UNIVERSIDADE FEDERAL DE ALFENAS

Mariana Gabriela Gusmão

# CÓDIGOS GEOMETRICAMENTE UNIFORMES SOBRE ANÉIS QUOCIENTE DE INTEIROS

ALFENAS-MG

2021

MARIANA GABRIELA GUSMÃO

# CÓDIGOS GEOMETRICAMENTE UNIFORMES SOBRE ANÉIS QUOCIENTES DE INTEIROS

**Trabalho de Conclusão de Curso submetido à Universidade Federal de Alfenas, como requisito necessário para obtenção do grau de Licenciada em Matemática**

ALFENAS-MG
2021

UNIVERSIDADE FEDERAL DE ALFENAS

MARIANA GABRIELA GUSMÃO

Esta Monografia foi julgada adequada para a obtenção do título de Licenciada em Matemática, sendo aprovada em sua forma final pela banca examinadora:

---

Orientador(a): Profª. Dra. Cátia Regina de Oliveira Quilles Queiroz
Universidade Federal de Alfenas - UNIFAL

---

Prof. Dr. Anderson José de Oliveira
Universidade Federal de Alfenas - UNIFAL

---

Prof. Dr. Marcelo Moreira da Silva
Universidade Federal de Alfenas - UNIFAL

---

Prof. Dr. Evandro Monteiro
Universidade Federal de Alfenas - UNIFAL

ALFENAS-MG
2021

# Agradecimentos

Acima de tudo agradeço a Deus, pela vida, pela conquista alcançada e por todas as vezes que acalmou meus pensamentos, meu coração e minha alma.

Agradeço à minha orientadora Cátia Regina Oliveira Quilles Queiroz por todo suporte, apoio e compreensão na produção deste trabalho. Você é uma mulher e profissional extraordinária, gratidão por tudo que fez por mim.

Aos meus pais Ana Maria e Marcus, que com muito trabalho e esforço permitiram que eu vivesse e me dedicasse tanto ao sonho de ser professora. Agradeço também aos meus irmãos Paloma e Lucas pelo companheirismo e por todas as vezes que me ajudaram nesses 4 anos de curso.

Ao meu namorado Guilherme, pelo amor e carinho que me confortaram nos dias difíceis e por ser tão presente em minha vida.

Aos meus amigos da vida Larissa, Isadora e Sérgio, que se mantiveram presentes em minha vida apesar da distância e de minha ausência em diversos momentos importantes em suas vidas. A minha prima Sara, pelo companheirismo e por todos momentos de descontração nos anos que vivemos juntas.

Aos grades amigos que esse curso meu deu, Amanda, Thales, Augusto, Edson e Mesek, obrigado por esses quatro anos de amizade e companheirismo, pelos longos dias de estudos, pelas trocas de ideias e ajuda mútua, pelas conversas e risadas no Hall do V e na escadinha do PCA, vocês são incríveis e amigos que desejo levar para a vida.

Aos professores do departamento de matemática que tanto contribuíram para minha formação. Em especial aos professores Anderson, Cátia, Claudinei, José Carlos, José Paulo, Marcelo e Rejane, vocês são exemplos de profissionais que, sem dúvidas, desejo seguir.

E a todos aqueles que, de alguma forma, contribuíram nesse ciclo da minha vida.

*"Presentemente eu posso me considerar um sujeito de sorte*
*Porque apesar de muito moço, me sinto são e salvo e forte*
*E tenho comigo pensado: Deus é brasileiro e anda do meu lado."*
*(Belchior)*

# Resumo

A Teoria dos Códigos Corretores de Erros tem como principal objetivo detectar e corrigir possíveis erros no processo de transmissão de uma mensagem, para que assim a mensagem possa chegar ao seu destino conforme foi enviada originalmente ou da forma mais confiável possível. No presente trabalho exploramos, por meio de um estudo teórico, os códigos geometricamente uniformes, mais especificamente as subclasses dos códigos perfeitos e quase perfeitos. Inicialmente nos atemos ao estudo de conceitos fundamentais da área de Álgebra, como grupos, subgrupos, anéis e anéis quocientes; sendo estes requisitos básicos para o estudo dos códigos corretores de erros, que foram estudados posteriormente e, finalmente analisamos e comparamos os ganhos obtidos com os códigos quase perfeitos em relação aos perfeitos. Esta classe de códigos possui propriedades muito interessantes e é capaz de corrigir mais erros que a classe de códigos perfeitos. Atualmente essa teoria está presente em pesquisas de diversas áreas, como Matemática, Estatística, Computação, Engenharia Elétrica e Biologia.

**Palavras-chave**: Álgebra. Grafos. Códigos Corretores de Erros.

# Abstract

The Error Correction Codes Theory has as main objective to detect and to correct possible transmission errors of a message, so that the message can reach its destination as it was originally sent. In this work we explore, through a theoretical study, the geometrically uniform codes, more specifically the subclasses of perfect and quasi perfect codes. Initially, we focus in the study of fundamental concepts of the Algebra area, such as groups, subgroups, rings and quotient rings; these being the basic requirements for the study of the error-correcting codes, which were studied later and, finally, we analyzed and compared the gains obtained with the quasi perfect codes in relation to the perfect ones. This class of codes has very interesting properties and is able to correct more errors than the class of perfect codes. Actually this theory is present in researches of several areas, such as Mathematics, Statistics, Computing, Electrical Engineering and Biology.

**Keywords**: Algebra. Graphs. Error-correcting Codes.

# Sumário

# 1 Introdução

Os códigos corretores de erros estão presentes de diversas formas em nosso cotidiano, contribuindo principalmente para o desenvolvimento tecnológico e garantindo a confiabilidade dos dados transmitidos digitalmente. Nessa teoria, pode-se ver como a matemática pura, especificamente a álgebra abstrata, se relaciona com problemas aplicados.

O estudo dos códigos corretores de erros teve sua origem na teoria da informação introduzida por Shannon em 1948 [1], com o artigo intitulado *"A Mathematical Theory of Communication"*, cujo principal objetivo é transmitir e armazenar dados de maneira confiável, de modo que ao recuperar uma informação, seja possível detectar e corrigir erros. Shannon ficou conhecido como "o pai da teoria da informação" com essa publicação. O trabalho inicial para a aquisição de bons códigos foi desenvolvido por um grupo restrito de matemáticos, pois exigia um profundo conhecimento de álgebra abstrata.

Dentre os diversos tipos de códigos sobre estruturas algébricas, temos os códigos de grupos. Slepian foi responsável por introduzir o conceito de códigos de grupos para o canal Gaussiano em 1968 [2], apresentando suas principais propriedades. Os códigos de grupos em $\mathbb{R}^n$ possuem todas as regiões de Voronoi, ou regiões de decisão, congruentes; todas as palavras-código têm a mesma probabilidade de erro e o perfil de distância é sempre o mesmo.

Em [3] Forney estuda uma classe de códigos intitulada "Códigos Geometricamente Uniformes", estes são mais gerais comparados aos códigos de Slepian e os códigos de treliça propostos por [4], pois é permitido que os elementos do grupo gerador sejam isometrias arbitrárias, em vez de apenas transformações ortogonais ou traduções, e o código pode ser definido como um conjunto de sequências possivelmente de dimensão infinita. Os códigos geometricamente uniformes apresentam uniformidade geométrica, que além de ser um tipo forte de simetria, permite outras qualidades, como regiões congruentes e grupo gerador isomorfo a um grupo de permutações transitivo.

Em 2007, a definição de novas métricas sobre espaços de sinais bidimensionais derivados da Teoria de Grafos sobre constelações em uma modelação QAM (Quadrature Amplitude Modulation) e de uma subclasse dos códigos geometricamente uniformes, chamada de códigos perfeitos, foi proposta por Martínez, C., Beivide, R., Gabidulin, E. em [5].

Uma generalização dos códigos perfeitos derivados de anéis quocientes de inteiros Gaussianos é realizada em [6] e de inteiros de Einsenstein-Jacobi em [7], essa generalização é intitulada de códigos quase perfeitos. Os códigos quase perfeitos, além de preservarem as propriedades dos códigos geometricamente uniformes, são capazes de corrigir mais padrões

de erro do que os códigos perfeitos.

Atualmente os códigos corretores de erros são amplamente utilizados em programas espaciais da NASA e do JPL (Jet Propulsion Laboraty), como na missão Galileo para Júpiter, na missão Cassini para Saturno e na missão Marte [8], bem como em aplicações mais próximas do cotidiano, como nos dígitos de controle presentes no CPF, nos cartões de crédito e na transmissão de dados via celular e internet [9].

Este trabalho tem como principal objetivo analisar os ganhos obtidos com códigos quase-perfeitos no processo de transmissão da informação em um sistema de comunicação frente aos códigos perfeitos. E para que se atinja este objetivo, o trabalho foi dividido em três capítulos, sendo o primeiro capítulo a presente introdução. O segundo capítulo, trata de uma revisão de conceitos algébricos necessários para o estudo dos códigos. Assim, na primeira seção definimos e apresentamos algumas propriedades de conteúdos como grupos, anéis, anéis quocientes, corpos e extensão de corpos, sendo [10], [11] e [12] as principais referências utilizadas nessa seção. Na segunda seção introduzimos conceitos básicos sobre grafos, as principais referências utilizadas são [13] e [14]. Por fim, na terceira seção, introduzimos o conceito de códigos corretores de erros, sendo [15] a principal referência utilizada.

No terceiro capítulo estudamos os códigos geometricamente uniformes no plano Euclidiano. Definimos o conceito de códigos perfeitos e quase perfeitos, e expusemos alguns exemplos destes. As principais referências utilizadas nesse capitulo são [6], [7] e [16].

Finalmente, no quarto capítulo, concluímos o trabalho, com uma avaliação dos resultados estudados e os ganhos obtidos para a vida acadêmica com a elaboração deste.

# 2 Revisão de Conceitos

Nesse capítulo veremos conceitos e resultados que darão embasamento ao estudo de códigos sobre anéis quocientes de inteiros, tais como teoria de grupos e anéis, anéis quocientes, extensão de corpos, norma e traço de um elemento, com ênfase nos Inteiros de Gauss e de Einsenstein-Jacobi e por fim alguns exemplos e teoremas importantes da teoria de grafos e de códigos corretores de erros.

## 2.1 Álgebra

Nesta seção, faremos uma revisão de estruturas algébricas, como grupos, anéis, anéis quocientes, extensão de corpos e a norma e traço de um elemento, além de apresentar os anéis de inteiros Gaussianos e de Einsenstein-Jacobi. As referencias utilizadas foram [10], [11] e [12].

### 2.1.1 Grupos

**Definição 1.** Um conjunto não vazio G munido de uma operação binária $(x, y) \mapsto x * y$ é chamado *grupo* se satisfaz as seguintes condições:

1. $(a * b) * c = a * (b * c), \forall\ a, b, c \in$ G; (associatividade)
2. Existe $e \in$ G tal que $a * e = e * a = a, \forall\ a \in$ G; (elemento neutro)
3. Para cada $a \in$ G, existe $a' \in$ G tal que $a * a' = a' * a = e$. (elemento simétrico)

**Observação 1.** Particularmente, quando a operação $*$ é a multiplicação, denotamos o simétrico de $a$ por $a^{-1}$ e o chamamos de inverso de $a$. Neste caso, o elemento neutro de $G$ é o 1, que é denotado por $1_G$, quando há risco de confusão. Agora, quando a operação $*$ é a adição, denotamos o simétrico de $a$ por $-a$ e o chamamos de oposto de $a$. Neste caso, o elemento neutro de $G$ é o 0, que é denotado por $0_G$, quando há risco de confusão.

**Definição 2.** Seja G um grupo em relação à operação $*$. Então G é chamado de *grupo comutativo*, ou um *grupo abeliano*, se $*$ é comutativa. Ou seja, $x * y = y * x,\ \forall\ x,\ y \in$ G.

**Propriedades de um grupo**
$G_1$) $\exists!\ e \in G$; (unicidade do elemento neutro)

*Demonstração:* Sejam $a \in G$ e $e, e'$ elementos neutros de G. Assim,

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

$$e' * a = a * e' = a.$$

Daí,

$$e = e * e' = e'.$$

□

$G_2$) $\exists!\ a^{-1}$, para cada $a \in G$; (unicidade do elemento simétrico)

*Demonstração:* Sejam $a \in G$ e $a', a''$ elementos simétricos de $a$. Assim,

$$a' * a = a * a' = e,$$

$$a'' * a = a * a'' = e.$$

Logo,

$$a' = e * a' = (a'' * a) * a' = a'' * (a * a') = a'' * e = a''.$$

□

$G_3$) $(a')' = a, \forall\ a \in G$;

*Demonstração:* Sejam $a \in G$, $a'$ o elemento simétrico de $a$ e $e \in G$ o elemento neutro de $G$.

$$(a')' = (a')' * e = (a')' * (a' * a) = ((a')' * a')a = e * a = a.$$

□

$G_4$) $(a * b)' = b' * a', \forall\ a, b \in G$;

*Demonstração:* Sejam $a, b \in G$.

$$\begin{aligned}
(a * b)' * (a * b) &= e \\
(a * b)' * (a * b) * b' &= e * b' \\
(a * b)' * a * (b * b') &= b' \\
(a * b)' * a * e &= b' \\
(a * b)' * a &= b' \\
(a * b)' * a * a' &= b' * a' \\
(a * b)' * e &= b' * a' \\
(a * b)' &= b' * a'
\end{aligned}$$

□

$G_5$) Se $a * x = a * y$, então $x = y$. O elemento $a$ é chamado de regular.

*Demonstração:* Sejam $a, x$ e $y \in G$. Suponhamos que $a * x = a * y$, logo

$$x = e * x = (a' * a) * x = a' * (a * x) = a' * (a * y) = (a' * a) * y = e * y = y.$$

□

### Classificação de um grupo

**Definição 3.** Se um grupo G tem um número finito de elementos, G é chamado de *grupo finito*. O número de elementos em G é chamado de ordem de G e é indicado por o(G) ou $|G|$. Se G não possui um número finito de elementos, G é chamado de *grupo infinito*.

### Alguns grupos importantes

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ são grupos abelianos.

  A adição é uma operação associativa e comutativa sobre $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$. O elemento neutro de todos esses grupos é 0, e o oposto $-a$ para cada $a \in \mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$.

- $(\mathbb{C}, +)$ é grupo comutativo. A soma de dois números complexos $z = a+bi$ e $w = c+di$ é dada por $z + w = (a + c) + (b + d)i$ e é associativa. O elemento neutro é $0 = 0 + 0i$. Por fim, para todo complexo $z = a + bi$, o número complexo $-z = (-a) + (-b)i$ é seu simétrico.

- $(\mathbb{Q}^*, \cdot)$ é grupo comutativo. O conjunto $\mathbb{Q}^*$ é fechado em relação à multiplicação, que é associativa em $\mathbb{Q}^*$, pois é no conjunto $\mathbb{Q}$. O elemento neutro dessa operação é 1. E para todo $a \in \mathbb{Q}^*$ existe o elemento oposto $a^{-1}$ em $\mathbb{Q}^*$.

- $(\mathbb{Z}_m, +)$ é um grupo comutativo para todo $m$, onde $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ é chamado conjunto das classes de resto módulo $m$. Portanto, $\overline{0}$ é formado por todos os inteiros côngruos a 0, módulo $m$, $\overline{1}$ por todos os inteiros côngruos a 1, módulo $m$, e assim por diante.

  A *adição módulo m* é uma operação em $\mathbb{Z}_m$ definida por

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

  a qual vale a associatividade e a comutatividade. Mais ainda, $\overline{0}$ é elemento neutro dessa operação, pois

  $$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}.$$

  E a classe $\overline{m - a}$ é o oposto de $\overline{a}$ em $\mathbb{Z}_m$ nesta operação, pois

  $$\overline{a} + \overline{m - a} = \overline{a + (m - a)} = \overline{m} = \overline{0}.$$

Então, $\overline{-a} = \overline{m-a}$.

A *multiplicação módulo m* em $\mathbb{Z}_m$ é uma operação definida por

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

Nessa operação também valem as propriedades associativa e comutativa. O elemento $\overline{1}$ é elemento neutro dessa operação, pois

$$\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a}.$$

Entretanto, o conjunto $\mathbb{Z}_m$ munido da operação "$\cdot$" é um grupo se, e somente se, $m$ é um número primo e o elemento $\overline{0}$ não pertence a $\mathbb{Z}_m$. Isso acontece pois nem todos os elementos de $\mathbb{Z}_m$ possuem inverso, como por exemplo o $\overline{0}$. A demonstração da existência do inverso de todos elementos apenas quando $m$ é primo pode ser verificada em [10].

