da Multiplicação:** Devemos mostrar que $(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$. Seja $S(x) = P(x) \cdot Q(x)$. O coeficiente de grau s em S é $d_s = \sum_{i+j=s} a_i b_j$. Agora, considere o produto $T(x) = S(x) \cdot R(x) = (P \cdot Q) \cdot R$. O coeficiente de grau n em T é:

   $$e_n = \sum_{s+k=n} d_s c_k = \sum_{s+k=n} \left(\sum_{i+j=s} a_i b_j \right) c_k$$

   Substituindo $s = i + j$, a soma percorre todos os índices tais que $(i + j) + k = n$:

   $$e_n = \sum_{i+j+k=n} a_i b_j c_k$$

   Se calcularmos o coeficiente de grau n para $P \cdot (Q \cdot R)$ da mesma maneira, chegaremos exatamente à mesma soma tripla $\sum_{i+j+k=n} a_i(b_j c_k)$, devido à associatividade de $\mathbb{K}$. Logo, a multiplicação é associativa.

3. **Comutatividade da Multiplicação:** O coeficiente de grau k de $P \cdot Q$ é $\sum_{i+j=k} a_i b_j$. O coeficiente de grau k de $Q \cdot P$ é $\sum_{j+i=k} b_j a_i$. Como a multiplicação no corpo $\mathbb{K}$ é comutativa $(a_i b_j = b_j a_i)$ e a adição de inteiros é comutativa $(i+j = j+i)$, os somatórios são idênticos. Logo, $P \cdot Q = Q \cdot P$.

4. **Elemento Unidade:** Considere o polinômio constante $1(x) = 1 + 0x + 0x^2 + \ldots$. O coeficiente de grau k do produto $P(x) \cdot 1(x)$ é:

   $$c_k = \sum_{i+j=k} a_i b_j$$

   Como $b_0 = 1$ e $b_j = 0$ para $j > 0$, o único termo não nulo da soma ocorre quando $j = 0$, o que implica $i = k$.

   $$c_k = a_k \cdot b_0 = a_k \cdot 1 = a_k$$

   Portanto, $P(x) \cdot 1(x) = P(x)$, e o polinômio constante 1 é a unidade.

5. **Distributividade:** O coeficiente de grau k de $P \cdot (Q + R)$ é:

$$\sum_{i+j=k} a_i(b_j + c_j)$$

Pela distributividade em $\mathbb{K}$:

$$\sum_{i+j=k} (a_i b_j + a_i c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j$$

Este é exatamente a soma dos coeficientes de grau k de $P \cdot Q$ e $P \cdot R$. Logo, $P \cdot (Q + R) = P \cdot Q + P \cdot R$.

Concluímos que $\mathbb{K}[x]$ satisfaz todos os axiomas e é um anel comutativo com unidade. □

Proposição 6.1.2 ($\mathbb{K}$[x] é um Domínio de Integridade)**.** Se $\mathbb{K}$ é um corpo (e, portanto, um domínio de integridade), então o anel de polinômios $\mathbb{K}[x]$ não possui divisores de zero. Consequentemente, para quaisquer $P, Q \in \mathbb{K}[x]$ não-nulos:

$$\deg(P \cdot Q) = \deg(P) + \deg(Q)$$

Demonstração. Sejam $P(x)$ e $Q(x)$ dois polinômios não-nulos em $\mathbb{K}[x]$ com $\deg(P) = n$ e $\deg(Q) = m$. Podemos escrevê-los como:

$$P(x) = a_n x^n + \cdots + a_0, \quad \text{com } a_n \neq 0$$

$$Q(x) = b_m x^m + \cdots + b_0, \quad \text{com } b_m \neq 0$$

O produto $P(x) \cdot Q(x)$ terá coeficientes c_k. O termo de maior grau possível provém do produto dos termos líderes de P e Q:

$$(a_n x^n) \cdot (b_m x^m) = (a_n \cdot b_m) x^{n+m}$$

Como $\mathbb{K}$ é um corpo, ele não possui divisores de zero. Sendo $a_n \neq 0$ e $b_m \neq 0$, o produto $a_n \cdot b_m$ é necessariamente diferente de zero. Isso implica que o coeficiente do termo x^{n+m} no produto não se anula. Portanto, $P(x) \cdot Q(x) \neq 0$ (o anel não tem divisores de zero) e o grau do produto é exatamente $n + m$. □

6.1.2 Raízes e Divisibilidade

Um polinômio $P \in \mathbb{K}[x]$ define uma função polinomial $f : \mathbb{K} \to \mathbb{K}$ através da substituição da variável x por um valor $\alpha \in \mathbb{K}$. O valor resultante é denotado por $P(\alpha)$.

Definição 6.1.3 (Raiz)**.** Um elemento $\alpha \in \mathbb{K}$ é chamado de **raiz** (ou zero) do polinômio $P(x)$ se:

$$P(\alpha) = 0$$

Teorema 6.1.1 (Algoritmo da Divisão em $\mathbb{K}$[x])**.** Sejam $P(x)$ e $D(x)$ polinômios em $\mathbb{K}[x]$, com $D(x) \neq 0$. Então, existem únicos polinômios $Q(x)$ (quociente) e $R(x)$ (resto) em $\mathbb{K}[x]$ tais que:

$$P(x) = D(x) \cdot Q(x) + R(x)$$

onde $\deg(R) < \deg(D)$ ou $R(x) = 0$.

Demonstração. A prova divide-se em duas partes: a existência e a unicidade dos polinômios $Q(x)$ e $R(x)$.

Sejam $\deg(P) = n$ e $\deg(D) = m$. Seja a_n o coeficiente líder de $P(x)$ e b_m o coeficiente líder de $D(x)$. Como estamos em um corpo $\mathbb{K}$, e $D(x) \neq 0$, sabemos que $b_m \neq 0$ e possui inverso multiplicativo b_m^{-1}.

Existência: Faremos a prova por indução sobre o grau n de $P(x)$.

Caso Base: Se $n < m$, basta tomarmos $Q(x) = 0$ e $R(x) = P(x)$. A equação $P(x) = D(x) \cdot 0 + P(x)$ é satisfeita e $\deg(R) = n < m = \deg(D)$, ou $R(x) = 0$ se $P(x) = 0$.

Hipótese de Indução: Suponha que a existência vale para todo polinômio com grau menor que n.