- $(A, \sigma)$ é um grupo, onde $A = \{1, 2, ..., n\}$ e $\sigma$ é uma função bijetiva que leva $A$ em $A$, chamada *permutação de A*. Um grupo de permutações de um conjunto $A$ é um conjunto de permutações de $A$ que, com a composição, forma um grupo.

  Agora consideremos o conjunto $A = S_n$. Como existem $n!$ permutações de $n$ elementos e o conjunto das permutações de $n$ elementos está em bijeção com $S_n$, a ordem de $S_n$ é $|S_n| = n!$

  A aplicação bijetiva $\sigma : S_n \to S_n$, pode ser representada da forma matricial:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

  O elemento neutro de $S_n$ é $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.

  O elemento inverso de $\sigma \in S_n$ é $\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$.

  E a composição é feita da seguinte forma:

  Dado $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$, então

  $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix}$.

**Exemplo 1.** $(\mathbb{N}, +)$ não é grupo! Note que $3 \in \mathbb{N}$, mas não existe $a \in \mathbb{N}$ tal que $3 + a = 0$.

**Exemplo 2.** $(\mathbb{Z}_3, +)$ é um grupo finito e abeliano, pois a adição módulo $m$ é associativa e comutativa. O elemento neutro para esta operação é $\overline{0}$. Agora, o elemento simétrico:

- de $\overline{0}$ é o próprio $\overline{0}$, pois ele é o elemento neutro;
- de $\overline{1}$ é $\overline{2}$, pois $\overline{1} + \overline{2} = \overline{0}$. Como a operação é comutativa, segue que o simétrico de $\overline{2}$ é $\overline{1}$.

Portanto todos elementos possuem inverso, e conclui-se que $(\mathbb{Z}_3, +)$ é um grupo abeliano. Por fim, a ordem de $\mathbb{Z}_3$ é 3.

### Tábua de Cayley

**Definição 4.** As operações entre os elementos de um grupo finito podem ser representadas em uma tabela de operações conhecida como *Tábua de Cayley*, que é dada pelos elementos de $G$ da seguinte forma:

| $*$ | $\cdots$ | $b$ |
|---|---|---|
| $\vdots$ | $\ddots$ | |
| $a$ | | $a * b$ |

Denominaremos a primeira linha e a primeira coluna da Tábua de Cayley como linha fundamental e coluna fundamental, respectivamente.

**Observação 2.** A propriedade $G_5$ garante que não ocorrem repetições nos resultados das operações de uma mesma linha e nem de uma mesma coluna. De fato, suponha que exista $b_1 \neq b_2$ que quando operados com $a$ resultem num mesmo resultado:

| $*$ | $b_1$ | $b_2$ |
|---|---|---|
| $\vdots$ | $\ddots$ | |
| $a$ | $c$ | $c$ |

Então, $a * b_1 = a * b_2$ e assim, pelo fato de todo elemento de um grupo ser regular, $b_1 = b_2$, o que é um absurdo!

### Propriedades de uma operação quando esta é dada por meio de uma tábua.

**a) Associativa**

Calculam-se todos os compostos do tipo $a_i * (a_j * a_k)$, com $i, j, k \in \{1, 2, \ldots, n\}$; depois calculam-se todos os compostos do tipo $(a_i * a_j) * a_k$, com $i, j, k \in \{1, 2, \ldots, n\}$; e por fim comparam-se os compostos que têm os mesmos $i, j$ e $k$. Esse método de verificação requer o cálculo de $2n^3$ compostos.

**b) Comutativa**

Uma operação $*$ é comutativa se $a_i * a_j = a_j * a_i$, ou seja, $a_{ij} = a_{ji}$, $\forall\ i, j \in \{1, 2, 3, \ldots, n\}$. Podemos verificar essa propriedade observando a posição dos elementos $a_{ij}, a_{ji}$, destacada na tábua a seguir, em relação à diagonal principal. Se estes forem simétricos, a operação $*$ é comutativa.

| $*$ | $a_1$ | $a_2$ | $\cdots$ | $a_i$ | $\cdots$ | $a_j$ | $\cdots$ | $a_n$ |
|---|---|---|---|---|---|---|---|---|
| $a_1$ | $a_{11}$ | | | | | | | |
| $a_2$ | | $a_{22}$ | | | | | | |
| $\cdots$ | | | $\cdots$ | | | | | |
| $a_i$ | | | | $a_{ii}$ | | $a_{ij}$ | | |
| $\cdots$ | | | | | $\cdots$ | | | |
| $a_j$ | | | | $a_{ji}$ | | $a_{jj}$ | | |
| $\cdots$ | | | | | | | $\cdots$ | |
| $a_n$ | | | | | | | | $a_{nn}$ |

**c) Elemento neutro**

Sabemos, pela definição de *grupo*, que um elemento $e$ é neutro para a operação $*$ quando dado um elemento qualquer $a$, em um grupo $G$, $a * e = a = e * a$.

Da igualdade $e * a = a$, decorre que a linha de $e$ é igual à linha fundamental. E da igualdade $a * e = a$ decorre que a coluna de $e$ é igual à coluna fundamental. Assim, basta observar se existe algum elemento cuja linha e coluna são iguais à linha e coluna fundamentais da tábua para saber se uma operação tem elemento neutro.

| $*$ | $a_1$ | $a_2$ | $a_3$ | $\cdots$ | $e$ | $\cdots$ | $a_n$ |
|---|---|---|---|---|---|---|---|
| $a_1$ | | | | | $a_1$ | | |
| $a_2$ | | | | | $a_2$ | | |
| $a_3$ | | | | | $a_3$ | | |
| $\cdots$ | | | | | $\cdots$ | | |
| $e$ | $a_1$ | $a_2$ | $a_3$ | $\cdots$ | $e$ | $\cdots$ | $a_n$ |
| $\cdots$ | | | | | $\cdots$ | | |
| $a_n$ | | | | | $a_n$ | | |

**d) Elemento simétrico**

Sabemos que um elemento $a_i \in G$ possui simétrico quando existe $a_j \in G$ tal que $a_i * a_j = e = a_j * a_i$. A igualdade $a_i * a_j = e$ nos garante que a coluna de $a_i$ deve apresentar ao menos um composto igual a $e$. E $a_j * a_i = e$ garante que a linha de $a_i$ também deve apresentar um composto igual a $e$. Observe que $a_{ij} = a_{ji} = e$. Então, assim como no item **b)**, o elemento $e$ deve ficar em posições simétricas à diagonal principal.

**Exemplo 3.** Dado o grupo $(\mathbb{Z}_3, +)$, visto no Exemplo 2, observe a tábua de operações desse grupo:

| $*$ | $a_1$ | $a_2$ | $\cdots$ | $a_i$ | $\cdots$ | $a_j$ | $\cdots$ | $a_n$ |
|---|---|---|---|---|---|---|---|---|
| $a_1$ | | | | | | | | |
| $a_2$ | | | | | | | | |
| $\cdots$ | | | | | | | | |
| $a_i$ | | | | | | $e$ | | |
| $\cdots$ | | | | | | | | |
| $a_j$ | | | | $e$ | | | | |
| $\cdots$ | | | | | | | | |
| $a_n$ | | | | | | | | |

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{0}$ | $\overline{1}$ |

Tabela 1 – Tábua de operação do grupo $(\mathbb{Z}_3, +)$

### Subgrupos

**Definição 5.** Dado um grupo $(G, *)$, um subconjunto $H$ de $G$ é chamado de subgrupo de $G$ se $H$ for um grupo com relação à operação binária $*$ definida em $G$, ou seja:

- $H \neq \emptyset$;
- $\forall\ a, b \in H;\ a * b \in H$.

Se $e$ é elemento neutro de $G$, então $\{e\}$ é subgrupo de $G$. $G$ também é subgrupo de si mesmo. Esses subgrupos são chamados de subgrupos *triviais* de $G$.

**Teorema 2.1.1.** Um subconjunto $H$ do grupo $G$ é um subgrupo de $G$ se e somente se $H \neq \emptyset$ e $\forall\ a, b \in H$, tem-se que $a * b' \in H$.

*Demonstração:* ($\Rightarrow$) Suponhamos que $H$ é subgrupo de $G$.

- $e \in H$

  Sejam $e$ e $e_h$ elementos neutros de $G$ e $H$, respectivamente. Assim,

  $$e_h * e_h = e_h = e_h * e.$$

  Pela Propriedade $G_5$ (elemento regular), $e_h = e$.

- $b \in H \Rightarrow b' \in H$

  Dado $b \in H$, indiquemos por $b'$ e $b'_h$ seu elemento simétrico em $G$ e $H$, respectivamente. Assim,

  $$a'_h * a = e_h = e = a' * a.$$

Novamente pela propriedade $G_5$ de grupos, temos que $a'_h = a'$.

Visto isto, $H \neq \emptyset$, pois $e \in H$ e se $a \in H$ e $b' \in H$, então $a * b' \in$ H, pois H é fechado em relação à operação $*$.

($\Leftarrow$) Suponhamos agora que $H \neq \emptyset$ e $a * b' \in H$. Da segunda hipótese, se $b = a$ então $a * a' = e \in H$. Tomemos $x \in H$, se $e \in H$ e $x \in H$ então $e * x' = x' \in H$. Assim, $H$ tem elemento inverso.

Mostremos agora que $H$ é fechado. Se $a, b \in H$, como $H$ contém inversos, $b' \in H$. Agora, se $a, b' \in H$ então $a * (b')' = a * b \in H$, também pela condição de $H$ possuir inversos. Portanto $H$ é fechado.

Por último, devemos mostrar que vale a associatividade em $H$. Como $H$ é subconjunto de $G$, se $a, b, c \in H$ então $a, b, c \in G$ e, portanto, $a * (b * c) = (a * b) * c$, visto que a associatividade vale em $G$.

Portanto, $H$ é subgrupo de $G$. □

**Exemplo 4.** O conjunto $H = \{x \in \mathbb{R}^* | x > 0\}$ é um subgrupo de $(\mathbb{R}^*, \cdot)$. Pois, se $a$, $b \in H$, então $a$, $b \in \mathbb{R}$ tal que $a > 0$ e $b > 0$. Mais ainda, se $b > 0$ então $b^{-1} > 0$, assim $ab^{-1} > 0$ e, portanto, $ab^{-1} \in H$.

### Homomorfismo e isomorfismo de grupos

**Definição 6.** Seja $G$ um grupo com relação à operação $*$, e $J$ um grupo com relação à operação $\circledast$. Um *homomorfismo* de $G$ em $J$ é uma aplicação $\phi : G \to J$, tal que, $\forall\ a, b \in G$

$$\phi(a * b) = \phi(a) \circledast \phi(b).$$

Se um homomorfismo é uma aplicação injetora, é chamado de *monomorfismo*. Se for uma aplicação sobrejetora, é chamado de *epimorfismo*. Quando $\phi$ é bijetora, denominamos de *isomorfismo*, conceito que será definido posteriormente de forma mais detalhada.

**Exemplo 5.** Sejam os grupos $(\mathbb{Z}, +)$, $(\mathbb{C}^*, \cdot)$. A aplicação $\phi : \mathbb{Z} \to \mathbb{C}^*$ definida por $\phi(a) = i^a$, é um homomorfismo de grupos pois,

$$\phi(a + b) = i^{a+b} = i^a \cdot i^b = \phi(a) \cdot \phi(b).$$

**Exemplo 6.** Dados dois grupos $G$ e $G'$ quaisquer, e $e'$ elemento neutro de $G'$. Vamos definir a aplicação $\phi : G \to G'$, tal que $\phi(a) = e'$, para todo $a \in G$. Assim, $\forall\ a, b \in G$,

$$\phi(a) \cdot \phi(b) = e' \cdot e' = e' = \phi(ab),$$

logo $\phi$ é um homomorfismo de $G$ em $G'$. Se $|G'| > 1$, essa aplicação não é um epimorfismo nem um monomorfismo, pois para todo $a, b \in G$, tal que $a \neq b$, temos que $\phi(a) = \phi(b) = e'$.

**Exemplo 7.** Dados um inteiro $m > 1$, os grupos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_m, \cdot)$ e a aplicação $\psi : \mathbb{Z} \to \mathbb{Z}_m$ definida por $\psi(a) = \overline{a}$. $\psi$ é um homomorfismo sobrejetor de grupos, pois $\psi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \psi(a) + \psi(b)$ e se $\overline{y} \in \mathbb{Z}_m$, então $\overline{y} = \overline{a}$, para algum $\overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$, portanto $\phi(a) = \overline{a} = \overline{y}$.

### Propriedades dos homomorfismos

Sejam $G$ um grupo com relação à operação $*$ e $J$ um grupo com relação à operação $\circledast$, cujos elementos neutros são $e$ e $u$, respectivamente, e $\phi : G \to J$ é um homomorfismo de grupos.

**Teorema 2.1.2.** Seja $\phi$ um homomorfismo do grupo $G$ para o grupo $J$, então

1. $\phi(e) = u$;
2. $\phi(a') = [\phi(a)]'$, $\forall\ a \in G$.

*Demonstração:* 1. Para todo $a \in$ G, temos $a * e = a$, logo

$$\begin{aligned} \phi(a * e) &= \phi(a) \\ \phi(a) \circledast \phi(e) &= \phi(a) \\ \phi(a) \circledast \phi(e) &= \phi(a) \circledast u \\ \phi(e) &= u, \end{aligned}$$

pelo fato dos elementos de um grupo serem regulares.

2. Temos $\phi(e) = u$, para todo $a \in$ G, tem-se:

$$\begin{aligned} \phi(a * a') &= u \\ \phi(a) \circledast \phi(a') &= u \\ \phi(a) \circledast \phi(a') &= \phi(a) \circledast [\phi(a)]' \\ \phi(a') &= [\phi(a)]', \end{aligned}$$

pelo fato dos elementos de um grupo serem regulares.

□

**Teorema 2.1.3.** Se $H$ é um subgrupo de $G$, então $\phi(H)$ é subgrupo de $J$.

*Demonstração:* Temos que $\phi(H) = \{\phi(a) : a \in H\}$.

i. É fácil ver que $\phi(H) \neq \emptyset$, pois se $H$ é subgrupo de $G$, $e \in H \to \phi(e) = u \to u \in \phi(H)$.

ii. $\forall\ c \in \phi(H)$, existe $a \in H$ tal que $\phi(a) = c$. Visto isto, se $\phi(a') = [\phi(a)]' = c'$, então $c' \in \phi(H)$, pois $a' \in H$.

iii. $\forall\ c, d \in \phi(H)$, existem $a, b \in H$ tais que $\phi(a) = c$ e $\phi(b) = d$. Assim, $\phi(a * b) = \phi(a) \circledast \phi(b) = c \circledast d$. Como $a * b \in H \to c \circledast d \in \phi(H)$.

Portanto, $\phi(H)$ é subgrupo de $J$. □

**Teorema 2.1.4.** Dados os grupos $(G, *), (J, \circledast)$ e $(L, \boxdot)$. Se $\phi : G \to J$ e $\psi : J \to L$ são homomorfismos de grupos, então $\psi \circ \phi : G \to L$ também é um homomorfismo de grupo.

*Demonstração:* $\forall\ a, b \in G$, temos

$$(\psi \circ \phi)(a * b) = \psi(\phi(a * b)) = \psi(\phi(a) \circledast \phi(b)) = \psi(\phi(a)) \boxdot \psi(\phi(b)) = (\psi \circ \phi)(a) \boxdot (\psi \circ \phi)(b).$$

□

**Definição 7.** Seja $\phi : G \to J$ um homomorfismo de grupos. O *núcleo de* $\phi$ é o subconjunto de $G$ denotado por $Ker(\phi)$, tal que

$$Ker(\phi) = \{a \in G : \phi(a) = u\},$$

onde $u$ é elemento neutro de $J$.

Notação: $N(\phi)$, $Ker(\phi)$.