Passo Indutivo: Seja $P(x)$ um polinômio de grau $n \geq m$. Vamos tentar reduzir o grau de $P(x)$ subtraindo um múltiplo adequado de $D(x)$. Considere o monômio $T(x) = \frac{a_n}{b_m} x^{n-m}$. Note que a divisão de coeficientes é possível pois $\mathbb{K}$ é um corpo. Agora, construímos um novo polinômio $S(x)$:

$$S(x) = P(x) - T(x) \cdot D(x)$$

Analisando o termo de maior grau:

$$S(x) = (a_n x^n + \dots) - \left(\frac{a_n}{b_m} x^{n-m}\right)(b_m x^m + \dots)$$

$$S(x) = (a_n x^n + \dots) - (a_n x^n + \dots)$$

O termo de grau n se cancela. Portanto, $\deg(S) < n$. Pela hipótese de indução, como o grau de $S(x)$ é menor que n, existem $q_1(x)$ e $r_1(x)$ tais que:

$$S(x) = D(x) \cdot q_1(x) + r_1(x)$$

onde $\deg(r_1) < \deg(D)$ ou $r_1(x) = 0$.

Substituindo a expressão de $S(x)$:

$$P(x) - T(x) \cdot D(x) = D(x) \cdot q_1(x) + r_1(x)$$

Isolando $P(x)$:

$$P(x) = D(x) \cdot [T(x) + q_1(x)] + r_1(x)$$

Definindo $Q(x) = T(x) + q_1(x)$ e $R(x) = r_1(x)$, a existência está provada.

Unicidade: Suponha que existam dois pares de polinômios (Q, R) e (Q', R') que satisfaçam as condições. Então:

$$P(x) = D(x)Q(x) + R(x) = D(x)Q'(x) + R'(x)$$

Isso implica:

$$D(x)[Q(x) - Q'(x)] = R'(x) - R(x)$$

Vamos analisar os graus dos dois lados da igualdade. Se $Q(x) \neq Q'(x)$, então o grau do lado esquerdo é:

$$\deg(D \cdot (Q - Q')) = \deg(D) + \deg(Q - Q') \geq \deg(D)$$

Por outro lado, sabemos que $\deg(R) < \deg(D)$ e $\deg(R') < \deg(D)$. Portanto, o grau da diferença no lado direito deve satisfazer:

$$\deg(R' - R) < \deg(D)$$

Chegamos a uma contradição: o grau do lado esquerdo é maior ou igual a $\deg(D)$, enquanto o grau do lado direito é estritamente menor que $\deg(D)$. A única possibilidade para evitar a contradição é se $Q(x) - Q'(x) = 0$, o que implica $Q(x) = Q'(x)$. Consequentemente, $0 = R'(x) - R(x)$, o que implica $R(x) = R'(x)$. Portanto, o quociente e o resto são únicos. □

Teorema 6.1.2 (Teorema do Resto)**.** O resto da divisão de um polinômio $P(x)$ pelo binômio $(x - \alpha)$ é igual a $P(\alpha)$.

Demonstração. Pelo algoritmo da divisão, temos $P(x) = (x-\alpha)Q(x)+R(x)$, onde o grau de R deve ser menor que o grau de $(x - \alpha)$, que é 1. Logo, $R(x)$ deve ser uma constante r. Substituindo $x = \alpha$:

$$P(\alpha) = (\alpha - \alpha)Q(\alpha) + r = 0 \cdot Q(\alpha) + r = r$$

Portanto, o resto é $P(\alpha)$. □

Teorema 6.1.3 (Teorema do Fator ou Teorema de D'Alembert)**.** Um elemento $\alpha \in \mathbb{K}$ é raiz de um polinômio $P(x)$ se, e somente se, $(x - \alpha)$ divide $P(x)$.

Demonstração. Pelo Teorema do Resto, $P(x) = (x - \alpha)Q(x) + P(\alpha)$.

- ($\Rightarrow$) Se α é raiz, $P(\alpha) = 0$. Logo, $P(x) = (x-\alpha)Q(x)$, ou seja, $(x-\alpha)$ divide $P(x)$.
- ($\Leftarrow$) Se $(x - \alpha)$ divide $P(x)$, então o resto é zero, logo $P(\alpha) = 0$.

□

Proposição 6.1.3. Seja $P(x) \in \mathbb{K}[x]$ um polinômio não-nulo de grau $n \geq 0$. Então, $P(x)$ possui, no máximo, n raízes em $\mathbb{K}$.

Demonstração. A demonstração será feita por indução sobre o grau n do polinômio.

Base da Indução ($n = 0$): Se $\deg(P) = 0$, então $P(x) = c$ para uma constante $c \in \mathbb{K}$ com $c \neq 0$. A condição para α ser raiz é $P(\alpha) = 0$, o que implicaria $c = 0$. Isso contradiz a hipótese de que o polinômio é não-nulo. Portanto, $P(x)$ não possui raízes. Como $0 \leq 0$, a proposição é válida para o caso base.

Hipótese de Indução: Suponha que a proposição seja verdadeira para qualquer polinômio de grau $k = n - 1$. Ou seja, todo polinômio de grau $n - 1$ possui no máximo $n - 1$ raízes.

Passo Indutivo: Seja $P(x)$ um polinômio de grau $n > 0$. Temos dois casos a considerar:

- **Caso 1:** $P(x)$ não possui raízes em $\mathbb{K}$. Neste caso, o número de raízes é 0. Como $n > 0$, temos $0 < n$, e a afirmação é trivialmente verdadeira.
- **Caso 2:** $P(x)$ possui pelo menos uma raiz $\alpha \in \mathbb{K}$. Pelo Teorema do Fator, como $P(\alpha) = 0$, o polinômio $(x - \alpha)$ divide $P(x)$. Portanto, podemos escrever:

$$P(x) = (x - \alpha) \cdot Q(x)$$

Como $\mathbb{K}[x]$ é um domínio de integridade, o grau do produto é a soma dos graus:

$$\deg(P) = \deg(x - \alpha) + \deg(Q) \implies n = 1 + \deg(Q) \implies \deg(Q) = n - 1$$

Agora, seja $\beta \in \mathbb{K}$ uma raiz qualquer de $P(x)$. Substituindo na equação fatorada:

$$P(\beta) = (\beta - \alpha) \cdot Q(\beta) = 0$$

Como $\mathbb{K}$ é um corpo, não existem divisores de zero. Logo, para que o produto seja nulo, um dos fatores deve ser nulo:

$$\beta - \alpha = 0 \quad \text{ou} \quad Q(\beta) = 0$$

$$\beta = \alpha \quad \text{ou} \quad \beta \text{ é raiz de } Q(x)$$

Isso demonstra que qualquer raiz de $P(x)$ ou é o próprio α ou é uma raiz do polinômio $Q(x)$. Pela **hipótese de indução**, como $Q(x)$ tem grau $n-1$, ele possui no máximo $n-1$ raízes distintas. Portanto, o conjunto das raízes de $P(x)$ contém α e, no máximo, outras $n-1$ raízes provenientes de $Q(x)$. Total de raízes $\leq 1+(n-1) = n$.