**Exemplo 8.** Sejam $(\mathbb{Z}, +), (\mathbb{C}^*, \cdot)$ e $\phi :\ \mathbb{Z} \to \mathbb{C}^*$ um homomorfismo de grupos definido por $\phi(a) = i^a$. Para encontrar o núcleo de $\phi$, basta encontrar o conjunto solução da equação $i^a = 1$, pois 1 é elemento neutro de $(\mathbb{C}^*, \cdot)$.

$$\begin{array}{lllll} i^0 = 1 & i^4 = 1 & i^8 = 1 & i^{10} = 1 & \cdots \\ i^1 = i & i^5 = i & i^9 = i & i^{11} = i & \cdots \\ i^2 = -1 & i^6 = -1 & \cdots & \cdots & \cdots \\ i^3 = -i & i^7 = -i & \cdots & \cdots & \cdots \end{array}$$

Observe que $i^a = 1$ quando $a$ é múltiplo de 4. Sendo assim, o núcleo de $\phi$, é:

$$Ker(\phi) = \{0, \pm 4, \pm 8, ...\}.$$

**Teorema 2.1.5.** Seja $\phi :\ G \to J$ um homomorfismo de grupos. Então

1. $Ker(\phi)$ é um subgrupo de $G$;
2. $\phi$ é um homomorfismo injetor se, e somente se, $Ker(\phi) = \{e\}$.

*Demonstração:* 1. É fácil ver que $Ker(\phi) \neq \emptyset$, se $\phi(e) = u$ então $e \in ker(\phi)$. Mais ainda, se existem elementos distintos $a$ e $b\ \in ker(\phi)$, então $\phi(a) = \phi(b) = u$ e, portanto

$$\phi(ab') = \phi(a)\phi(b') = \phi(a)[\phi(b)]' = uu' = u,$$

assim, $ab' \in Ker(\phi)$. De acordo com o Teorema 2.1.1, $Ker(\phi)$ é subgrupo de $G$.

2. ($\Rightarrow$) Dado um elemento qualquer $a \in Ker(\phi)$ temos que $\phi(a) = u$. Sabemos que $\phi(e) = u$, logo $\phi(a) = u = \phi(e)$. Como, por hipótese, $\phi$ é injetor, conclui-se que $a = e$. Portanto, $ker(\phi) = \{e\}$.

   ($\Leftarrow$) Suponhamos que $ker(\phi) = \{e\}$, então

$$\phi(a) = \phi(b)$$

$$\phi(a)[\phi(b)]' = \phi(b)[\phi(b)]'$$

$$\phi(a)[\phi(b)]' = u.$$

   Pelo Teorema 2.1.2 e por $\phi$ ser um homomorfismo, temos que

$$\phi(ab') = u.$$

   Portanto, $ab' \in ker(\phi) = \{e\}$. Então, $ab' = e \Rightarrow a = b$, consequentemente, $\phi$ é injetora.

□

**Definição 8.** Seja $\phi : G \to J$ um homomorfismo de grupos. Se $\phi$ for também uma bijeção, então $\phi$ é um *isomorfismo* de grupos, dizemos que $G$ e $J$ são isomorfos e escrevemos $G \simeq J$. No caso em que $G = J$, $\phi$ é um isomorfismo de $G$.

Notação: $G \simeq J$.

**Exemplo 9.** Os grupos $(\mathbb{R}, +)$ e $(\mathbb{R}^+, \cdot)$ são isomorfos. De fato, a aplicação $\phi : \mathbb{R} \to \mathbb{R}^+$ definida por $\phi(a) = e^a$ é um isomorfismo.

- $\phi$ é um homomorfismo, pois $\phi(a + b) = e^{a+b} = e^a \cdot e^b = \phi(a) \cdot \phi(b)$.
- Devemos mostrar que $\phi$ é bijetiva. De fato, $\phi$ é injetora, pois $\phi(a) = \phi(b) \Rightarrow a = b$. $\phi$ é sobrejetora, pois dado $c \in \mathbb{R}^+$ podemos definir $a = \ln c$, e então $\phi(a) = e^a = e^{\ln c} = c$.

**Exemplo 10.** Dado o grupo $(\mathbb{R}^+, +)$, a aplicação $\phi : \mathbb{R}^+ \to \mathbb{R}^+$ definida por $\phi(a) = a^3$ não é um isomorfismo, por mais que seja uma aplicação bijetiva, pois existem $x, y \in \mathbb{R}^+$ tais que $(x + y)^3 \neq x^3 + y^3$.

**Teorema 2.1.6.** Se $\phi : G \to J$ é um isomorfismo de grupos, então $\phi' : J \to G$ também é um isomorfismo de grupos.

*Demonstração:* Sabemos que, se $\phi$ é uma aplicação bijetiva, então $\phi'$ também é bijetiva. Portanto, neste caso, devemos apenas mostrar que $\phi'$ é um homomorfismo, ou seja, conserva as operações.

Sejam $y_1$ e $y_2 \in J$, $y_1 = \phi(x_1)$ e $y_2 = \phi(x_2)$, onde $x_1$, $x_2 \in G$. Isso é possível pois $\phi$ é sobrejetora. Visto isso, $\phi'(y_1) = \phi'(\phi(x_1)) = x_1$ e, analogamente, $\phi'(y_2) = x_2$. Assim,

$$\phi'(y_1y_2) = \phi'(\phi(x_1)\phi(x_2)) = \phi'(\phi(x_1x_2)) = x_1x_2 = \phi'(y_1)\phi'(y_2).$$

□

**Grupos Cíclicos**

Antes de introduzirmos o conceito de Grupos Cíclicos é importante definir que se $a \in G$ e $m \in \mathbb{Z}$, a potencia $m$-ésima de $a$ é o elemento de $G$ denotado por $a^m$ e definido da seguinte forma:

- Se $m \geq 0$, por recorrência,

$$\begin{aligned} a^0 &= e \qquad \text{(elemento neutro de } G\text{)} \\ a^m &= a^{m-1} \cdot a, \qquad \text{se } m \geq 1 \end{aligned}$$

- Se $m < 0$,

$$a^m = (a^{-m})^{-1}$$

Observe que com essa definição obtemos que $e^m = e$, para todo $m \in \mathbb{Z}$. Além disso, se tomarmos $m, n \in \mathbb{Z}$ e $a \in G$, valem as igualdades a seguir para qualquer operação:

- $a^m \cdot a^n = a^{m+n}$;
- $a^{-m} = (a^m)^{-1}$;
- $(a^m)^n = a^{m \cdot n}$

As demonstrações dessas igualdades podem ser verificadas em [10].

Se $a$ é um elemento do grupo multiplicativo $(G, \cdot)$, $[a]$ é subconjunto de $G$ formado pelas potências inteiras de $a$, isto é, $[a] = \{a^m | \, m \in \mathbb{Z}\}$. Mais ainda, $G \neq \emptyset$, pois $e = a^0$.

Note que, se usarmos a notação aditiva, o subgrupo gerado por $a$ será: $[a] = \{m \cdot a | \, m \in \mathbb{Z}\}$.

**Definição 9.** Um grupo $G$ é chamado *grupo cíclico* se $G = [a]$ para algum $a \in G$. O elemento $a$ é chamado gerador do grupo $G$.

**Teorema 2.1.7.** Dados $(G, \cdot)$ e $a \in G$, temos que o subconjunto $[a]$ é um subgrupo de $G$, chamado *subgrupo cíclico* gerado por $a$.

*Demonstração:* $[a] \neq \emptyset$, pois o elemento neutro $e$ de $G$, pertence à $[a]$, uma vez que $e = a^0$. Agora, dados elementos distintos $u, v \in [a]$, $u = a^m$ e $v = a^n$, com $m, n \in \mathbb{Z}$. Assim,

$$uv' = a^m(a^n)' = a^m a^{n'} = a^{m-n},$$

logo $uv' \in [a]$.

Portanto, $[a]$ é subgrupo de G. □

**Observação 3.** Se $H$ é subgrupo de $G$ e $a \in H$, então $[a] \subset H$. De fato, se $a \in H$, então toda potência de $a$ pertence a $H$, logo $[a] \subset H$. Podemos dizer que $[a]$ é o menor subgrupo de $G$ que inclui $a$.

**Exemplo 11.** O subgrupo gerado por $i$ em $(\mathbb{C}^*, \cdot)$ é dado por $[i] = \{i^m | m \in \mathbb{Z}\}$. Sabemos que esse conjunto possui apenas os elementos 1, $i$, -1, $-i$, que podem ser obtidos pelas potências $m = 4k$, $m = 4k + 1$, $m = 4k + 2$ e $m = 4k + 3$, onde $k \in \mathbb{N}$. Portanto $[i] = \{1, i, -1, -i\}$. Observe a tábua de operações desse grupo:

| $\cdot$ | 1 | -1 | $i$ | $-i$ |
|---|---|---|---|---|
| 1 | 1 | -1 | $i$ | $-i$ |
| -1 | -1 | 1 | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | -1 | 1 |
| $-i$ | $-i$ | $i$ | 1 | -1 |

**Exemplo 12.** O grupo aditivo $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$ é um grupo cíclico gerado por $\overline{1}$, pois todo elemento $\overline{k} \in \mathbb{Z}_n$ pode ser escrito por

$$\overline{k} = k\overline{1},$$

onde $k\overline{1}$ é um múltiplo de $\overline{1}$.

Elementos diferentes de $\overline{1}$ também podem ser geradores de $\mathbb{Z}_n$. Observe o caso particular a seguir:

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

O elemento $\overline{5}$ é um gerador de $\mathbb{Z}_6$, visto que $\overline{5}$ é elemento simétrico de $\overline{1}$, e

$$\begin{aligned}
1 \cdot \overline{5} &= \overline{5} \\
2 \cdot \overline{5} &= \overline{5} + \overline{5} = \overline{4} \\
3 \cdot \overline{5} &= \overline{5} + \overline{5} + \overline{5} = \overline{3} \\
4 \cdot \overline{5} &= \overline{2} \\
5 \cdot \overline{5} &= \overline{1} \\
6 \cdot \overline{5} &= \overline{0}.
\end{aligned}$$

**Exemplo 13.** Dado $(\mathbb{Z}_4, +)$, observe que:

$[\overline{0}] = \{\overline{0}\}$

$[\overline{1}] = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4$.

$[\overline{2}] = \{\overline{0}, \overline{2}\}$

$[\overline{3}] = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4$

Portanto, $\mathbb{Z}_4$ é cíclico, gerado por $\overline{1}$ ou $\overline{3}$.

**Teorema 2.1.8.** Um subgrupo de um grupo cíclico é cíclico.

*Demonstração:* $H$ é um subgrupo do grupo cíclico $G = [a]$ e $H \neq \{e\}$, pois já se sabe que $\{e\}$ é cíclico gerado por $a^0 = e$, e qualquer potência de $e$ é igual a $e$. Então $H$ contém $a^m$, $m \neq 0$. Mas, como $(a^m)^{-1} = a^{-m} \in H$, então $H$ possui um elemento de expoente estritamente positivo.

Seja $k$ o menor inteiro positivo tal que $a^k \in H$. Como $H$ é fechado e contém inversos, e $a^k \in H$, todas as potências $(a^k)^t = a^{kt}$ pertencem a $H$. Vamos mostrar que todo elemento em $H$ é uma potência de $a^k$. Tomemos $a^n \in H$. Logo, existem inteiros $q$ e $r$ tais que

$$n = kq + r \quad \text{com } 0 \leq r < k.$$

Assim, $a^{-kq} = (a^k)^{-q} \in H$ e $a^n \in H$ implica que

$$a^n \cdot a^{-kq} = a^{kq+r} \cdot a^{-kq} = a^r$$

também pertence à $H$. Agora, como $0 \leq r < k$ e $k$ é o menor inteiro positivo tal que $a^k \in H$, $r$ deve ser 0 pois se $r > 0$ teríamos um elemento em $H$ de expoente positivo e menor que k, o que não é possível. Assim, $a^n = a^{kq}$ e, portanto, $H = [a^k]$. □

**Exemplo 14.** Dado o Teorema 2.1.8, podemos garantir que um subconjunto não vazio $H \subset \mathbb{Z}$ é um subgrupo de $(\mathbb{Z}, +)$ se, e somente se, $H = [m]$, para algum inteiro $m \in H$. Observe os subgrupos de $\mathbb{Z}$:

$$[0] = \{0\}, [1] = \mathbb{Z}, [2] = [-2] = \{0, \pm 2, \pm 4, ...\}, [3] = [-3] = \{0, \pm 3, \pm 6, ...\}, \text{etc.}$$

**Classificação de grupos cíclicos**

Seja $G = [a]$ um grupo cíclico. Dois casos podem ocorrer:

**Caso 1:** $a^r \neq a^s$ sempre que $r \neq s$.

Observe o subgrupo $G = [2]$ no grupo multiplicativo $\mathbb{Q}^*$, $G = [2] = \{..., 2^{-2}, 2^{-1}, 2^0 = 1, 2^1, 2^2, ...\}$. Temos a seguinte aplicação de $\mathbb{Z}$ em $G$:

No caso geral de um grupo cíclico $G = [a]$, ela é definida por $r \to a^r$. Denotaremos essa aplicação por $\phi$. Portanto, $\phi : \mathbb{Z} \to \mathbb{G} = [a]$ é a aplicação definida por $\phi(r) = a^r$.

$$\begin{array}{ccccccccccc} ... & \text{-2}, & \text{-1}, & & 0, & & 1, & 2, & ..., & r, & ... \\ & \downarrow & \downarrow & & \downarrow & & \downarrow & \downarrow & & \downarrow & \\ ... & 2^{-2}, & 2^{-1}, & 2^0 & = & 1, & 2^1, & 2^2, & ..., & 2^r, & ... \end{array}$$

**Teorema 2.1.9.** Se $G = [a]$ é um grupo cíclico que satisfaz a condição do caso 1, então a aplicação $\phi : \mathbb{Z} \to G = [a]$ definida por $\phi(r) = a^r$ é um isomorfismo de grupos.

*Demonstração:* A aplicação $\phi$ é injetora, de fato, se tomarmos $\phi(r) \neq \phi(s)$, temos que $a^r \neq a^s$, pelo Caso 1 da classificação de grupos cíclicos, temos que $r \neq s$. A aplicação $\phi$ é sobrejetora, pois todo $y \in G$ pode ser escrito como $y = a^r$, para algum inteiro $r$, ou seja, $\phi(r) = a^r = y$. E, por fim, $\phi$ é um homomorfismo do grupo aditivo $\mathbb{Z}$ no grupo $G$, pois

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

Portanto, $\phi$ é um isomorfismo de grupos. □

**Observação 4.** Como $\phi$ é bijetora, os conjuntos $\mathbb{Z}$ e $G$ têm a mesma cardinalidade, ou seja, G é infinito. Por essa razão os grupos que se enquadram no Caso 1 são chamados *grupos cíclicos infinitos*. Mais ainda, o fato de $\phi$ ser um isomorfismo leva à conclusão de que todos os grupos cíclicos infinitos são cópias do grupo aditivo $\mathbb{Z}$.

**Caso 2:** $a^r = a^s$, para algum par de inteiros distintos, $r$ e $s$.

Suponhamos $r > s$. Então $a^r(a^s)^{-1} = a^s(a^s)^{-1} = e$, logo $a^{r-s} = e$, em que $r - s > 0$. Com isso, podemos ver que há potências de $a$, com expoentes estritamente positivos, iguais ao elemento neutro $e$. Assim, vamos tomar $h$ o menor inteiro positivo tal que $a^h = e$. Inicialmente mostraremos que os elementos

$$a^0 = e, a^1 = a, a^2, ..., a^{h-1}$$

são todos distintos. De fato, suponhamos $a^i = a^j$, com $0 \leq i < j < h$. Então $0 < j - i < h$ e $a^{j-i} = a^j(a^i)^{-1} = e$, o que é um absurdo, visto que $h$ é o menor inteiro positivo tal que $a^h = e$.
Agora, devemos mostrar que qualquer potência de $a$ é igual a um dos elementos, $a^0 = e, a, a^2, ..., a^{h-1}$. Seja $a^m$ um elemento arbitrário. Pelo algoritmo da divisão, existem inteiros $q$ e $r$ tais que

$$m = hq + r \quad (0 \leq r < h).$$

Assim,

$$\begin{aligned} a^m &= a^{hq+r} \\ &= (a^h)^q a^r \\ &= e^q a^r \\ &= ea^r \\ &= a^r, \end{aligned}$$

onde $r$ está no conjunto $\{0, 1, 2, ..., h-1\}$. Portanto, $[a] = \{a^0 = e, a^1 = a, a^2, ..., a^{h-1}\}$ e a ordem desse grupo é $h$. As afirmações anteriores demonstram o seguinte teorema.

**Teorema 2.1.10.** Seja $G = [a]$ um grupo cíclico que cumpre as condições do Caso 2. Então existe um inteiro $h > 0$ tal que:

1. $a^h = e$
2. $a^r \neq e$, $0 < r < h$.

Neste caso, a ordem do grupo é $h$ e

$$G = [a] = \{e, a, a^2, ..., a^{h-1}\}.$$

**Definição 10.** A ordem de um elemento $a$ de um grupo $G$, denotada por $o(a)$ ou $|a|$, é um inteiro $h > 0$ se:

1. $a^h = e$;
2. $a^r \neq e$, $\forall\ r$ tal que $0 < r < h$.

A ordem de $a$ é a ordem do subgrupo gerado por $a$. Isto é, $o(a) = o([a])$.

O grupo do Teorema 2.1.10 é chamado *grupo cíclico finito*, e o expoente $h$ de ordem de $a$. Se, para qualquer inteiro $r \neq 0$, $a^r \neq e$, então se diz que a ordem de $a$ é zero. Mais ainda, se $|a| = 0$ então ele gera um subgrupo cíclico infinito. De fato, não se pode ter $m \neq n$ e $a^m = a^n$, pois, suponhamos que $m > n$, então $a^{m-n} = e$, o que é absurdo, pois $m \neq n$.

**Exemplo 15.** Observe o grupo

$$G = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\} \ \subseteq \mathbb{Z}_{16},$$

com respeito à multiplicação em $\mathbb{Z}_{16}$. O elemento $\overline{5} \in G$ gera um subgrupo cíclico de ordem 4, pois $\overline{5}^4 = \overline{1}$, e 4 é o menor inteiro positivo $m$ tal que $\overline{5}^m = \overline{1}$. Então

$$[\overline{5}] = \{\overline{5}^0, \overline{5}^1, \overline{5}^2, \overline{5}^3\} = \{\overline{1}, \overline{5}, \overline{9}, \overline{13}\},$$

e a ordem do elemento $\overline{5}$ é 4.

**Exemplo 16.** A ordem de 1 no grupo multiplicativo de $\mathbb{C}$ é 1, pois $1^1 = 1$, a ordem de -1 é 2, pois $(-1)^1 = -1$ e $(-1)^2 = 1$, a ordem de $i$ e $-i$ é 4, pois $i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ e $(-i)^0 = 1, (-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$, respectivamente.

O elemento $2i \in (\mathbb{C}^*, \cdot)$, tem ordem zero, uma vez que $(2i)^n = 2^n i^n = 1 \Leftrightarrow n = 0$.

**Teorema 2.1.11.** Seja $a$ um elemento de ordem $h > 0$ de um grupo $G$. Então $a^m = e$, se, e somente se, $h \mid m$.

*Demonstração:* ($\Rightarrow$) Pelo algoritmo da divisão, existem inteiros $q$ e $r$ tais que

$$m = hq + r \quad (0 \leq r < h).$$

Assim,

$$\begin{aligned} e &= a^m \\ &= a^{hq+r} \\ &= (a^h)^q a^r \\ &= e^q a^r \\ &= ea^r \\ &= a^r. \end{aligned}$$

Ou seja, $a^r = e$. Como não se pode ter $r > 0$, pois contraria a hipótese de que a ordem de $a$ é $h$, então $r = 0$. Portanto, $m = hq$, ou seja, $h \mid m$.

($\Leftarrow$) Se $h \mid m$, então $m = hq$, para algum $q \in \mathbb{Z}$. Então,

$$a^m = a^{hq} = (a^h)^q = e^q = e.$$

□

**Teorema 2.1.12.** Seja $G = [a]$ um grupo cíclico finito de ordem $h$. Então a correspondência $\overline{s} \to a^s$ é uma aplicação de $\mathbb{Z}_h$ em $G$. Essa aplicação é um isomorfismo do grupo $(\mathbb{Z}_h, +)$ no grupo $(G, \cdot)$.

*Demonstração:* (i) Uma aplicação de $\mathbb{Z}_h$ em $G$ é uma lei que associa a todo elemento do conjunto $\mathbb{Z}_h$, um único elemento do conjunto $G$. Suponhamos que $\overline{r} = \overline{t}$. Então, $r - t = hq$, para algum $q \in \mathbb{Z}$. Assim, temos

$$a^r = a^{t+hq} = a^t(a^h)^q = a^t e^q = a^t e = a^t.$$

Portanto, se $\overline{r} = \overline{t}$, então $a^r = a^t$.

(ii) Seja $\phi : \mathbb{Z}_h \to G$ definida por $\phi(\overline{r}) = a^r$. Primeiro, vamos mostrar que $\phi$ é injetora. De fato, se $a^r = a^s$, então $a^{r-s} = e$ e então, devido ao Teorema 2.1.12, $r - s = hq$, para algum $q \in \mathbb{Z}$. Daí $r \equiv s (\text{mod } h)$ e, portanto, $\overline{r} = \overline{s}$. A aplicação $\phi$ é sobrejetora, pois dado $y \in G$ temos que $y = a^r$ para algum inteiro $r$ tal que $0 \leq r < h$. De onde, $\overline{r} \in \mathbb{Z}_h$ e

$$\phi(\overline{r}) = a^r = y.$$

Por fim, sejam $\overline{r}$, $\overline{s} \in \mathbb{Z}_h$. Então:

$$\phi(\overline{r}+\overline{s}) = \phi(\overline{r+s}) = a^{r+s} = a^r a^s = \phi(\overline{r})\phi(\overline{s})$$

e, portanto, $\phi$ é um isomorfismo de grupos. □

**Classes Laterais e Teorema de Lagrange**

Seja $(G, *)$ um grupo e $H$ um subgrupo de $G$. Se a ordem de $G$ é finita, a ordem de $H$ também é finita e, pelo Teorema de Lagrange veremos que $|H|$ divide $|G|$. Para isso, vamos definir uma relação de equivalência em $G$ de forma que possamos visualizar o grupo por meio de suas classes de equivalência.

**Definição 11.** Seja $H$ um subgrupo do grupo $(G, *)$. Dados $a, b \in H$, para quaisquer elementos $a, b \in H$:

$$a \equiv b \ (mod\, H) \text{ se, e somente se, } a' * b \in H.$$

Neste caso, dizemos que $a$ é congruente a $b$ módulo $H$, caso contrário dizemos que $a$ não é congruente a $b$ módulo $H$ e denotamos $a \not\equiv b \ (mod\, H)$.

**Exemplo 17.** Seja $H$ um subgrupo do grupo $(G, \cdot)$. Dados $a, b \in H$, Para quaisquer elementos $a, b \in H$:

$$a \equiv b \ (mod\, H) \ \Leftrightarrow \ a^{-1}b \in H.$$

**Exemplo 18.** Seja $H = n\mathbb{Z}$ um subgrupo do grupo $(\mathbb{Z}, +)$, com $n > 1$. Para quaisquer $a, b \in \mathbb{Z}$, temos que:

$$a \equiv b \ (mod\, n\mathbb{Z}) \ \Leftrightarrow \ a - b \in n\mathbb{Z} \Leftrightarrow n|(a-b) \Leftrightarrow a \equiv b \ (mod\, n).$$

Assim, temos que a congruência $mod\, n\mathbb{Z}$ é a congruência $mod\, n$.

**Teorema 2.1.13.** Seja $H$ um subgrupo arbitrário de $(G,*)$.

1. A relação $\equiv$ sobre $G$ definida por "$a \equiv b$ se, e somente se, $a' * b \in H$" é uma relação de equivalência;
2. Se $a \in G$, então a classe de equivalência determinada por $a$ é o conjunto $a * H = \{a * h |\ h \in H\}$.

*Demonstração:* 1. Para provar que essa relação é de equivalência, devemos mostrar que ela é reflexiva, simétrica e transitiva.

Reflexiva: $e = a' * a$ e $e \in H$, então $a \equiv a$ e, portanto vale a reflexividade.

Simétrica: Suponha que $a \equiv b$. Então $a' * b \in H$, mas como $H$ é um subgrupo de $G$, então $(a' * b)' = b' * a \ \in H$, e $b \equiv a$. Logo, vale a simetria.

Transitiva: Suponha que $a \equiv b$ e $b \equiv c$. Então $a' * b \in H$ e $b' * c \in H$. Mas, como $H$ é um subgrupo de $G$, $(a' * b)(b' * c) = a' * c \ \in H$, e $a \equiv c$. Logo, vale a transitividade.

2. Suponha que $\overline{a}$ é a classe de equivalência do elemento $a$. Se $x \in \overline{a}$ então $x \equiv a$, ou seja, $x' * a \in H$. Portanto, $x' * a = h$, para algum $h \in H$, ou seja, $x = a * h'$. Portanto, $x \in a * H$, visto que $h' \in H$. Agora, se $x \in a * H$, então $x = a * h$, para algum $h \in H$. Daí, $x' * a = h' \in H$ e, portanto, $x \equiv a$ e $x \in \overline{a}$.

□

O conjunto quociente de $G$ pela relação $\equiv$, denotado por $G/H$, é o conjunto das classes laterais $a * H$, com $a \in G$. Um dos elementos desse conjunto é o próprio $H$, pois $H = e * H$.

**Definição 12.** Para cada $a \in G$, a classe de equivalência $aH$ definida pela relação $\equiv$ introduzida no Teorema 2.1.13 é chamada *classe lateral à direita*, módulo H, determinada por $a$.

**Observação 5.** Uma decorrência imediata do Teorema 2.1.13 é que o conjunto das classes laterais à direita, módulo $H$, determina uma partição em $G$, ou seja:

1. Se $a \in G$, então $a * H \neq \emptyset$;

2. Se $a, b \in G$, então $a * H = b * H$ ou $a * H \cap b * H = \emptyset$;

3. A união de todas as classes laterais é igual a $G$.

De maneira análoga se demonstra que a relação $\equiv$ definida por "$a \equiv b$ se, e somente se, $a * b' \in H$" também é uma relação de equivalência sobre $G$. Neste caso, a classe de equivalência de um elemento $a \in G$ é o subconjunto $H * a = \{h * a |\ h \in H\}$, chamado *classe lateral à esquerda*, módulo $H$, determinada por $a$.

**Observação 6.** Se $G$ for um grupo comutativo, então as classes laterais são iguais, ou seja, $a * H = H * a$, para qualquer $a \in G$.

**Observação 7.** Se $H$ é um subgrupo de um grupo multiplicativo $G$, então as classes laterais à direita, módulo $H$, são os conjuntos $aH$, com $a \in G$, e se $H$ é um subgrupo de um grupo aditivo $G$, então as classes laterais à direita, módulo $H$, são os conjuntos $a + H$, com $a \in G$.

**Exemplo 19.** Considere o subgrupo $H = \{1, -1\}$ do grupo multiplicativo $G = \{1, -1, i, -i\}$. As classes laterais neste caso são:

$$\begin{aligned} 1H &= \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\}, \\ (-1)H &= \{(-1) \cdot 1, (-1) \cdot (-1)\} = \{-1, 1\}, \\ iH &= \{i, -i\}, \\ (-i)H &= \{-i, i\}. \end{aligned}$$

Observe que $1H \cup iH = G$. Portanto, $G/H = \{1H, iH\}$.

**Exemplo 20.** Considere o subgrupo $H = \{\overline{0}, \overline{3}\}$ do grupo aditivo $\mathbb{Z}_6$, logo:

$$\begin{aligned} \overline{0} + H &= \{\overline{0}, \overline{3}\}, \\ \overline{1} + H &= \{\overline{1}, \overline{4}\}, \\ \overline{2} + H &= \{\overline{2}, \overline{5}\}. \end{aligned}$$

No item 2) da Observação 5 vimos que as classes laterais são disjuntas e no item 3) que a união de todas as classes é igual a G. Com isso, não existem mais classes distintas das obtidas anteriormente, visto que a união destas é igual a $\mathbb{Z}_6$. Portanto, $G/H = \{H, \overline{1} + H, \overline{2} + H\}$.

**Teorema 2.1.14.** Seja $H$ um subgrupo de $G$. Então duas classes laterais quaisquer módulo $H$ são subconjuntos de $G$ que têm a mesma cardinalidade.

*Demonstração.* Dadas duas classes laterais $aH$ e $bH$ e a aplicação $\varphi : aH \to bH$ dada por $\varphi(ah) = bh$. Vamos mostrar que que $\varphi$ é bijetora:

- $\varphi$ é injetora: De fato, dados $h, h_1 \in H$. Seja $\varphi(ah) = \varphi(ah_1)$, então $bh = bh_1$; como todo elemento de $G$ é regular, temos que: $h = h_1$.
- $\varphi$ é sobrejetora: Seja $y \in bH$. Então $y = bh$, para algum $h \in H$. Tomando $x = ah \in aH$, então $\varphi(x) = \varphi(ah) = bh = y$.

Portanto, $\varphi$ é bijetora $\Rightarrow |aH| = |bH|$. □

**Definição 13.** Seja $H$ um subgrupo de $G$. O número de elementos distintos de $G/H$ é chamado *índice de* $H$ em $G$ e é denotado por $(G : H)$.

**Observação 8.** Como $a * H \to H * a'$ é uma aplicação bijetora, então o índice de $H$ em $G$ é o mesmo, quer se considere as classes laterais à direita ou à esquerda, módulo $H$.

**Exemplo 21.** Nos Exemplos 19 e 20 o índice de $H$ em $G$ é $(G : H) = 2$ e $(G : H) = 3$, respectivamente.

**Teorema 2.1.15.** *(Teorema de Lagrange)* Seja $H$ um subgrupo de um grupo finito $G$. Então $|G| = |H|(G : H)$ e, portanto, $|H| \mid |G|$.

*Demonstração.* Suponhamos que $(G : H) = r$ e o conjunto de todas as classes laterais à esquerda é dado por $G/H = \{a_1H, a_2H, ..., a_rH\}$. Sabemos que $G = a_1H \cup a_2H \cup ... \cup a_iH$ e que $a_rH \cap a_jH = \emptyset$, $i \neq j$. Segundo o Teorema 2.1.14, todas as classes têm a mesma cardinalidade de $H$, ou seja, as ordens são iguais a $|H|$. Portanto:

$$|G| = |H| + |H| + ... + |H|,$$

em que o número de parcelas é $r = (G : H)$. Assim,

$$|G| = (G : H)|H|$$

e $|h| \mid |G|$. □

**Corolário 2.1.16.** Seja $G$ um grupo finito. Então a ordem de um elemento $a \in G$ divide a ordem de $G$ e o quociente é $(G : H)$, em que $H = [a]$.

*Demonstração.* Sabemos que a ordem de $a$ é igual a ordem de $[a]$. Daí, pelo Teorema de Lagrange, temos que:

$$|G| = (G : H)|[a]|.$$

□

**Corolário 2.1.17.** Se $a$ é um elemento de um grupo finito $G$, então $a^{|G|} = e$.

*Demonstração.* Seja $h$ a ordem de $a$, ou seja, $a^h = e$ e $a^k \neq e$, $0 < k < h$. Pelo Corolário 2.1.16 temos que:

$$|G| = (G : H)|[a]|$$

$$|G| = (G : H)h,$$

em que $H = [a]$. Portanto:

$$a^{|G|} = a^{(G:H)h} = (a^h)^{(G:H)} = e^{(G:H)} = e.$$

□

**Corolário 2.1.18.** Todo grupo finito de ordem prima é cíclico.

*Demonstração.* Seja $p$ um primo e $G$ um grupo, tal que $|G| = p$. Então $G$ contém mais de um elemento, pois $p > 1$. Seja $a \in G$ tal que $a \neq e$ (elemento neutro de G). Então $[a]$ contém mais de um elemento. Como $[a]$ é subgrupo de $G$, pelo Teorema de Lagrange, $|[a]| \mid p$, uma vez que $|[a]| > 1$ e $|[a]| \mid p$, $|[a]| = p = |G|$. Portanto, $G = [a]$. □

**Observação 9.** Os únicos subgrupos do grupo G apresentado anteriormente são os subgrupos triviais, $\{e\}$ e $G$. Quando $|[a]| = 1 \Rightarrow [a] = \{e\}$, quando $|[a]| = p \Rightarrow [a] = G$.

$$\sigma_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\}, \qquad \sigma_4 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\},$$

$$\sigma_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}, \quad \sigma_5 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

$$\sigma_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}, \quad \sigma_6 = S_3.$$

**Exemplo 22.** O Teorema de Lagrange é de grande valia se quisermos encontrar os subgrupos de um grupo finito. Observe os subgrupos de $S_3$.