Isso completa o passo indutivo e a demonstração. □

6.2 Polinômios Simétricos

Definição 6.2.1 (Ação de Permutação)**.** Dada uma permutação $\sigma \in S_n$ e um polinômio $P \in \mathbb{K}[x_1, \ldots, x_n]$, definimos a ação de σ sobre P, denotada por P^σ, como:

$$P^\sigma(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Exemplo 6.2.1. Considere o polinômio $P(x_1, x_2, x_3) = x_1 - 2x_2 + x_3^2$. Seja $\sigma = (1\ 2) \in S_3$ a permutação que troca os índices 1 e 2 (ou seja, $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$). A ação de σ sobre P resulta em:

$$P^\sigma(x_1, x_2, x_3) = P(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}) = P(x_2, x_1, x_3)$$

Substituindo na expressão do polinômio, temos:

$$P^\sigma = x_2 - 2x_1 + x_3^2$$

Definição 6.2.2 (Polinômio Simétrico)**.** Um polinômio $P \in \mathbb{K}[x_1, \ldots, x_n]$ é dito **simétrico** se ele é invariante sob a ação de qualquer permutação $\sigma \in S_n$. Ou seja:

$$P^\sigma = P, \quad \forall \sigma \in S_n$$

Exemplo 6.2.2. Considere o polinômio $P = x_1^2 + x_2^2 + 3x_1x_2 \in \mathbb{K}[x_1, x_2]$. Seja $\sigma = (1\ 2) \in S_2$ a transposição que troca 1 e 2. A ação de σ em P resulta em:

$$P^\sigma = x_{\sigma(1)}^2 + x_{\sigma(2)}^2 + 3x_{\sigma(1)}x_{\sigma(2)} = x_2^2 + x_1^2 + 3x_2x_1$$

Como a adição e multiplicação em $\mathbb{K}[x_1, x_2]$ são comutativas, $P^\sigma = P$. Logo, P é simétrico. Já para $Q = x_1 - x_2$, temos $Q^\sigma = x_2 - x_1 = -(x_1 - x_2) \neq Q$. Logo, Q não é simétrico.

Definição 6.2.3 (Polinômios Simétricos Elementares)**.** Definimos os seguintes polinômios

especiais, chamados de **polinômios simétricos elementares**:

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + \cdots + x_n = \sum_{1\leq i\leq n} x_i \\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sum_{1\leq i<j\leq n} x_ix_j \\
\sigma_3 &= \sum_{1\leq i<j<k\leq n} x_ix_jx_k \\
&\vdots \\
\sigma_k &= \sum_{1\leq i_1<\cdots<i_k\leq n} x_{i_1}\ldots x_{i_k} \\
&\vdots \\
\sigma_n &= x_1x_2\ldots x_n
\end{aligned}$$

Teorema 6.2.1 (Fórmula de Viète)**.** Seja $P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0$ um polinômio mônico com coeficientes em um anel A. Suponha que $P(t)$ se fatora totalmente em A, isto é, existem $x_1, x_2, \ldots, x_n \in A$ tais que:

$$P(t) = (t - x_1)(t - x_2)\cdots(t - x_n)$$

Então, os coeficientes a_k estão relacionados às funções simétricas elementares σ_k avaliadas nas raízes da seguinte forma:

$$a_{n-k} = (-1)^k\sigma_k(x_1, \ldots, x_n)$$

Para $1 \leq k \leq n$.

Demonstração. Considere a expansão do produto:

$$P(t) = (t - x_1)(t - x_2)\cdots(t - x_n)$$

Para determinar o coeficiente de t^{n-k} nesta expansão, observamos como os termos são formados. Ao expandir o produto, cada termo é resultado da escolha de exatamente um somando de cada um dos n fatores $(t - x_i)$.

Para obter uma potência t^{n-k}, devemos escolher a variável t em exatamente $n - k$ fatores. Consequentemente, nos k fatores restantes, somos obrigados a escolher o termo constante $-x_i$.

Sejam $i_1, i_2, \ldots, i_k$ os índices dos k fatores onde escolhemos os termos constantes, com $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. O produto desses termos é:

$$(-x_{i_1})(-x_{i_2})\cdots(-x_{i_k}) = (-1)^k x_{i_1}x_{i_2}\cdots x_{i_k}$$

O coeficiente total de t^{n-k} no polinômio expandido é a soma de todos os produtos possíveis formados dessa maneira, variando sobre todas as escolhas de k índices distintos:

$$\text{Coeficiente de } t^{n-k} = \sum_{1 \leq i_1 < \cdots < i_k \leq n} (-1)^k x_{i_1} x_{i_2} \cdots x_{i_k}$$

Podemos colocar o fator $(-1)^k$ em evidência:

$$\text{Coeficiente de } t^{n-k} = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

Pela definição de polinômio simétrico elementar σ_k, o somatório à direita é exatamente $\sigma_k(x_1, \ldots, x_n)$. Portanto:

$$\text{Coeficiente de } t^{n-k} = (-1)^k \sigma_k(x_1, \ldots, x_n)$$

Por outro lado, a forma original do polinômio é dada por:

$$P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_{n-k}t^{n-k} + \cdots + a_0$$

Comparando os coeficientes de t^{n-k} nas duas expressões de $P(t)$, concluímos que:

$$a_{n-k} = (-1)^k \sigma_k(x_1, \ldots, x_n)$$

□

6.2.1 Teorema Fundamental das Funções Simétricas

Teorema 6.2.2 (Teorema Fundamental das Funções Simétricas)**.** Todo polinômio simétrico $P \in \mathbb{K}[x_1, \ldots, x_n]$ pode ser escrito como um polinômio nas funções simétricas elementares $\sigma_1, \ldots, \sigma_n$. Isto é, se P é simétrico, existe Q tal que:

$$P(x_1, \ldots, x_n) = Q(\sigma_1, \ldots, \sigma_n)$$

Demonstração. A demonstração será feita por indução sobre o número de variáveis n.

Base da Indução ($n = 2$): Seja $P(x_1, x_2)$ um polinômio simétrico em duas variáveis. Podemos encarar P como um polinômio na variável x_1 com coeficientes no anel $\mathbb{K}[x_2]$.

$$P(x_1, x_2) = \sum_{j=0}^{k} A_j(x_2) x_1^j$$

Sabemos que $\sigma_1 = x_1 + x_2$, o que implica $x_2 = \sigma_1 - x_1$. Substituindo essa relação nos

coeficientes $A_j(x_2)$, cada A_j torna-se um polinômio em x_1 com coeficientes que dependem de σ_1. Reagrupando os termos, podemos reescrever P na forma de um polinômio na variável x_1 cujos coeficientes pertencem a $\mathbb{K}[\sigma_1]$:

$$P(x_1, x_2) = B_0(\sigma_1) + B_1(\sigma_1)x_1 + B_2(\sigma_1)x_1^2 + \cdots + B_m(\sigma_1)x_1^m$$

Vamos definir um polinômio auxiliar $K(t)$ na variável t substituindo x_1 por t na expressão acima:

$$K(t) = B_0(\sigma_1) + B_1(\sigma_1)t + \cdots + B_m(\sigma_1)t^m \in \mathbb{K}[\sigma_1][t]$$

Note que, por construção, $K(x_1) = P(x_1, x_2)$. Devido à simetria de P, temos que $P(x_1, x_2) = P(x_2, x_1)$. Além disso, como os coeficientes $B_j(\sigma_1)$ dependem apenas de σ_1, que é invariante por permutação, a forma funcional de K é a mesma para qualquer variável. Portanto, $K(x_2)$ resulta na mesma expressão, apenas trocando x_1 por x_2, o que corresponde a $P(x_2, x_1)$. Logo, temos que $K(x_1) = P$ e $K(x_2) = P$.

Considere agora o polinômio mônico cujas raízes são x_1 e x_2:

$$M(t) = (t - x_1)(t - x_2) = t^2 - (x_1 + x_2)t + x_1x_2 = t^2 - \sigma_1 t + \sigma_2$$

Note que $M(t) \in \mathbb{K}[\sigma_1, \sigma_2][t]$. Pelo Algoritmo da Divisão de polinômios na variável t no anel $\mathbb{K}[\sigma_1, \sigma_2][t]$, podemos dividir $K(t)$ por $M(t)$:

$$K(t) = M(t) \cdot Q(t) + R(t)$$

onde $Q(t), R(t) \in \mathbb{K}[\sigma_1, \sigma_2][t]$ e o grau de $R(t)$ é estritamente menor que o grau de $M(t)$, ou seja, $\deg_t(R) < 2$. Podemos escrever $R(t) = C_1t + C_0$, com $C_1, C_0 \in \mathbb{K}[\sigma_1, \sigma_2]$.

Substituindo $t = x_1$ na equação da divisão:

$$K(x_1) = \underbrace{M(x_1)}_{0} \cdot Q(x_1) + R(x_1) \implies P = C_1x_1 + C_0$$

Substituindo $t = x_2$:

$$K(x_2) = \underbrace{M(x_2)}_{0} \cdot Q(x_2) + R(x_2) \implies P = C_1x_2 + C_0$$

Igualando as duas expressões para P:

$$C_1x_1 + C_0 = C_1x_2 + C_0 \implies C_1(x_1 - x_2) = 0$$

Como estamos em um domínio de integridade (anel de polinômios) e $x_1 \neq x_2$ (como variáveis independentes), concluímos que $C_1 = 0$. Portanto, $P = C_0$. Como

$C_0 \in \mathbb{K}[\sigma_1, \sigma_2]$, demonstramos que P é um polinômio nas funções simétricas elementares.

Passo Indutivo: Suponha que o teorema seja verdadeiro para $n-1$ variáveis. Vamos provar para n variáveis. Seja $P(x_1, \ldots, x_n)$ um polinômio simétrico. Encaramos P como um polinômio em x_1 com coeficientes em $\mathbb{K}[x_2, \ldots, x_n]$:

$$P = \sum_{j=0}^{k} A_j(x_2, \ldots, x_n) x_1^j$$

Como P é simétrico, ele é invariante por permutações das variáveis $\{x_2, \ldots, x_n\}$. Logo, os coeficientes A_j são polinômios simétricos nas $n-1$ variáveis $x_2, \ldots, x_n$. Pela hipótese de indução, cada A_j pode ser escrito em termos das funções simétricas elementares dessas $n-1$ variáveis, que denotaremos por $\tau_1, \ldots, \tau_{n-1}$. As relações entre as funções simétricas τ_k (de $x_2, \ldots, x_n$) e σ_k (de $x_1, \ldots, x_n$) são dadas por:

$$\begin{aligned}
&\sigma_1 = x_1 + \tau_1 \implies \tau_1 = \sigma_1 - x_1 \\
&\sigma_2 = x_1\tau_1 + \tau_2 \implies \tau_2 = \sigma_2 - x_1\tau_1 = \sigma_2 - x_1(\sigma_1 - x_1) \\
&\quad \vdots \\
&\sigma_k = x_1\tau_{k-1} + \tau_k \implies \tau_k = \sigma_k - x_1\tau_{k-1}
\end{aligned}$$

Recursivamente, vemos que cada τ_k pode ser expresso como um polinômio em x_1 com coeficientes em $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$. Substituindo essas expressões em P, obtemos, de forma análoga ao caso base, que P pode ser escrito como um polinômio na variável x_1 com coeficientes no anel das funções simétricas $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$. Definimos então o polinômio auxiliar $K(t) \in \mathbb{K}[\sigma_1, \ldots, \sigma_n][t]$ tal que $K(x_1) = P$. Pela simetria de P e a invariância dos coeficientes (que dependem apenas de σ), temos que $K(x_i) = P$ para todo $i = 1, \ldots, n$.

Considere o polinômio:

$$M(t) = \prod_{i=1}^{n}(t - x_i) = t^n - \sigma_1 t^{n-1} + \cdots + (-1)^n \sigma_n$$

Temos que $M(t) \in \mathbb{K}[\sigma_1, \ldots, \sigma_n][t]$. Pelo Algoritmo da Divisão em $\mathbb{K}[\sigma_1, \ldots, \sigma_n][t]$, dividimos $K(t)$ por $M(t)$:

$$K(t) = M(t) \cdot Q(t) + R(t)$$

com $\deg_t(R) < n$. Substituindo $t = x_i$ para cada $i \in \{1, \ldots, n\}$, temos $M(x_i) = 0$, logo:

$$R(x_i) = K(x_i) = P$$

Considere agora o polinômio $S(t) = R(t) - P$. Neste ponto, estamos considerando $S(t)$ como um elemento do anel $\mathbb{K}[x_1, \ldots, x_n][t]$. Isso ocorre porque $P \in \mathbb{K}[x_1, \ldots, x_n]$ e

os coeficientes de $R(t)$, que dependem dos elementares σ_i, também são polinômios nas variáveis $x_1, \ldots, x_n$. O grau de $S(t)$ é o mesmo de $R(t)$, ou seja, menor que n. No entanto, $S(x_i) = R(x_i) - P = 0$ para todo $i = 1, \ldots, n$. O polinômio $S(t)$ possui n raízes distintas $(x_1, \ldots, x_n)$. O único polinômio de grau estritamente menor que n que possui n raízes é o polinômio identicamente nulo. Logo, $S(t) = 0 \implies R(t) = P$. Como $R(t) \in \mathbb{K}[\sigma_1, \ldots, \sigma_n][t]$ e é igual à constante P (em relação a t), concluímos que P não depende de t e seus coeficientes estão em $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$. Portanto, $P \in \mathbb{K}[\sigma_1, \ldots, \sigma_n]$, o que conclui a prova. □

6.3 Teorema Fundamental da Álgebra

Proposição 6.3.1 (Polinômios de Grau 2 em $\mathbb{C}$)**.** Todo polinômio de grau 2 com coeficientes complexos possui raízes em $\mathbb{C}$.