Os subgrupos de $S_3$ devem ter ordem 1, 2, 3 ou 6. Não é necessário escrever todos os subgrupos como feito anteriormente, pois isso é garantido pelo Teorema de Lagrange. Os de ordem 1 e 6 são os triviais. E os de ordem 2 e 3 são cíclicos, pelo Corolário 2.1.18.

**Exemplo 23.** Observe o subconjunto $\sigma$ do grupo $S_4$, dado por:

$$\sigma = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}.$$

O número de elementos de $\sigma$ é 2 e de $S_4$ é 24. Temos que 2 divide 24, mas $\sigma$ não é subgrupo de $S_4$, uma vez que

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \notin \sigma.$$

Portanto, não vale a recíproca do Teorema de Lagrange.

### Subgrupos Normais

**Definição 14.** Um subgrupo $N$ de um grupo $G$ é um subgrupo *normal* (ou invariante) se $aN = Na$ para todo $a \in G$.

Notação: $N \triangleleft G$.

Se $N$ é subgrupo normal de $G$ indicamos por $G/N$ o conjunto das clases laterais à esquerda, ou à direita, módulo $N$ em $G$. Se $G$ é abeliano, então obviamente todo subgrupo de $G$ é normal.

**Exemplo 24.** Analisando o Exemplo 22, $\sigma_5$, é um subgrupo normal de $S_3$. Mas, observe que o subgrupo $H = \sigma_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$ do grupo $S_3$ não é um subgrupo normal. De fato, se tomarmos $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, temos que:

$$aH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

e,

$$Ha = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Assim, $aH \neq Ha$ e, portanto, $H$ não é subgrupo normal em $S_3$.

**Teorema 2.1.19.** Seja $N$ um subgrupo normal do grupo $G$. Então, $(aN)(bN) = (ab)N$ para quaisquer $a,\ b \in G$.

*Demonstração.* ($\subset$) Seja $x \in (aN)(bN)$, então $x = uv$, tal que $u \in (aN)$ e $v \in (bN)$. Podemos escrever $u = an_1$ e $v = bn_2$, com $n_1, n_2 \in N$. Assim, $x = (an_1)(bn_2) = a(n_1b)n_2$, mas como $n_1b \in Nb = bN$, existe $n \in N$ tal que $n_1b = bn$. Daí, $x = a(n_1b)n_2 = a(bn)n_2 = (ab)(nn_2)$, $nn_2 \in N$, portanto $x \in (ab)N$. Ou seja, $(aN)(bN) \subset (ab)N$.

($\supset$) Seja $x \in (ab)N$, então $x = (ab)n$ para algum $n \in N$. Podemos reescrever $x$ da seguinte forma, $x = a(bn) \Rightarrow x = (ae)(bn)$, como $e$, elemento neutro, pertence a $N$, temos que $ae \in aN$. Agora, como $bn \in N$, $x = (ae)(bn) \in (aN)(bN)$. Ou seja, $(aN)(bN) \supset (ab)N$.

Portanto, $(aN)(bN) = (ab)N$.

□

**Grupos Quocientes**

Seja $N$ um subgrupo normal de $G$. Temos que

- $(aN)(bN) = (ab)N$, para todo $a, b \in G$;
- $[(aN)(bN)](cN) = (aN)[(bN)(cN)]$, para todo $a, b, c \in G$;
- Para todo $a \in G$, temos que $(aN)(eN) = (ae)N = aN = (ea)N = (eN)(aN)$;
- Para todo $a \in G$, temos que $(aN)(a^{-1}N) = (aa^{-1})N = eN = N$.

**Definição 15.** Seja $G$ um grupo e $N$ um subgrupo normal de $G$. Nas condições anteriores, o grupo quociente de $G$ por $N$ é o par formado pelo conjunto quociente $G/N$.

**Exemplo 25.** Sejam $G = \{1, -1, i, -i\}$ o grupo multiplicativo das raízes quárticas da unidade e $N = \{1, -1\}$. Como $G$ é abeliano, $N$ é subgrupo normal de $G$. Então $G/N = \{N, iN\}$.

**Exemplo 26.** Sejam $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e $H = \{\overline{0}, \overline{3}\}$. O Grupo quociente é $G/H = \{H, \overline{1} + H, \overline{2} + H\}$.

**Teorema 2.1.20.** Se $N$ é um subgrupo normal de $G$, então a aplicação $\mu : G \to G/N$ definida por $\mu(a) = aN$, é um homomorfismo sobrejetor de grupos cujo núcleo é $N$.

*Demonstração.* Primeiro verificaremos que a aplicação $\mu$ é um homomorfismo. De fato,

$$\mu(ab) = (ab)N = (aN)(bN) = \mu(a)\mu(b).$$

Agora, verificaremos que a aplicação é sobrejetora. Se $y \in G/N$, então $y = aN$, para algum $a \in G$. Como $\mu(a) = aN = y$, $\mu$ é uma aplicação sobrejetora.

O núcleo de $\mu$ é $N$. De fato, temos que o elemento neutro do grupo quociente é a classe $N$. Agora, se $a \in Ker(\mu)$, então $\mu(a) = aN = N$. Como, porém, $a \in aN$, pois $a = ae$ e $e \in N$. Logo, $Ker(\mu) \subset N$. Por outro lado, se $a \in N$, então $aN = N$, e $\mu(a) = aN = N$, portanto $a \in Ker(\mu)$. Logo, $Ker(\mu) \supset N$. Portanto, $Ker(\mu) = N$. □

O homomorfismo $\mu : G \to G/N$ definida acima por $\mu(a) = aN$ é chamado homomorfismo canônico de $G$ sobre $G/N$.

**Teorema do Homomorfismo**

O Teorema do Isomorfismo é um dos resultados mais importantes da teoria de grupos. E para demonstrá-lo é necessário o seguinte lema.

**Lema 2.1.21.** Se $\phi : G \to L$ é um homomorfismo de grupos, então $N = Ker(\phi)$ é um subgrupo normal de $G$ e, portanto, $G/N$ tem uma estrutura de grupo.

*Demonstração.* Provaremos que $N = Ker(\phi)$ é um subgrupo normal de $G$.

($\subset$) Se $x \in aN$, então $x = an$, para algum $n \in N$. Temos que $\phi(ana^{-1}) = \phi(a)\phi(n)\phi(a^{-1}) = \phi(a)e\phi(a)^{-1} = u$, elemento neutro de L. Portanto, $ana^{-1} \in N = Ker(\phi)$. Agora, como $x = an = (ana^{-1})a$, então $x \in Na$. Logo, $aN \subset Na$.

($\supset$) A demonstração de $aN \supset Na$ é análoga.

Portanto, $aN = Na$, ou seja, $N = Ker(\phi)$ é um subgrupo normal de $G$. □

**Teorema 2.1.22.** (Teorema do Isomorfismo) Seja $\phi : G \to L$ um homomorfismo sobrejetor de grupos. Se $N = Ker(\phi)$, então $G/N \simeq L$.

*Demonstração.* Observe que a correspondência $aN \to \phi(a)$ de $G/N$ em $L$ é uma aplicação. De fato, suponhamos que $aN = bN$, então $b^{-1}a \in N$ e, portanto, $\phi(b^{-1}a) = u$, elemento neutro de $L$. Mas $\phi(b^{-1}a) = \phi(b^{-1})\phi(a) = [\phi(b)]^{-1}\phi(a)$. Assim, temos que $[\phi(b)]^{-1}\phi(a) =$

$u \Leftrightarrow \phi(a) = \phi(b)u = \phi(b)$. Portanto $aN \to \phi(a)$ é uma aplicação. Agora, dada a aplicação $\sigma : G/N \to L$, definida por $\sigma(aN) = \phi(a)$, vamos mostrar que $\sigma$ é uma aplicação injetora. Suponhamos que $\phi(a) = \phi(b)$, $a, b \in G$. Então $[\phi(b)]^{-1}\phi(a) = [\phi(b)]^{-1}\phi(b) = u$. Como $\phi$ é um homomorfismo de grupos, temos que $[\phi(b)]^{-1}\phi(a) = u \Leftrightarrow \phi(b^{-1}a) = u$. Logo, $b^{-1}a \in N$ e, portanto, $aN = bN$.

Agora, devemos mostrar que $\sigma$ é um isomorfismo. Primeiro é preciso ver que $\sigma$ é sobrejetora. De fato, se $y \in L$, então $y = \phi(a)$, $a \in G$. Tomando $x = aN \in G/N$. Temos que $\sigma(x) = \sigma(aN) = \phi(a) = y$.

Por último, mostremos que $\sigma$ é um homomorfismo de grupos. De fato,

$$\sigma[(aN)(bN)] = \sigma[(ab)N] = \phi(ab) = \phi(a)\phi(b) = \sigma(aN)\sigma(bN).$$

Portanto, $\sigma$ é um isomorfismo de grupos.

□

### 2.1.2 Anéis e Corpos

**Definição 16.** Um conjunto não vazio $A$, juntamente com duas operações binárias $*$ e $\circledast$, é dito ser um *anel* se:

1. $(A, *)$ é um grupo abeliano;
2. A segunda operação é associativa, isto é: se $a, b, c \in A$, então $a \circledast (b \circledast c) = (a \circledast b) \circledast c$;
3. Valem as leis distributivas: se $a, b, c \in A$, então $a \circledast (b * c) = (a \circledast b) * (a \circledast c)$ e $(a * b) \circledast c = (a \circledast c) * (b \circledast c)$.

Notação: $(A, *, \circledast)$.

Dado o anel $(A, *, \circledast)$, como $(A, *)$ é um grupo abeliano, o anel possui a mesma propriedade que esse grupo em relação à primeira operação.

Um anel $(A, *, \circledast)$ em que o conjunto $A$ é finito, chama-se *anel finito*. Se $A$ é um anel finito, as tábuas da adição e da multiplicação são úteis para visualizar algumas de suas características.

**Alguns anéis importantes**

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são anéis numéricos. Estes são os anéis mais importantes, e estão munidos das operações usuais. Em cada caso, a operação $\cdot$ é comutativa e 1 é o elemento neutro para esta operação.

- $(\mathbb{Z}_m, +, \cdot)$ é um anel, chamado anel das classes de resto módulo $m$. Para todo inteiro $m > 1$, é dado pelo conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ em relação as seguintes operações:

$$\overline{a} + \overline{b} = \overline{a+b} \quad e \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$

  (i) Temos que $(\mathbb{Z}_m, +)$ é um grupo abeliano, conforme vimos na Subseção 2.1.1.

  (ii) A multiplicação é associativa. De fato, se $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, então $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{abc} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

  (iii) A multiplicação é distributiva em relação à adição. De fato, se $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, então $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b+c} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac}$. A distributiva à direita é análoga.

  Portanto, $(\mathbb{Z}_m, +, \cdot)$ é um anel. O zero desse anel é a classe $\overline{0}$ e o oposto de um elemento $\overline{a} \in \mathbb{Z}_m$ é a classe $\overline{m-a}$.

**Exemplo 27.** Vamos construir as tábuas do anel $(\mathbb{Z}_4, +, \cdot)$:

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{0}$ | $\overline{2}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Observe a tábua da multiplicação, temos que esse anel não é regular na respectiva operação e tem divisor de zero. Por exemplo:

$\overline{2} \cdot \overline{2} = \overline{0}$ (zero do anel), mas nenhum dos fatores é igual a $\overline{0}$;

$\overline{2} \cdot \overline{1} = \overline{2} \cdot \overline{3}$, mas $\overline{1} \neq \overline{3}$.

### Subanéis

**Definição 17.** Um subconjunto não vazio $S$ de um anel $(A, *, \circledast)$ é um *subanel* de $A$ se, $S$ é um anel com as operações induzidas de $A$.

Considerando-se as operações usuais sobre os conjuntos numéricos: $\mathbb{Z}$ é subanel de $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{Q}$ é subanel de $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{R}$ é subanel de $\mathbb{C}$.

**Teorema 2.1.23.** Sejam $(A, +, \cdot)$ um anel e $S$ um subconjunto não vazio de $A$. Então $S$ é um subanel de $A$ se, e somente se, para todo $a, b \in S$, $a - b = a + (-b) \in S$ e $a \cdot b \in S$.

*Demonstração.* ($\Rightarrow$) Se $S$ é subanel de $A$, então para todo $a, b \in S$, temos que $-b \in S$ e $a \in S$. Logo $a - b \in S$, pois $S$ é fechada para a operação $+$ e, $a \cdot b \in S$, pois $\cdot$ é uma operação em $S$.

($\Leftarrow$) Temos, por hipótese, que sempre que $a, b \in S$, $a - b \in S$. Logo, pelo Teorema 2.1.1, $S$ é um subgrupo aditivo de $A$. Agora, como $S$ é fechado em relação à operação $\cdot$, temos que:

- Se $a, b \in S$, então $a, b \in A$. Assim, por $A$ ser anel, $a + b = b + a$.
- Se $a, b, c \in S$, então $a, b, c \in A$ e, portanto, $a(bc) = (ab)c$. Portanto, a multiplicação é associativa em $S$.
- Se $a, b, c \in S$, então $a, b, c \in A$ e, portanto, $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$. Portanto, a multiplicação é distributiva em relação à adição em $S$.

□

**Exemplo 28.** Dado o conjunto $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Temos que $S_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $S_2 = \{\overline{0}, \overline{3}\}$ são subanéis de $\mathbb{Z}_6$, pois $\overline{2} \cdot \overline{4} = \overline{2}$, $-\overline{2} = \overline{4}$; $\overline{3} = -\overline{3}$, $\overline{3} \cdot \overline{3} = \overline{3}$.

Observe que $1_{\mathbb{Z}_6} = \overline{1}$, $1_{S_1} = \overline{4}$ e $1_{S_2} = \overline{3}$. Assim, para $i = 1, 2$, $S_i \subset \mathbb{Z}_6$ são subanéis com 1 tais que $1_{S_i} \neq 1_{\mathbb{Z}_6}$.

**Exemplo 29.** Seja $L = \{a + b\sqrt{2} |\ a, b \in \mathbb{Z}\}$, $L$ é um subanel de $\mathbb{R}$, pois, se $a + b\sqrt{2}$, $c + d\sqrt{2} \in L$, então:

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \ \in L;$$

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

O subanel $L = \{a + b\sqrt{2} |\ a, b \in \mathbb{Z}\}$ de $\mathbb{R}$ é usualmente denotado por $\mathbb{Z}[\sqrt{2}]$.

Dado $S$ um subconjunto não vazio de $\mathbb{Z}$. Então $S$ é subanel de $\mathbb{Z}$ (operações usuais) se, e somente se, $S$ é um subgrupo aditivo de $\mathbb{Z}$. De fato, pela definição de subanel temos que se $S$ é subanel de $\mathbb{Z}$, então $S$ é subgrupo de $\mathbb{Z}$. A volta é recíproca, $S$ é subgrupo cíclico do grupo aditivo $\mathbb{Z}$, pois $\mathbb{Z}$ é um grupo aditivo cíclico. Então $S = [a] = \{0, \pm a, \pm 2a, ...\}$, com $a \in S$. Agora, se $b, c \in S$, então $b = ax$ e $c = ay$, $x, y \in \mathbb{Z}$ e, portanto, $b - c = (x - y)a \in S$ e $bc = (axy)a \in S$. Pelo Teorema 2.1.23, $S$ é subanel de $\mathbb{Z}$.

### Anéis comutativos

**Definição 18.** Um anel $(A, *, \circledast)$ onde a operação $\circledast$ é comutativa, é chamado *anel comutativo*. Um anel $(A, *, \circledast)$ onde a operação
*circledast* tem elemento neutro é chamado *anel com unidade* ou simplesmente, *anel com 1*.

Um anel que possui unidade e cuja multiplicação é comutativa é denominado *anel comutativo com unidade*.