Demonstração. Seja $P(z) = az^2 + bz + c$ com $a, b, c \in \mathbb{C}$ e $a \neq 0$. Podemos completar o quadrado:

$$az^2 + bz + c = 0 \iff z^2 + \frac{b}{a}z = -\frac{c}{a}$$

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

$$\left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

Seja $\Delta = b^2 - 4ac$. Pela propriedade das raízes n-ésimas (aplicada aqui para $n = 2$), garantimos que existem números complexos cujo quadrado é igual a Δ. Seja $\sqrt{\Delta}$ uma dessas raízes fixada (tal que $(\sqrt{\Delta})^2 = \Delta$). Podemos reescrever a equação como:

$$\left(z + \frac{b}{2a}\right)^2 = \left(\frac{\sqrt{\Delta}}{2a}\right)^2$$

Para simplificar a argumentação, defina $W = z + \frac{b}{2a}$ e a constante $K = \frac{\sqrt{\Delta}}{2a}$. A equação torna-se $W^2 = K^2$, ou equivalentemente, $W^2 - K^2 = 0$. Observe que:

- Se substituirmos W por K, temos $K^2 = K^2$, logo K é solução.
- Se substituirmos W por $-K$, temos $(-K)^2 = (-1)^2K^2 = K^2$, logo $-K$ também é solução.

Como $W^2 - K^2 = 0$ é uma equação polinomial de grau 2 sobre um corpo, ela possui no máximo duas raízes distintas. Como já identificamos duas soluções (K e $-K$), estas são as únicas possíveis. Portanto, podemos afirmar com segurança que:

$$z + \frac{b}{2a} = \pm K = \pm\frac{\sqrt{\Delta}}{2a}$$

Isolando z:

$$z = \frac{-b \pm \sqrt{\Delta}}{2a}$$

Como todas as operações envolvidas (soma, produto, inverso e extração de raiz) são fechadas em $\mathbb{C}$, as raízes z pertencem a $\mathbb{C}$. □

Teorema 6.3.1 (Existência de Corpos de Decomposição)**.** Seja $\mathbb{K}$ um corpo e $P(t) \in \mathbb{K}[t]$ um polinômio de grau $n \geq 1$. Existe uma extensão de corpos $\mathbb{F} \supseteq \mathbb{K}$ tal que $P(t)$ se fatora completamente em $\mathbb{F}[t]$ como produto de fatores lineares:

$$P(t) = c(t - x_1)(t - x_2) \cdots (t - x_n)$$

onde $c \in \mathbb{K}$ é o coeficiente líder de $P(t)$ e $x_1, \ldots, x_n \in \mathbb{F}$. O corpo $\mathbb{F}$ é chamado de **corpo de decomposição** de $P(t)$.

Demonstração. A demonstração será feita por **indução sobre o grau** n do polinômio $P(t)$.

Caso Base ($n = 1$): Se $\partial P = 1$, então $P(t)$ é da forma $at + b$ com $a \neq 0$. A raiz deste polinômio é $x_1 = -a^{-1}b$, que pertence ao próprio corpo $\mathbb{K}$. Neste caso, o corpo de decomposição é o próprio $\mathbb{K}$ (ou seja, $\mathbb{F} = \mathbb{K}$), e a base da indução é válida.

Passo Indutivo: Suponha que o teorema seja verdadeiro para qualquer polinômio de grau $n - 1$. Vamos provar que ele vale para um polinômio $P(t)$ de grau n.

Seja $p(t)$ um fator irredutível de $P(t)$ em $\mathbb{K}[t]$. Construímos a extensão $\mathbb{E}$ como o anel quociente:

$$\mathbb{E} = \frac{\mathbb{K}[t]}{\langle p(t) \rangle}$$

Como $p(t)$ é irredutível, $\mathbb{E}$ é um corpo. Além disso, os elementos de $\mathbb{K}$ podem ser identificados com as classes dos polinômios constantes em $\mathbb{E}$, de modo que temos a inclusão $\mathbb{K} \subseteq \mathbb{E}$.

O elemento $\alpha_1 = [t] = t + \langle p(t) \rangle \in \mathbb{E}$ é uma raiz de $p(t)$, pois $p(\alpha_1) = [p(t)] = 0$. Consequentemente, α_1 também é raiz de $P(t)$. Portanto, no anel de polinômios $\mathbb{E}[t]$, podemos fatorar $P(t)$ como:

$$P(t) = (t - \alpha_1) \cdot Q(t)$$

Pelas propriedades de grau, como $\partial P = n$, o polinômio $Q(t)$ deve ter grau $n - 1$.

Agora, aplicamos a **Hipótese de Indução** ao polinômio $Q(t) \in \mathbb{E}[t]$. Existe um corpo $\mathbb{F} \supseteq \mathbb{E}$ onde $Q(t)$ se fatora completamente:

$$Q(t) = c(t - x_2) \cdots (t - x_n)$$

com $x_2, \ldots, x_n \in \mathbb{F}$.

Substituindo de volta na expressão de $P(t)$ e fazendo $x_1 = \alpha_1$, obtemos:

$$P(t) = c(t - x_1)(t - x_2) \cdots (t - x_n)$$

Como $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{F}$, o corpo $\mathbb{F}$ é a extensão procurada onde $P(t)$ se decompõe totalmente. □

Proposição 6.3.2. Seja $P(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n \in \mathbb{R}[t]$ um polinômio com coeficientes reais e grau $n \geq 1$. Então $P(t)$ admite uma raiz complexa.

Demonstração. Antes de iniciar a indução, observe que as raízes de $P(t)$ são exatamente as mesmas raízes do polinômio $H(t) = \frac{1}{a_n}P(t)$. De fato, dado um polinômio arbitrário $P(t)$ com $a_n \neq 0$, podemos definir o polinômio normalizado $H(t) = a_n^{-1} \cdot P(t)$. Como a_n é uma constante não nula, temos que:

$$H(\alpha) = 0 \iff a_n^{-1} \cdot P(\alpha) = 0 \iff P(\alpha) = 0$$

Ou seja, o conjunto de raízes de $P(t)$ é idêntico ao conjunto de raízes de $H(t)$. Portanto, sem perda de generalidade, assumiremos no restante desta demonstração que $P(t)$ é mônico, isto é, $a_n = 1$.

Pelo Teorema Fundamental da Aritmética, podemos escrever o grau do polinômio como $n = 2^m\alpha$, onde $m \geq 0$ é um inteiro e α é um número ímpar. Faremos a prova por indução sobre m.