**Exemplo 30.** Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são bons exemplos de anéis comutativos com unidade. Os anéis $\mathbb{Z}_m$ das classes de resto, módulo $m$, também são anéis comutativos com unidade, pois o resto da divisão de $ab$ por $m$ é igual ao resto da divisão de $ba$ por $m$, e a unidade é a classe $\overline{1}$, pois $\overline{a} \cdot \overline{1} = \overline{a} = \overline{1} \cdot \overline{a}$, com $\overline{a}, \overline{b} \in \mathbb{Z}_m$.

Seja $A$ um anel com unidade e $L$ um subanel de $A$. As seguintes situações podem ocorrer:

- $L$ possui unidade e esta é a mesma de $A$. Nesse caso diz-se que $L$ é um subanel unitário de $A$;
- $L$ não possui unidade, mesmo $A$ sendo um anel com unidade;
- $L$ e $A$ são anéis com unidade, mas as unidades são diferentes;
- Nem $L$ nem $A$ possuem unidade;
- $A$ não é um anel com unidade, mas $L$ possui unidade.

### Anéis de integridade

Um elemento $a \in A$, $a \neq 0$ é um *divisor de zero à esquerda* se existe $b \neq 0$ em $A$, tal que $a \circledast b = 0$. Analogamente $a \neq 0$ é um *divisor de zero à direita* se existe $b \neq 0$ tal que $b \circledast a = 0$.

**Definição 19.** Um anel $(A, *, \circledast)$ comutativo com unidade é um *domínio*, ou um *anel de integridade*, se, e somente se, para todo $a, b \in \mathbb{R}$, $a \circledast b = 0 \Rightarrow a = 0$ ou $b = 0$.

Também podemos definir um *domínio*, ou um *anel de integridade* se este for um anel comutativo com unidade que não possui divisores de zero.

Todos os anéis numéricos, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, são anéis de integridade (ou domínios). Já os anéis $\mathbb{Z}_m$ das classes de resto, módulo $m$, não são domínios se $m > 1$ é um inteiro composto, pois sempre teremos divisores de zero no anel. De fato, neste caso é possível encontrar inteiros $a$ e $b$ tais que $0 < a$, $b < m$ e $m = ab$. Portanto, $\overline{a}$, $\overline{b} \in \mathbb{Z}_m$, $\overline{a}, \overline{b} \neq \overline{0}$ e $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$. Mas e no caso em que $m$ é um número primo?

**Teorema 2.1.24.** Um anel de classes de restos $\mathbb{Z}_m$ é um anel de integridade se, e somente se, $m$ é um número primo.

*Demonstração.* ($\Rightarrow$) Vamos provar por contrapositiva, ou seja, se $m$ é composto $\Rightarrow \mathbb{Z}_m$ não é um anel de integridade. Suponhamos que $m$ é um número composto, então $\mathbb{Z}_m$ possui divisores de zero, como dito anteriormente. E isso é um absurdo, pois por definição um anel de integridade é um anel comutativo com unidade e sem divisores de zero.

($\Leftarrow$) Temos que $\mathbb{Z}_m$ é um anel comutativo com unidade, para todo $m > 1$. Suponhamos que $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{0}$, para algum par de elementos $\overline{a}, \overline{b} \in \mathbb{Z}_m$. Daí, $ab = mq$ (com $q \in \mathbb{Z}$) e, portanto, $m|ab$. Mas, como $m$ é primo, por hipótese, então $m|a$ ou $m|b$. Porém, assim temos que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Ou seja, se $m$ é primo, então $\mathbb{Z}_m$ não possui divisores de zero. Portanto, por definição, $\mathbb{Z}_m$ é um anel de integridade. □

### Corpos

**Definição 20.** Se $\mathbb{K}$ é um anel comutativo com unidade e todo elemento não nulo de $\mathbb{K}$ é inversível, então $\mathbb{K}$ é chamado *corpo*.

Os anéis numéricos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, são corpos. Mas o anel $\mathbb{Z}$ não é um corpo, pois os elementos 1 e -1 são os únicos inversíveis, contrariando a definição. O anel $\mathbb{Z}_m$, com $m$ primo, também é um corpo.

**Observação 10.** Se o corpo $\mathbb{F}$ possuir número finito de elementos, dizemos que ele é um corpo finito, denotado por $\mathbb{F}_q$, onde $q$ é a quantidade de elementos do corpo.

**Teorema 2.1.25.** Todo corpo é um anel de integridade.

*Demonstração.* Temos por definição que um corpo é um anel comutativo com unidade, portanto basta mostrar que vale a lei do cancelamento do produto. De fato, sejam $\mathbb{K}$ um corpo e $a, b \in \mathbb{K}$ tais que $ab = 0$. Suponhamos que $a \neq 0$ e que $a$ é inversível. Multiplicando a igualdade $ab = 0$ por $a^{-1}$, obtemos:

$$a^{-1} \cdot (ab) = a^{-1} \cdot 0 = 0.$$

Mas, como $a^{-1} \cdot (ab) = b$, então $b = 0$. De maneira análoga mostra-se que, se $b \neq 0$, então $a = 0$. Logo, a multiplicação de dois elementos de $\mathbb{K}$ é nula apenas se um dos elementos é nulo. Portanto $\mathbb{K}$ é um anel de integridade. □

A recíproca do teorema acima é verdadeira quando o anel de integridade é finito!

**Definição 21.** Seja $(\mathbb{L}, *, \circledast)$ um corpo. Um subconjunto $\mathbb{K}$ de $\mathbb{L}$ é chamado *subcorpo* de $\mathbb{L}$ se é fechado para as duas operações de $\mathbb{L}$ e se $\mathbb{K}$ também tem uma estrutura de corpo (para as operações induzidas em $\mathbb{L}$).

**Exemplo 31.** $\mathbb{Q}$ é subcorpo de $\mathbb{R}$, e $\mathbb{R}$ é subcorpo de $\mathbb{C}$.

### Homomorfismos e isomorfismos de anéis

**Definição 22.** Dados $(A, *, \circledast)$ e $(B, \oplus, \odot)$ anéis, uma aplicação $\phi : A \to B$ será denominada *homomorfismo de anéis*, se para todo $a, b \in A$:

$$\phi(a * b) = \phi(a) \oplus \phi(b), \qquad (\phi \text{ é um homomorfismo de grupos})$$

$$\phi(a \circledast b) = \phi(a) \odot \phi(b).$$

Quando $\phi$ é uma bijeção, chamamos isomorfismo de $A$ em $B$. Neste caso, dizemos que os anéis $A$ e $B$ são isomorfos e denotamos por $A \cong B$. Dois anéis são considerados idênticos se forem isomorfos, ou seja, existe entre eles um isomorfismo. O isomorfismo $\phi : A \to A$ é chamado automorfismo.

**Exemplo 32.** Dado os anéis $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$ e $m > 1$, seja $\phi_m : \mathbb{Z} \to \mathbb{Z}_m$, definida por $\phi_m(a) = \overline{a}$, para cada $a \in \mathbb{Z}$. $\phi_m$ é um homomorfismo de anéis. De fato, para todo $a, b \in \mathbb{Z}$,

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

$$\phi_m(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \phi_m(a) \cdot \phi_m(b).$$

Observe que, $\phi_m$ é um homomorfismo sobrejetor, pois todo $x \in \mathbb{Z}_m$ é uma classe $x = \overline{a}$, que vem de $a \in \mathbb{Z}$ através de $\phi_m$. Mas $\phi_m$ não é um homomorfismo injetor, pois $\phi_m(a) = \phi_m(a + m)$, para todo $a \in \mathbb{Z}$.

**Teorema 2.1.26.** Dado os anéis $(A, +, \cdot)$ e $(B, \oplus, \odot)$. Se $\phi : A \to B$ é um homomorfismo de anéis, então:

1. $\phi(0_A) = 0_B$;
2. $\phi(-a) = -\phi(a)$;
3. $\phi(a - b) = \phi(a) - \phi(b)$;
4. Se $A$ tem $1_A$, então $\phi(1_A) = 1_{\phi(A)}$;
5. Se $a \in A$ é inversível, então $\phi(a)$ também é, e $[\phi(a)]^{-1} = \phi(a^{-1})$.

*Demonstração.* 1. Temos que

$$\phi(0_A) \oplus 0_B = \phi(0_A) \text{ e } \phi(0_A) = \phi(0_A + 0_A) = \phi(0_A) \oplus \phi(0_A).$$

Assim, pela lei do cancelamento, segue que $0_B = \phi(0_A)$.

2. Temos que

$$0_B = \phi(0_A) = \phi(a + (-a)) = \phi(a) \oplus \phi(-a),$$

para todo $a \in A$. Daí, $\phi(-a) = -\phi(a)$.

3. $\phi(a - b) = \phi(a + (-b)) = \phi(a) \oplus \phi(-b) = \phi(a) - \phi(b)$.

4. Para todo $\phi(a) \in \phi(A)$,

$$\phi(a) \odot \phi(1_A) = \phi(a \cdot 1_A) = \phi(a) = \phi(1_A \cdot a) = \phi(1_A) \odot \phi(a) \Longrightarrow \phi(1_a) = 1_{\phi(A)}.$$

5. Se $a \in A$ é inversível, então

$$\phi(a) \odot \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(1_A) = 1_B,$$

e de modo análogo

$$\phi(a^{-1}) \odot \phi(a) = \phi(a^{-1} \cdot a) = \phi(1_A) = 1_B.$$

Portanto, $\phi(a^{-1}) = [\phi(a)]^{-1}$.

□

**Teorema 2.1.27.** Se $\varphi : A \to B$ é um homomorfismo de anéis e $S$ é um subanel de A, então $\varphi(S)$ é um subanel de $B$.

*Demonstração.* De fato, $\varphi(S) \neq \emptyset$, pois como $\varphi^{-1}(0_B) = 0_A \in S \Rightarrow 0_B \in \varphi(S)$.

Para todo $a, b \in \varphi(S)$, $x, y \in S$. Agora, como $S$ é subanel de $A$, temos que $x - y \in S$ e, consequentemente, $\varphi(x - y) \in \varphi(S)$. Como $\varphi(x - y) = \varphi(x) - \varphi(y) = a - b$, temos que $a - b \in \varphi(S)$.

Novamente, como $S$ é subanel de $A$, $x \cdot y \in S$, então $\varphi(x \cdot y) \in \varphi(S)$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = a \cdot b$. Logo, $a \cdot b \in \varphi(S)$.

Portanto, pelo Teorema 2.1.23, $\varphi(S)$ é um subanel de $B$. □

**Teorema 2.1.28.** Seja $\phi : A \to B$ um isomorfismo de anéis. Então $\phi^{-1} : B \to A$ também é um isomorfismo de anéis.

*Demonstração.* Seja $\phi$ um isomorfismo do grupo aditivo $A$ no grupo aditivo $B$, então $\phi^{-1}$ é um isomorfismo do grupo aditivo B no grupo aditivo $A$. Agora, para mostramos que $\phi^{-1}$ é um isomorfismo de anéis, resta provar que preserva a multiplicação. De fato, como $\phi$ é sobrejetora temos que, $b_1 = \phi(a_1)$ e $b_2 = \phi(a_2)$, com $a_1, a_2 \in A$ e $b_1, b_2 \in B$. Assim, $a_1 = \phi^{-1}(b_1)$ e $a_2 = \phi^{-1}(b_2)$. Isso posto:

$$\phi^{-1}(b_1 \cdot b_2) = \phi^{-1}(\phi(a_1) \cdot \phi(a_2)) = \phi^{-1}(\phi(a_1 \cdot a_2)) = a_1 \cdot a_2 = \phi^{-1}(b_1) \cdot \phi^{-1}(b_2).$$

□

### Núcleo de um homomorfismos de anéis

**Definição 23.** Seja $\phi : A \to B$ um homomorfismo de anéis. Denominamos de núcleo de $\phi$, e denotamos por $N(\phi)$ ou $Ker(\phi)$, o seguinte subconjunto de $A$:

$$Ker(\phi) = \{x \in A \,|\, \phi(x) = 0_B\}.$$

Observe que, como $\phi(0_A) = 0_B$, então $0_A \in Ker(\phi)$. Assim, o zero de $A$ sempre pertencerá ao núcleo de $\phi$.

**Exemplo 33.** Seja $\phi_m : \mathbb{Z} \to \mathbb{Z}_m$ um homomorfismo de anéis, definido por $\phi_m(a) = \overline{a}$, para cada $a \in \mathbb{Z}$. Vamos determinar o núcleo desse homomorfismo:

$$\begin{aligned} a \in Ker(\phi) &\Leftrightarrow \overline{a} = \overline{0}; \\ &\Leftrightarrow a \equiv 0 \ (\text{mod } m); \\ &\Leftrightarrow a \text{ é múltiplo de } m. \end{aligned}$$

Sendo assim, $Ker(\phi_m) = \{0, \pm m, \pm 2m, \pm 3m, ...\}$.

**Teorema 2.1.29.** Seja $\phi : A \to B$ um homomorfismo de anéis. Então:

1. $Ker(\phi)$ é um subanel de $A$;
2. $\phi$ é injetor se, e somente se, $Ker(\phi) = \{0_A\}$.

*Demonstração.* 1. Suponhamos que $a, b \in Ker(\phi)$, então $\phi(a) = \phi(b) = 0_B$. Agora vamos mostrar que $Ker(\phi)$ é subanel de $A$ pelo Teorema 2.1.23. Temos que

$$\phi(a - b) = \phi(a) - \phi(b) = 0_B \text{ e } \phi(a \cdot b) = \phi(a) \cdot \phi(b) = 0_B \cdot 0_B = 0_B.$$

Sendo assim, $a - b \in Ker(\phi)$ e $a \cdot b \in Ker(\phi)$.

2. Suponhamos $A$ e $B$ grupos aditivos e $\phi$ um homomorfismo de grupos aditivos. Então, pelo Teorema 2.1.5, $\phi$ é injetor se, e somente se, $Ker(\phi) = \{0_A\}$.

□

**Definição 24.** Seja $A$ um anel comutativo, e $I$ um subconjunto de $A$, não vazio. Chamamos $I$ de ideal de $A$ se para todo $x, y \in I$ e $a \in A$, verificarem-se as relações seguintes:

1. $x - y \in I$;
2. $a \cdot x \in I$.

**Exemplo 34.** Se $A$ é um anel comutativo, então $\{0_A\}$ e $A$ são ideais triviais do anel.

Um ideal $I$ de um anel $A$ é um subanel de $A$, mas a recíproca não é verdadeira. De fato, se tomarmos $x, y \in I$ temos que $x - y \in I$ e $x \cdot y \in I$, visto que I é um ideal, com isso I é um subanel pelo Teorema 2.1.23. Mas se tomarmos $\mathbb{Z}$, que é um subanel de $\mathbb{Q}$, $\mathbb{Z}$ não é um ideal em $\mathbb{Q}$, visto que $1 \in \mathbb{Z}$ e $\frac{1}{2} \in \mathbb{Q}$, mas $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

O núcleo de um homomorfismo de anéis $\phi : A \to B$ é um ideal de $A$. De fato, como $\phi(0_A) = 0_B$, $0_A \in A$, assim $Ker(\phi) \neq \emptyset$. Suponhamos agora que $x, y \in Ker(\phi)$, então $\phi(x) = \phi(y) = 0_B$, logo $\phi(x - y) = \phi(x) - \phi(y) = 0_B - 0_B = 0_B$ e, portanto, $x - y \in Ker(\phi)$. Se $x \in Ker(\phi)$, então $\phi(x) = 0_B$ e, portanto, para todo $a \in A$ temos que $\phi(a \cdot x) = \phi(a) \cdot \phi(x) = \phi(a) \cdot 0_B = 0_B$, assim $a \cdot x \in Ker(\phi)$.

**Definição 25.** Sejam $A$ um anel comutativo e $a \in A$. A interseção de todos os ideais de $A$ que contém $a$ é o *ideal principal gerado por a* e denotado por $[a]$. Se todos os ideais de um anel comutativo são principais, então esse anel recebe o nome de *anel principal*.

**Teorema 2.1.30.** Seja $A$ um anel comutativo com unidade. Então $A$ é um corpo se, e somente se, os únicos ideais de $A$ são os triviais.

*Demonstração.* ($\Rightarrow$) Suponhamos que $A$ é um corpo e que $I$ um ideal em $A$. Vamos mostrar que $I = A$. Seja $a \in I$, $a \neq 0$, $a$ é inversível pois $A$ é corpo, então $a^{-1} \in A$, logo $a \cdot a^{-1} \in I$, e assim $1 \in I$. Mais ainda, dado $a' \in A, a' = a' \cdot 1 \in I$. Portanto, $A \subseteq I$, logo $A = I$.

($\Leftarrow$) Suponhamos que os ideais triviais, $\{0\}$ e A, são os únicos ideais de $A$. Vamos mostrar que todo elemento de $A$ é inversível. Sejam $a \in A$, $a \neq 0$, e $I = [a]$ um ideal. Como $I \neq \{0\}$, pois $a \in I$, então, por hipótese, $I = A$ e, portanto, $1 \in I = [a]$. Assim, $1 = a^m$, $a \cdot a^{m-1} = 1$, logo $a$ é inversível. □

Se $P$ é um ideal em um anel comutativo $A$, com $P \neq A$ e para todo $a, b \in A$, $ab \in P$, implica que $a \in P$ ou $b \in P$, então $P$ é chamado um *ideal primo* de $A$. Já um ideal $M$ de $A$, $M \neq A$, é chamado *ideal maximal* se, para todo ideal $I$ tal que $M \subset I \subset A$ e $M \neq I$, temos que $I = A$.

### 2.1.3 Anéis Quocientes

Se $I$ é um ideal em um anel comutativo $A$, então $I$ é um subanel de $A$ e um subgrupo do grupo aditivo $A$. Como $A$ é comutativo, $I$ é subgrupo normal de $(A, +)$. Com isso, podemos considerar o grupo quociente $A/I$ cujos elementos são as classes laterais $a + I$, $a \in A$. O elemento neutro de $A/I$ é a classe lateral $0 + I = I$ e o elemento oposto de $a + I$ é a classe $(-a) + I$. A adição é definida por

$$(a + I) + (b + I) = (a + b) + I, \ a, b \in A,$$

e a multiplicação é definida por

$$(a + I) \cdot (b + I) = (a \cdot b) + I.$$

$(A/I, +, \cdot)$ é chamado *anel quociente*.

Observe que as operações $+$ e $\cdot$ estão bem definidas, ou seja, não dependem da escolha dos representantes das classes de equivalência.

Se $a + I = a_1 + I$ e $b + I = b_1 + I$, então existem $x_1, x_2 \in I$ tais que $a = a_1 + x_1$ e $b = b_1 + x_2$.

Assim,

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I \\ &= ((a_1+x_1)+(b_1+x_2))+I \\ &= ((a_1+b_1)+(x_1+x_2))+I \\ &= (a_1+b_1)+I+\underbrace{(x_1+x_2)}_{\in I}+I \\ &= (a_1+b_1)+I+I \\ &= (a_1+I)+(b_1+I),\end{aligned}$$

e

$$\begin{aligned}(a+I)\cdot(b+I) &= (a\cdot b)+I \\ &= (a_1+x_1)\cdot(b_1+x_2)+I \\ &= (a_1b_1+a_1x_2+x_1b_1+x_1x_2)+I \\ &= (a_1b_1+I)+((\underbrace{a_1x_2+x_1b_1+x_1x_2}_{\in I})+I) \\ &= (a_1b_1+I) \\ &= (a_1b_1)+I \\ &= (a_1+I)\cdot(b_1+I).\end{aligned}$$

$A/I$ não é um anel de integridade sempre que $A$ é um anel de integridade. Consideremos o anel de integridade $\mathbb{Z}$ e o ideal $I=[6]$ nesse anel. Temos que $\mathbb{Z}_6$ não é um anel de integridade pelo Teorema 2.1.24, como $\mathbb{Z}_6 \cong \mathbb{Z}/[6]$ concluímos que $\mathbb{Z}/[6]$ também não é um anel de integridade.

**Teorema 2.1.31.** Seja $I$ um ideal em um anel comutativo $A$ e consideremos a aplicação $\mu : A \to A/I$, definida como $\mu(a) = a+I$, para cada $a \in A$. Então $\mu$ é um homomorfismo sobrejetor de anéis cujo núcleo é $I$.

*Demonstração.* Primeiro vamos mostrar que $\mu$ é um homomorfismo sobrejetor.

Se $a, b \in A$, então:

- $\mu(a+b) = (a+b)+I = (a+I)+(b+I) = \mu(a)+\mu(b)$;
- $\mu(a\cdot b) = (a\cdot b)+I = (a+I)\cdot(b+I) = \mu(a)\cdot\mu(b)$;

Se $y \in A/I$, então $y = a+I$, para algum $a \in A$. Suponhamos que $x = a$, então $\mu(x) = \mu(a) = a+I = y$. Portanto, $\mu$ é de fato um homomorfismo sobrejetor.

Agora, se $a \in Ker(\mu) \Leftrightarrow \mu(a) = a+I = I \Leftrightarrow a \in I$. Portanto, $Ker(\mu) = I$. □

O homomorfismo introduzido no Teorema 2.1.31 é chamado de *homomorfismo canônico* de $A$ sobre $A/I$.

**Teorema 2.1.32.** Seja $\phi : A \to B$ um homomorfismo sobrejetor de anéis. Se $I = Ker(\phi)$, então o anel quociente $A/I$ é isomorfo a $B$.

*Demonstração.* Suponhamos que $\phi : A \to B$ é um homomorfismo sobrejetor, então $I = Ker(\phi)$ é um ideal de $A$. Vamos introduzir a aplicação $\mu : A/I \to B$, definida por $\mu(a + I) = \phi(a)$, para todo $a \in A$, e mostrar que $\mu$ é um isomorfismo de anéis.

- $\mu$ é um homomorfismo de anéis:
  - $\mu((a+I)+(b+I)) = \mu((a+b)+I) = \phi(a+b) = \phi(a)+\phi(b) = \mu(a+I)+\mu(b+I)$;
  - $\mu((a + I) \cdot (b + I)) = \mu((a \cdot b) + I) = \phi(a \cdot b) = \phi(a) \cdot \phi(b) = \mu(a + I) \cdot \mu(b + I)$.
- $\mu$ é uma aplicação bijetora:
  - injetora:$a + I = b + I \Leftrightarrow a - b \in I \Leftrightarrow \phi(a - b) = 0_B \Leftrightarrow \phi(a) - \phi(b) = 0_B \Leftrightarrow \phi(a) = \phi(b)$;
  - sobrejetora: seja $y \in B$, como $\phi$ é uma aplicação sobrejetora, existe $a \in A$, tal que $\phi(a) = y$. Assim, $\mu(a + I) = \phi(a) = y$.

□

**Corolário 2.1.33.** Se $\phi : A \to B$ é um homomorfismo de anéis, então

$$A/Ker(\phi) \cong \phi(A) = \mathrm{Im}(\phi).$$

O resultado acima é conhecido como Primeiro Teorema do Isomorfismo.

**Teorema 2.1.34.** Seja $A$ um anel comutativo. Então $A$ é um domínio se, e somente se, $A$ é um subanel de um corpo.

*Demonstração.* ($\Leftarrow$) Suponhamos que $A$ seja um subanel de um corpo $K$, e sejam $a, b \in A$ tal que $ab = 0$. Vamos mostrar que $a = 0$ ou $b = 0$. Suponhamos, sem perda de generalidade, que $a \neq 0$. Como $K$ é um corpo, existe $a^{-1} \in K$, multiplicando $a^{-1}$ pela igualdade $ab = 0$ temos que, $a^{-1}ab = a^{-1} \cdot 0 \Leftrightarrow b = 0$.

($\Rightarrow$) Suponhamos que $A$ é um domínio, então $A$ é um subanel de um corpo. Seja $S = A \times (A - \{0\}) = \{(a, b) |\, a, b \in A,\, b \neq 0\}$. Vamos definir a relação $\sim$ em $S$ por:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Essa relação é de equivalência. De fato, vamos mostrar que $\sim$ é reflexiva, simétrica e transitiva.

- Reflexiva: Para todo $(a,b) \in S$, como $A$ é comutativo, temos que $ab = ba$, logo $(a,b) \sim (a,b)$.

- Simétrica: Sejam $(a,b),(c,d) \in S$, tais que $(a,b) \sim (c,d)$, então $ad = bc$. Como $A$ é comutativo, temos que $cb = da$, logo $(c,d) \sim (a,b)$.

- Transitiva: Sejam $(a,b),(c,d)$ e $(e,f) \in S$, tais que $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$, então $ad = bc$ e $cf = de$. Multiplicando a igualdade $ad = bc$ por $f$ e a igualdade $cf = de$ por $b$, temos que: $f(ad) = f(bc)$ e $b(cf) = b(de)$, então $fad = bde$, como $A$ é comutativo $d(af) = d(be)$, como $d \neq 0$ temos que $af = be$, logo $(a,b) \sim (e,f)$.

Seja $K$ o conjunto das classes de equivalência dos elementos de $S$. O conjunto quociente é $K = S/\sim = \{(a,b)_\sim |\ (a,b) \in S\}$. Vamos usar a notação $\frac{a}{b} = (a,b)_\sim$. $K = \{\frac{a}{b} |\ a,b \in A,\ b \neq 0\}$ é a estrutura de corpo que procuramos.

Vamos mostrar que as operações $+$ e $\cdot$ definidas abaixo fazem de $K$ um corpo.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

- $+$ esta bem definida. Se $\frac{a}{b} = \frac{x}{y}$ e $\frac{c}{d} = \frac{z}{w}$, então $ay = bx$ e $cw = dz$ respectivamente. Precisamos mostrar que $\frac{a}{b} + \frac{c}{d} = \frac{x}{y} + \frac{z}{w}$, ou seja, $\frac{ad+bc}{bd} = \frac{xw+yz}{yw}$, ou seja, $(ad+bc)(yw) = (xw+yz)(bd)$. Como $A$ é anel comutativo, temos que $(ad+bc)(yw) = adyw + bcyw = (ay)(dw) + (by)(cw) = (bx)(dw) + (by)(dz) = (bd)(xw+yz)$.

- $\cdot$ está bem definida. Se $\frac{a}{b} = \frac{x}{y}$ e $\frac{c}{d} = \frac{z}{w}$, então $ay = bx$ e $cw = dz$ respectivamente. Precisamos mostrar que $\frac{a}{b} \cdot \frac{c}{d} = \frac{x}{y} \cdot \frac{z}{w}$, ou seja, $\frac{ac}{bd} = \frac{xz}{yw}$, ou seja, $(ac)(yw) = (bd)(xz)$. Como $A$ é um anel comutativo, temos que $(ac)(yw) = (ay)(cw) = (bx)(dz) = (bd)(xz)$.

- $(K,+)$ é um grupo comutativo, onde $\frac{0}{1}$ é elemento neutro e o inverso de $\frac{a}{b}$ é $\frac{-a}{b}$.

  $+$ é associativa. De fato,

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)f + bde}{bdf} = \frac{adf + bcf + bde}{bdf},$$

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf + b(cf+de)}{bdf} = \frac{adf + bcf + bde}{bdf}.$$

- $(K,\cdot)$ é um monoide comutativo, ou seja, a operação $\cdot$ é associativa e comutativa, com elemento neutro $\frac{1}{1}$.

  Como $A$ é anel, então a operação $\cdot$ é associativa em $A$. Vamos mostrar que a operação $\cdot$ é associativa em $K$,

$$\frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{ace}{bdf} = \frac{ac}{bd} \cdot \frac{e}{f} = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f}.$$

É comutativa pois

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\cdot\frac{a}{b},$$

visto que $A$ é comutativo.

- Propriedade distributiva: Se $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in K$, então $\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\left(\frac{a}{b}\cdot\frac{c}{d}\right)+\left(\frac{a}{b}\cdot\frac{e}{f}\right)$ e $\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{e}{f}=\left(\frac{a}{b}\cdot\frac{e}{f}\right)+\left(\frac{c}{d}\cdot\frac{e}{f}\right)$. De fato, $\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{cf+de}{df}=\frac{a(cf+de)}{bdf}$ e $\left(\frac{a}{b}\cdot\frac{c}{d}\right)+\left(\frac{a}{b}\cdot\frac{e}{f}\right)=\frac{ac}{bd}+\frac{ae}{bf}=\frac{acbf+bdae}{bdbf}$ são iguais pois $a(cf+de)(bdbf)=bdf(acbf+bdae)$.

  Como $\cdot$ é comutativo, a outra igualdade também é verdadeira.

- Todo elemento $\frac{a}{b}\in K$, diferente de zero, possui inverso. De fato, como $\frac{a}{b}\neq\frac{0}{1}$, temos que $a\cdot 1\neq b\cdot 0$, ou seja, $a\neq 0$, logo $\frac{b}{a}\in K$. E $\frac{b}{a}$ é inverso de $\frac{a}{b}$ pois, $\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=\frac{1}{1}$, visto que $A$ é comutativo.

Dados os pontos mostrados anteriormente, podemos concluir que $K$ é um corpo. E podemos usar a seguinte notação para $A$, $A:=\{\frac{a}{1}|\ \in A\}$, que é um subanel de $K$, onde $\frac{a}{1}+\frac{b}{1}=\frac{ab}{1}$ e $\frac{a}{1}\cdot\frac{b}{1}=\frac{ab}{1}$. □

O corpo $(K,+,\cdot)$ construído na demonstração do Teorema 2.1.34 é um corpo chamado *corpo quociente* ou *corpo de frações* de $A$ e indicado como $K(A)$.

**Definição 26.** Seja $A$ um anel. Um $A$-módulo $M$ é um grupo abeliano $(M,+)$, junto com a função $\alpha:A\times M\to M$ definida por $\alpha(a,m)=am$, com $a\in A$ e $m\in M$, satisfazendo para todo $a,b\in A$, $m,n\in M$:

1. $(a+b)m=am+bm$;
2. $a(m+n)=am+an$;
3. $a(b\cdot m)=(a\cdot b)m$;
4. $1\cdot m=m$.

A função $\alpha$ é denominada $A$-ação sobre $M$. Se $A$ é um corpo $\mathbb{K}$, então um $A$-módulo é o mesmo que um espaço vetorial sobre $\mathbb{K}$.

### 2.1.4 Extensões de Corpos

Sejam $\mathbb{L}$ e $\mathbb{K}$ corpos tal que $\mathbb{K}\subseteq\mathbb{L}$. Um elemento $\alpha\in\mathbb{L}$ é chamado *elemento algébrico* sobre $\mathbb{K}$ se for raiz de um polinômio com coeficientes em $\mathbb{K}$. Dizemos que $\mathbb{L}$ é *algébrico* sobre $\mathbb{K}$ se todo elemento de $\mathbb{L}$ é algébrico sobre $\mathbb{K}$.

**Definição 27.** Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos. $\mathbb{L}$ é uma *extensão algébrica* de $\mathbb{K}$ se, e somente se, $\mathbb{K}$ é um subcorpo de $\mathbb{L}$. Neste caso, $\mathbb{K} \subset \mathbb{L}$, $\mathbb{K}$ é um corpo com as operações induzidas em $\mathbb{L}$ e $1_{\mathbb{K}} = 1_{\mathbb{L}}$.

Todo corpo $\mathbb{K}$ é uma extensão de si mesmo, e as seguintes extensões são chamadas de extensões naturais: $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{C}$ e $\mathbb{R} \subset \mathbb{C}$.

**Definição 28.** Sejam $\mathbb{K}$ um corpo e $\mathbb{S} \subseteq \mathbb{K}$ um subconjunto. O *subanel de* $\mathbb{K}$ *gerado por* $\mathbb{S}$ é a interseção de todos os subanéis de $\mathbb{K}$ que contém $\mathbb{S}$. O *subcorpo de* $\mathbb{K}$ *gerado por* $\mathbb{S}$ é a interseção de todos os subcorpos de $\mathbb{K}$ que contém $\mathbb{S}$.

**Exemplo 35.** O subanel de $\mathbb{R}$ gerado por $\{1\}$ é $\mathbb{Z}$ e o subcorpo de $\mathbb{R}$ gerado por $\{1\}$ é $\mathbb{Q}$.

**Lema 2.1.35.** Sejam $\mathbb{K}$ um corpo e $\mathbb{S} \subseteq \mathbb{K}$ um subconjunto com $1_{\mathbb{K}} \in \mathbb{S}$. Se $R$ é o subanel de $\mathbb{K}$ gerado por $\mathbb{S}$, então $R$ é um domínio e $\mathbb{F}$, o subcorpo de $\mathbb{K}$ gerado por $\mathbb{S}$, é o corpo de frações de $R$.