Base da Indução ($m = 0$): Neste caso, $n = 2^0\alpha = \alpha$, que é um número ímpar. Como assumimos que $P(t)$ é mônico, temos $P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$. Para $|t|$ suficientemente grande, o termo t^n determina o sinal do polinômio. Como n é ímpar, temos os seguintes limites:

$$\lim_{t \to +\infty} P(t) = +\infty \quad \text{e} \quad \lim_{t \to -\infty} P(t) = -\infty$$

Portanto, existem números reais $a < b$ tais que $P(a) < 0$ e $P(b) > 0$.

Vamos construir indutivamente uma sequência de pares de números reais (a_k, b_k) tal que, para todo k, tenhamos $a_k \leq b_k$ e $P(a_k) < 0 \leq P(b_k)$. Definimos o par inicial como $(a_0, b_0) = (a, b)$. Para cada passo $k \geq 0$, seja $m_k = \frac{a_k + b_k}{2}$ o ponto médio. Temos três possibilidades:

1. Se $P(m_k) = 0$, encontramos a raiz e a prova termina.
2. Se $P(m_k) < 0$, definimos o próximo par como $(a_{k+1}, b_{k+1}) = (m_k, b_k)$.
3. Se $P(m_k) > 0$, definimos o próximo par como $(a_{k+1}, b_{k+1}) = (a_k, m_k)$.

Dessa construção, obtemos duas sequências $(a_k)_{k \in \mathbb{N}}$ e $(b_k)_{k \in \mathbb{N}}$ com as seguintes propriedades:

- A sequência (a_k) é não decrescente $(a_0 \leq a_1 \leq a_2 \dots)$.
- A sequência (b_k) é não crescente $(b_0 \geq b_1 \geq b_2 \dots)$.
- A distância entre os termos é dada por $b_k - a_k = \frac{b-a}{2^k}$.

Quando $k \to \infty$, a distância $b_k - a_k$ tende a zero. Isso implica que (a_k) e (b_k) são sequências de Cauchy em $\mathbb{R}$. Pela completude dos números reais, ambas as sequências convergem para um mesmo limite $\xi \in \mathbb{R}$.

Agora, utilizamos as propriedades aritméticas de limites. Como o limite da soma é a soma dos limites e o limite do produto é o produto dos limites, temos que:

$$\lim_{k\to\infty} P(a_k) = P\left(\lim_{k\to\infty} a_k\right) = P(\xi)$$

Como $P(a_k) < 0$ para todo k, segue que $P(\xi) \leq 0$. Analogamente, para a sequência (b_k):

$$\lim_{k\to\infty} P(b_k) = P(\xi)$$

Como $P(b_k) \geq 0$ para todo k, segue que $P(\xi) \geq 0$.

Sendo $P(\xi) \leq 0$ e $P(\xi) \geq 0$, concluímos obrigatoriamente que $P(\xi) = 0$. Portanto, existe $\xi \in \mathbb{R} \subset \mathbb{C}$ que é raiz de $P(t)$.

Passo Indutivo: Suponha que o teorema seja verdadeiro para qualquer polinômio com coeficientes reais cujo grau seja da forma $2^{m-1}\beta$, com β ímpar. Vamos provar que vale para um polinômio $P(t)$ de grau $n = 2^m\alpha$ $(m \geq 1)$.

Seja $P(t) \in \mathbb{R}[t]$ com grau $n = 2^m\alpha$. Pelo Teorema da Existência do Corpo de Decomposição, sabemos que existe um corpo $\mathbb{F}$ que é uma extensão de $\mathbb{R}$ (isto é, $\mathbb{R} \subseteq \mathbb{F}$) tal que $P(t)$ se fatora completamente em $\mathbb{F}$. Sejam $x_1, \dots, x_n \in \mathbb{F}$ as raízes de $P(t)$ neste corpo estendido. Nosso objetivo é mostrar que, apesar de estarem a principio em um corpo $\mathbb{F}$ desconhecido, pelo menos uma dessas raízes pertence a $\mathbb{C}$.

Fixe um número real $\gamma \in \mathbb{R}$. Para cada par de índices $\{i, j\}$ com $1 \leq i < j \leq n$, definimos o elemento:

$$z_{i,j}^{(\gamma)} = x_i + x_j + \gamma x_i x_j$$

Seja $\mathcal{F}_2$ o conjunto de todos os pares $\{i, j\}$. O número de tais pares é $K = \binom{n}{2} = \frac{n(n-1)}{2}$. Substituindo $n = 2^m\alpha$:

$$K = \frac{2^m\alpha(2^m\alpha - 1)}{2} = 2^{m-1}\alpha(2^m\alpha - 1)$$

Como α é ímpar e $(2^m\alpha - 1)$ é ímpar (pois $m \geq 1$, logo 2^m é par), o produto $\beta = \alpha(2^m\alpha - 1)$ é ímpar. Portanto, o número de elementos $z_{i,j}^{(\gamma)}$ é $K = 2^{m-1}\beta$.

Definimos agora um novo polinômio $Q_\gamma(t)$ cujas raízes são esses elementos:

$$Q_\gamma(t) = \prod_{\{i,j\}\in\mathcal{F}_2} (t - z_{i,j}^{(\gamma)})$$

O grau de $Q_\gamma(t)$ é $K = 2^{m-1}\beta$.

Vamos analisar os coeficientes de $Q_\gamma(t)$. Eles são (a menos de sinal) as funções simétricas elementares das raízes $z_{i,j}^{(\gamma)}$. Para garantir que esses coeficientes são invariantes sob permutações das raízes originais x_k, utilizamos o seguinte resultado auxiliar:

Lema: (Permutação em Pares de Índices)
Seja S_n o grupo das permutações do conjunto $\{1, 2, \ldots, n\}$ e seja $\mathcal{F}_2$ o conjunto de todos os subconjuntos de $\{1, 2, \ldots, n\}$ contendo exatamente dois elementos. Dada uma bijeção $\sigma \in S_n$, a função induzida $\sigma^* : \mathcal{F}_2 \to \mathcal{F}_2$ definida por:

$$\sigma^*(\{i, j\}) = \{\sigma(i), \sigma(j)\}$$

é também uma bijeção.

Prova do Lema. Como σ é injetiva, se $i \neq j$, então $\sigma(i) \neq \sigma(j)$, o que garante que a imagem $\{\sigma(i), \sigma(j)\}$ é de fato um elemento de $\mathcal{F}_2$. Para mostrar que σ^* é uma bijeção, basta exibir sua inversa. Considere a permutação inversa $\sigma^{-1} \in S_n$. Definimos $(\sigma^{-1})^* : \mathcal{F}_2 \to \mathcal{F}_2$ por $\{u, v\} \mapsto \{\sigma^{-1}(u), \sigma^{-1}(v)\}$. A composição $(\sigma^* \circ (\sigma^{-1})^*)(\{u, v\}) = \{\sigma(\sigma^{-1}(u)), \sigma(\sigma^{-1}(v))\} = \{u, v\}$ mostra que σ^* é sobrejetiva e injetiva. Portanto, σ^* é bijetiva. □

Retornando à prova principal: Observe que qualquer permutação $\sigma \in S_n$ das raízes originais $x_1, \ldots, x_n$ permuta os pares $\{i, j\}$ e, consequentemente, permuta os elementos $z_{i,j}^{(\gamma)}$. Como os coeficientes de $Q_\gamma(t)$ são funções simétricas nas variáveis $z_{i,j}^{(\gamma)}$, eles permanecem invariantes sob qualquer permutação das raízes x_k. Pelo Teorema Fundamental das Funções Simétricas, qualquer expressão polinomial nas raízes $x_1, \ldots, x_n$ que seja invariante por permutações pode ser escrita em termos das funções simétricas elementares de x_k. As funções simétricas elementares de $x_1, \ldots, x_n$ são exatamente os coeficientes de $P(t)$ (a menos de sinal), que são números reais. Portanto, os coeficientes de $Q_\gamma(t)$ são números reais.

Como $Q_\gamma(t) \in \mathbb{R}[t]$ e seu grau é $2^{m-1}\beta$, podemos aplicar a **hipótese de indução**. Logo, $Q_\gamma(t)$ possui pelo menos uma raiz complexa. Isso significa que, para cada $\gamma \in \mathbb{R}$, existe um par $\{i, j\}$ tal que:

$$x_i + x_j + \gamma x_i x_j \in \mathbb{C}$$

Como existem infinitos valores possíveis para γ (todos os números reais) e apenas um número finito de pares $\{i, j\}$, deve existir um mesmo par $\{i, j\}$ que satisfaz a condição

para dois valores reais distintos de γ, digamos γ_1 e γ_2 (com $\gamma_1 \neq \gamma_2$). Assim, temos:

$$x_i + x_j + \gamma_1 x_i x_j = c_1 \in \mathbb{C}$$
$$x_i + x_j + \gamma_2 x_i x_j = c_2 \in \mathbb{C}$$

Subtraindo as duas equações:

$$(\gamma_1 - \gamma_2) x_i x_j = c_1 - c_2$$

Como $\gamma_1 - \gamma_2$ é um número real não nulo e $c_1 - c_2 \in \mathbb{C}$, concluímos que:

$$x_i x_j = \frac{c_1 - c_2}{\gamma_1 - \gamma_2} \in \mathbb{C}$$

Substituindo $x_i x_j$ na primeira equação, vemos que $x_i + x_j$ também deve ser complexo:

$$x_i + x_j = c_1 - \gamma_1 (x_i x_j) \in \mathbb{C}$$

Agora, x_i e x_j são raízes do polinômio quadrático:

$$R(t) = (t - x_i)(t - x_j) = t^2 - (x_i + x_j)t + (x_i x_j)$$

Os coeficientes deste polinômio pertencem a $\mathbb{C}$. Como já provamos as raízes de um polinômio quadrático com coeficientes complexos são números complexos. Portanto, $x_i \in \mathbb{C}$ e $x_j \in \mathbb{C}$. Como x_i é uma raiz de $P(t)$, provamos que $P(t)$ admite uma raiz complexa. □

Proposição 6.3.3. Seja $P(z) = \sum_{k=0}^{n} a_k z^k$ um polinômio com coeficientes complexos ($a_k \in \mathbb{C}$). Definimos o polinômio conjugado $\overline{P}(z)$ tomando o conjugado de cada coeficiente:

$$\overline{P}(z) = \sum_{k=0}^{n} \overline{a_k} z^k$$

O polinômio produto $Q(z) = P(z) \cdot \overline{P}(z)$ tem coeficientes reais.

Demonstração. Para mostrar que um número complexo é real, basta mostrar que ele é igual ao seu conjugado. Vamos verificar isso para os coeficientes de $Q(z)$. Observe que para qualquer $z \in \mathbb{R}$ (onde $z = \overline{z}$):

$$\overline{Q(z)} = \overline{P(z) \cdot \overline{P}(z)} = \overline{P(z)} \cdot \overline{\overline{P}(z)} = \overline{P}(z) \cdot P(z) = Q(z)$$

De forma mais explícita nos coeficientes, seja $Q(z) = \sum C_k z^k$. O coeficiente k-ésimo C_k

é dado por:

$$C_k = \sum_{j=0}^{k} a_j \cdot (\text{coef. de } z^{k-j} \text{ em } \overline{P}) = \sum_{j=0}^{k} a_j \cdot \overline{a_{k-j}}$$

Tomando o conjugado de C_k:

$$\overline{C_k} = \overline{\sum_{j=0}^{k} a_j \overline{a_{k-j}}} = \sum_{j=0}^{k} \overline{a_j} a_{k-j}$$

Para verificar que esta soma é igual a C_k, fazemos uma mudança de índices. Seja $m = k-j$. Quando j percorre de 0 a k, m percorre de k a 0. A soma pode ser reescrita como:

$$\overline{C_k} = \sum_{m=0}^{k} \overline{a_{k-m}} a_m = \sum_{m=0}^{k} a_m \overline{a_{k-m}}$$

Esta expressão final é exatamente a definição original de C_k. Como $\overline{C_k} = C_k$, todos os coeficientes de $Q(z)$ são reais. □

Teorema 6.3.2 (Teorema Fundamental da Álgebra)**.** Todo polinômio de grau positivo com coeficientes complexos admite pelo menos uma raiz complexa.

Demonstração. Seja $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ um polinômio com coeficientes complexos e grau positivo ($n \geq 1$). Considere o polinômio conjugado $\overline{P}(z) = \overline{a_n} z^n + \overline{a_{n-1}} z^{n-1} + \cdots + \overline{a_1} z + \overline{a_0}$.

Pela proposição anterior, sabemos que o polinômio produto $Q(z) = P(z) \cdot \overline{P}(z)$ possui coeficientes reais. O grau de $Q(z)$ é a soma dos graus de $P(z)$ e $\overline{P}(z)$, ou seja, $\deg(Q) = n + n = 2n$. Como $n \geq 1$, o grau de $Q(z)$ é pelo menos 2.

Como $Q(z)$ é um polinômio de coeficientes reais e grau positivo, aplicamos a proposição que nos diz que esse tipo de polinômio admite uma raiz complexa, para concluir que existe um $\xi \in \mathbb{C}$ tal que $Q(\xi) = 0$.

Substituindo na definição de $Q(z)$:

$$P(\xi) \cdot \overline{P}(\xi) = 0$$

Como $\mathbb{C}$ é um corpo, e portanto um domínio de integridade, o produto de dois elementos só é zero se pelo menos um deles for zero. Temos duas possibilidades:

1. $P(\xi) = 0$. Neste caso, ξ é uma raiz de $P(z)$, e o teorema está demonstrado.

2. $\overline{P}(\xi) = 0$. Sabemos que $\overline{P}(\xi) = \sum \overline{a_k} \xi^k$. Tomando o conjugado desta equação:

$$\overline{\overline{P}(\xi)} = \overline{0} \implies \sum a_k \overline{\xi}^k = 0 \implies P(\overline{\xi}) = 0$$

   Neste caso, o conjugado de ξ, ou seja, $\overline{\xi}$, é uma raiz de $P(z)$.

Em qualquer caso, encontramos um número complexo que é raiz de $P(z)$, demonstrando o teorema. □

Corolário 6.3.2.1 (Raízes em Pares Conjugados)**.** Se $P(z)$ é um polinômio com coeficientes reais, então se $\xi \in \mathbb{C}$ é uma raiz de $P(z)$, seu conjugado $\overline{\xi}$ também é uma raiz de $P(z)$.

Demonstração. A demonstração segue exatamente a lógica utilizada no final do teorema anterior. O fato fundamental é que a aplicação conjugação $f : \mathbb{C} \to \mathbb{C}$ dada por $f(z) = \overline{z}$ é um **homomorfismo de anéis**, isto é, preserva a adição e a multiplicação:

$$\overline{z + w} = \overline{z} + \overline{w} \quad \text{e} \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

Aplicando isso a um polinômio $P(z) = \sum a_k z^k$ com coeficientes reais (onde $\overline{a_k} = a_k$):

$$\overline{P(\xi)} = \overline{\sum a_k \xi^k} = \sum \overline{a_k}\overline{\xi^k} = \sum a_k (\overline{\xi})^k = P(\overline{\xi})$$

Portanto, se ξ é raiz, temos $P(\xi) = 0$. Aplicando o conjugado em ambos os lados:

$$\overline{P(\xi)} = \overline{0} \implies P(\overline{\xi}) = 0$$

Logo, $\overline{\xi}$ também é raiz. □

Corolário 6.3.2.2 (Fatoração Completa em $\mathbb{C}$)**.** Todo polinômio de grau $n \geq 1$ com coeficientes complexos $P(t) = a_n t^n + \cdots + a_1 t + a_0$ se fatora em termos lineares. Isto é, existem $z_1, z_2, \ldots, z_n \in \mathbb{C}$ tais que:

$$P(t) = a_n (t - z_1)(t - z_2) \cdots (t - z_n)$$

Demonstração. A demonstração será feita por indução sobre o grau n do polinômio.

Base da Indução ($n = 1$): Seja $P(t) = a_1 t + a_0$ com $a_1 \neq 0$. Podemos colocar a_1 em evidência:

$$P(t) = a_1 \left(t + \frac{a_0}{a_1} \right)$$

Definindo $z_1 = -\frac{a_0}{a_1}$, temos $P(t) = a_1(t - z_1)$. O corolário é válido para $n = 1$.

Hipótese de Indução: Suponha que todo polinômio de grau $n - 1$ com coeficientes complexos possa ser fatorado na forma $c(t - r_1) \cdots (t - r_{n-1})$.

Passo Indutivo: Seja $P(t)$ um polinômio de grau n com coeficiente líder a_n. Pelo **Teorema Fundamental da Álgebra**, sabemos que $P(t)$ admite pelo menos uma raiz complexa, digamos $z_1 \in \mathbb{C}$.

Pelo **Teorema do Fator**, como $P(z_1) = 0$, o polinômio $(t - z_1)$ divide $P(t)$. Logo,

existe um polinômio $Q(t)$ tal que:

$$P(t) = (t - z_1)Q(t)$$

Comparando os graus e os coeficientes líderes:

- O grau de $Q(t)$ deve ser $n - 1$.
- O coeficiente líder de $Q(t)$ deve ser o mesmo de $P(t)$, ou seja, a_n.

Como $Q(t)$ tem grau $n - 1$, podemos aplicar a **Hipótese de Indução**. Existem $z_2, \ldots, z_n \in \mathbb{C}$ tais que:

$$Q(t) = a_n(t - z_2)(t - z_3) \cdots (t - z_n)$$

Substituindo essa expressão de volta na equação de $P(t)$:

$$P(t) = (t - z_1) \cdot [a_n(t - z_2) \cdots (t - z_n)]$$

Reorganizando os termos:

$$P(t) = a_n(t - z_1)(t - z_2) \cdots (t - z_n)$$

Isso conclui a indução e a prova do corolário. □

Referências Bibliográficas

[1] HEFEZ, Abramo. *Curso de Álgebra, vol. 1.* 3ª ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2002. (Coleção Matemática Universitária).

[2] MONTEIRO, L. H. Jacy. *Iniciação às Estruturas Algébricas.* 2ª ed. São Paulo: G. E. E. M., 1969. (Série Professor, n. 6).

[3] YARTEY, Joseph Nee Anyah. *Álgebra II.* Salvador: UFBA, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017.

[4] LIMA, Elon Lages. *Curso de Análise, Vol. 1.* 14ª ed. Rio de Janeiro: IMPA, 2017.

[5] DOMINGUES, Hygino H.; IEZZI, Gelson. *Álgebra Moderna.* 5ª ed. São Paulo: Saraiva Educação, 2018.

[6] JESUS, Ivanilton Sales de. *Isometrias no Plano – Uma abordagem aplicável ao ensino básico.* Salvador: UFBA, 2017. Dissertação (Mestrado Profissional em Matemática).

[7] MATTOS, Guylherme de Barros. *A Construção dos Números.* Volta Redonda: UFF, 2021. Trabalho de Conclusão de Curso (Bacharelado em Matemática).

[8] AMORIM, Artur Assis. *Teoria algébrica dos números aplicada a equações diofantinas não lineares.* Juiz de Fora: UFJF, 2022. Trabalho de Conclusão de Curso (Bacharelado em Matemática).

[9] SOUZA, Viviane de França. *Uma Abordagem de Grupos Cíclicos Finitos.* Arapiraca: UFAL, 2017. Trabalho de Conclusão de Curso (Licenciatura em Matemática).

[10] BRANDÃO, Huan Elvis Campelo. *Uma Demonstração Algébrica do Teorema Fundamental da Álgebra.* Araguaína: UFT, 2022. Trabalho de Conclusão de Curso (Licenciatura em Matemática).

[11] LIMA, Alexandre Mendonça. *Teorema Fundamental das Funções Simétricas.* Itabaiana: UFS, 2025. Trabalho de Conclusão de Curso (Licenciatura em Matemática).

[12] CASTRO, Danilo Elias. *Cálculo do Grupo de Galois.* São Paulo: IME-USP, 2007. Trabalho de Formatura Supervisionado (Bacharelado em Ciência da Computação).