*Demonstração.* Por hipótese, $R$ é um subanel então, $R \subset \mathbb{F}$ pois todo subcorpo é um subanel. Agora, como $1_{\mathbb{K}} \in \mathbb{S} \subseteq R$, temos que $1_R = 1_{\mathbb{K}} = 1$. Mais ainda, como $R \subseteq \mathbb{K}$, temos que $R$ é um domínio.

Seja $\mathbb{F}' = \{a \cdot b^{-1}; a, b \in R, b \neq 0\}$ o corpo de frações de $R$. Desde que $R \subseteq \mathbb{F}$ e $\mathbb{F}'$ é o menor corpo que contém $R$, temos que $\mathbb{F}' \subseteq \mathbb{F}$. Mas temos $\mathbb{S} \subseteq R \subseteq \mathbb{F}' \subseteq \mathbb{K}$, ou seja, $\mathbb{F}'$ é um subcorpo de $\mathbb{K}$ que contém $\mathbb{S}$. Então, por definição, $\mathbb{F} \subseteq \mathbb{F}'$. Assim, $\mathbb{F}' = \mathbb{F}$. □

**Teorema 2.1.36.** Seja $\mathbb{K}$ um corpo. Temos que:

1. O subanel de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ é $\mathbb{Z} \cdot 1_{\mathbb{K}} = \{a \cdot 1_{\mathbb{K}} \,|\, a \in \mathbb{Z}\}$ e o subcorpo de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ é o corpo de frações de $\mathbb{Z} \cdot 1_{\mathbb{K}}$;

2. Se $\varphi : \mathbb{Z} \to \mathbb{K}$ definida por $\varphi(a) = a \cdot 1_{\mathbb{K}}$, para todo $a \in \mathbb{Z}$, então $\varphi$ é um homomorfismo de anéis com $\mathrm{Im}(\varphi) = \mathbb{Z} \cdot 1_{\mathbb{K}}$ e $Ker(\varphi) = p\mathbb{Z}$, para algum $p$ primo em $\mathbb{Z}$;

3. Se $Ker(\varphi) = \{0\}$, então $\mathbb{Z} \cdot 1_{\mathbb{K}} \cong \mathbb{Z}$ e o subcorpo de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ é isomorfo a $\mathbb{Q}$.

4. Se $Ker(\varphi) = p\mathbb{Z}$, com $p$ primo, então $\mathbb{Z} \cdot 1_{\mathbb{K}} \cong \mathbb{Z}_p$ e o subcorpo de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ é também isomorfo a $\mathbb{Z}_p$.

*Demonstração.* 1. Todo subanel de $\mathbb{K}$ que contém $1_{\mathbb{K}}$ contém $\mathbb{Z} \cdot 1_{\mathbb{K}}$ e, $\mathbb{Z} \cdot 1_{\mathbb{K}}$ é um subanel de $\mathbb{K}$ que contém $1_{\mathbb{K}}$. Então $\mathbb{Z} \cdot 1_{\mathbb{K}}$ é subanel de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ e, do Lema 2.1.35, seu corpo de frações é o subcorpo de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$.

2. É fácil ver que $\varphi$ é um homomorfismo de anéis onde $\text{Im}(\varphi) = \mathbb{Z} \cdot 1_{\mathbb{K}}$. Pelo Teorema 2.1.22 temos que $\mathbb{Z}/\text{Ker}(\varphi) \simeq \text{Im}\,(\varphi) = \mathbb{Z} \cdot 1_{\mathbb{K}}$, como é um subanel de um corpo com 1, é um domínio. Logo, $\text{Ker}(\varphi)$ é um ideal primo de $\mathbb{Z}$, ou seja, $\text{Ker}(\varphi) = \{0\}$ ou $\text{Ker}(\varphi) = p\mathbb{Z}$, com $p$ primo em $\mathbb{Z}$.

3. Se $Ker(\varphi) = \{0\}$, então $\varphi$ é injetor e $\mathbb{Z} \cong \mathbb{Z}/Ker(\varphi) \cong \text{Im}(\varphi) = \mathbb{Z} \cdot 1_{\mathbb{K}}$. O subcorpo de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ é o corpo de frações de $\mathbb{Z} \cdot 1_K$ pelo 1., que é isomorfo ao corpo de frações de $\mathbb{Z}$, que é $\mathbb{Q}$.

4. Se $Ker(\varphi) = p\mathbb{Z}$, com $p$ primo em $\mathbb{Z}$, então $\mathbb{Z} \cdot 1_{\mathbb{K}} = \text{Im}(\varphi) \cong \mathbb{Z}/Ker(\varphi) = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$, que é corpo e, portanto, igual ao seu corpo de frações.

□

**Definição 29.** O subcorpo de $\mathbb{K}$ gerado por $\{1_{\mathbb{K}}\}$ é chamado de *corpo primo* de $\mathbb{K}$, é a interseção de todos os subcorpos de $\mathbb{K}$.

**Corolário 2.1.37.** Sejam $\mathbb{K}$ um corpo e $\varphi : \mathbb{Z} \to \mathbb{K}$ um homomorfismo de anéis definido por $\varphi(a) = a \cdot 1_{\mathbb{K}}$. Se $Ker(\varphi) = \{0\}$, então o corpo primo de $\mathbb{K}$ é isomorfo a $\mathbb{Q}$. Se $Ker(\varphi) = p\mathbb{Z}$, com $p$ primo, então o corpo primo de $\mathbb{K}$ é isomorfo a $\mathbb{Z}_p$.

**Definição 30.** Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{K}$. A dimensão de $\mathbb{L}$ sobre $\mathbb{K}$ é chamada *grau da extensão*, ou grau de $\mathbb{L}$ sobre $\mathbb{K}$, e é denotada por $[\mathbb{L} : \mathbb{K}]$. Se o grau de $\mathbb{L}$ sobre $\mathbb{Q}$ é finito, dizemos que $\mathbb{L}$ é um *corpo de números*.

**Exemplo 36.** $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ é uma extensão finita de grau 2. De fato, $\{1, \sqrt{2}\}$ gera $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ como $\mathbb{Q}$-espaço vetorial. Suponhamos que $a + b\sqrt{2} = 0$, com $a, b \in \mathbb{Q}$. Se $b \neq 0$, então $\sqrt{2} = -a \cdot b^{-1} \in \mathbb{Q}$, o que é um absurdo. Logo, $b = 0$ e, consequentemente, $a = 0$. Portanto, $\{1, \sqrt{2}\}$ é linearmente independente sobre $\mathbb{Q}$. Então, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

A extensão de grau 2 sobre o corpo $\mathbb{Q}$ dos números racionais do Exemplo 36 é chamada *corpo quadrático*. Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde $d$ é um inteiro livre de quadrados, ou seja, $d \not\equiv 0 \ (mod\, 4)$.

**Teorema 2.1.38.** Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático, onde $d$ é um inteiro livre de quadrados. Além disso, se

(i) $d \not\equiv 1 \ (mod\, 4)$, então o anel dos inteiros $\mathbb{I}_{\mathbb{K}}$ é $\mathbb{Z}[\sqrt{d}]$ e $\{1, \sqrt{d}\}$ é base de $\mathbb{Z}[\sqrt{d}]$ como um $\mathbb{Z}$-*módulo*.

(ii) $d \equiv 1 \ (mod\, 4)$, então o anel dos inteiros $\mathbb{I}_{\mathbb{K}}$ é $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ e $\{1, \frac{1+\sqrt{d}}{2}\}$ é base de $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ como um $\mathbb{Z}$-*módulo*.

Uma demonstração do Teorema 2.1.38 pode ser encontrada em [16].

### 2.1.5 Norma e Traço de um Elemento

Sejam $\mathbb{K}$ um corpo de números de grau $n$ e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Para qualquer $\alpha \in \mathbb{K}$ definimos respectivamente a norma e o traço de $\alpha$, como

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad e \quad Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Como os $\sigma_i's$ são monomorfismos segue que

$$N(\alpha \cdot \beta) = N(\alpha)N(\beta),$$

para quaisquer $\alpha, \beta \in \mathbb{K}$.

**Teorema 2.1.39.** Sejam $\mathbb{K}$ um corpo de números, $I_{\mathbb{K}}$ o anel de inteiros de $K$ e $[\alpha]$ o ideal de $I_{\mathbb{K}}$ gerado por $\alpha$, então o anel quociente $\frac{I_{\mathbb{K}}}{[\alpha]}$ tem $N(\alpha)$ elementos.

Uma demonstração do Teorema 2.1.39 pode ser encontrada em [12].

**Corolário 2.1.40.** Seja $\alpha \in I_{\mathbb{K}}$.

1. Se $\beta \in I_{\mathbb{K}}$ é tal que $\beta | \alpha$, então o ideal $[\beta] \subset \frac{I_{\mathbb{K}}}{[\alpha]}$ tem ordem $N(\alpha)/N(\beta)$;
2. Se $\beta \in I_{\mathbb{K}}$ é tal que $\beta \not| \alpha$ e $\gamma = mdc(\alpha, \beta)$, então o ideal $[\beta] \subset \frac{I_{\mathbb{K}}}{[\alpha]}$ é gerado por $\gamma$ e tem ordem $N(\alpha)/N(\gamma)$.

### 2.1.6 Anéis de Inteiros Gaussiano e de Einsenstein-Jacobi

Dado o corpo de números $\mathbb{K} = \mathbb{Q}[i] = \{a + bi \,|\, a, b \in \mathbb{Q}\}$, pelo Teorema 2.1.38 o anel dos inteiros de $\mathbb{K}$ é $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$, chamado *anel dos inteiros de Gauss*.

A norma de $\mathbb{Z}[i]$ é dada pela aplicação $N : \mathbb{Z}[i] \to \mathbb{Z}_+$, definida como $N(\alpha) = \alpha \cdot \overline{\alpha}$, onde $\alpha = a + bi$ e $\overline{\alpha}$ é o conjugado de $\alpha, a - bi$.

A aplicação $N$ é um monomorfismo. De fato, como $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$, temos que $N(\alpha \cdot \beta) = \alpha \cdot \beta \cdot \overline{\alpha \cdot \beta} = \alpha \cdot \beta \cdot \overline{\alpha} \cdot \overline{\beta} = \alpha \cdot \overline{\alpha} \cdot \beta \cdot \overline{\beta} = N(\alpha) \cdot N(\beta)$. Assim, $N$ é um homomorfismo, e a aplicação $N$ é injetora pois, dados $\alpha = a + bi$ e $\beta = c + di$, se $\alpha \neq \beta$, então $a \neq c$ e $b \neq d$, logo $N(\alpha) = (a+bi) \cdot (a-bi) = a^2 + b^2 \neq c^2 + d^2 = (c+di) \cdot (c-di) = N(\beta)$, então $N(\alpha) \neq N(\beta)$.

O anel quociente $\frac{\mathbb{Z}[i]}{[\alpha]}$, denotado por $\mathbb{Z}[i]_\alpha$, possui $N(\alpha) = a^2 + b^2$ elementos, conforme o Teorema 2.1.39.

**Exemplo 37.** Observe os elementos do anel quociente $\mathbb{Z}[i]_{3+4i}$,

$$\begin{aligned}\mathbb{Z}[i]_{3+4i} = \{&0, 1, 2, 3, -1, -2, -3, i, 2i, 3i, -i, -2i, -3i, 1+i, 1+2i, 1-i, 1-2i, -1-i, -1-2i,\\ &-1+i, -1+2i, 2+i, -2+i, 2-i, -2-i\}.\end{aligned}$$

Como $\alpha = 3+4i$, temos que $N(\alpha) = 25$, ou seja, o quociente do anel $\mathbb{Z}[i]$ e o ideal $[3+4i]$, possui 25 elementos.

Agora, tomando o corpo de números $\mathbb{K} = \mathbb{Q}[\sqrt{-3}]$, novamente pelo Teorema 2.1.38 o anel dos inteiros de $\mathbb{K}$ é $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$, chamado *anel dos inteiros de Eisenstein-Jacobi* e denotado por $\mathbb{Z}[\omega] = \{a+b\omega |\ a,b \in \mathbb{Z}\}$, onde $\omega = \left(\frac{-1+\sqrt{-3}}{2}\right)$. Temos que $\omega^2+\omega+1=0$. Assim, se $\alpha = a+b\omega \in \mathbb{Z}[\omega]$ sua norma é dada por

$$\begin{aligned} N(\alpha) &= \alpha \cdot \overline{\alpha} = (a+b\omega)(a+b\omega^2) \\ &= (a+b\omega)((a-b)-b\omega) = a^2+b^2-ab. \end{aligned}$$

De maneira análoga mostramos que a aplicação que defini a norma de um inteiro de Einsenstein-Jacobi é um monomorfismo.

O anel quociente $\frac{\mathbb{Z}[\omega]}{[\alpha]}$, denotado por $\mathbb{Z}[\omega]_\alpha$, possui $N(\alpha) = a^2+b^2-ab$ elementos, conforme o Teorema 2.1.39.

**Exemplo 38.** Observe agora os elementos do anel quociente $\mathbb{Z}[\omega]_{3+4\omega}$

$$\mathbb{Z}[\omega]_{3+4\omega} = \{0,1,-1,2,-2,\omega,-\omega,2\omega,-2\omega,1+\omega,-1-\omega,2+2\omega,-2-2\omega\}.$$

Como $\alpha = 3+4\omega$, temos que $N(\alpha) = 13$, ou seja, o quociente do anel $\mathbb{Z}[\omega]$ e o ideal $[3+4\omega]$, possui 13 elementos.

## 2.2 Grafos

Um grafo $G$ consiste de um conjunto finito e não vazio $V(G)$ de elementos denominados *vértices* e um conjunto $A(G)$ de elementos denominados *arestas*, que são pares não ordenados de vértices.

É uma função de incidência $\psi : A \to V \times V$ definida como $\psi(a) = uv$ (ou $\psi(a) = vu$, pois a ordem não importa) que associa a cada aresta $a$ um par não ordenado de vértices $u, v$, os quais chamamos de extremos de $a$. Podemos representar um grafo da seguinte forma:

$$G = (V, A),$$

onde $V = V(G)$ e $A = A(G)$.

Se $G = (V, A)$ é um grafo e $u$ e $v$ são dois de seus vértices, diremos que $u$ e $v$ são vizinhos ou adjacentes se $\{u, v\} \in A$; neste caso, dizemos que a aresta $\{u, v\}$ incide nos vértices $u$ e $v$. Se $u$ e $v$ não forem adjacentes, dizemos que são vértices não adjacentes de $G$. Denotamos a aresta $\{u, v\}$ por $uv$, sempre que não houver perigo de confusão.

Grafos são representados por diagramas, onde os elementos de $V$ correspondem a pontos no plano e os elementos de $A$ são os arcos que ligam os pontos correspondentes.

Um grafo pode ter diferentes representações gráficas, o propósito da figura gerada é apenas representar esquematicamente as relações de adjacência entre os vértices de $G$.

**Exemplo 39.** Dado $G = (\{a, b, c, d\}; \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}\})$, o grafo $G$ pode ser representado de duas formas apresentadas na Figura 1, pois as duas ilustram as mesmas relações de adjacência entre os vértices.

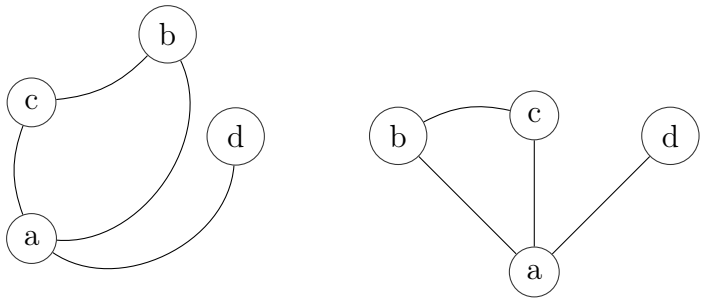


Figura 1 – Representações do grafo $G$.

Fonte: Autor.

O número de vértices de $G$ é denotado por $n(G)$ e o número de arestas por $m(G)$. Assim, $n(G) = |V(G)|$ e $m(G) = |A(G)|$. Um grafo é dito *completo* se possui $n$ vértices, com dois quaisquer deles conectados por um arco. Um grafo completo com $n$ vértices é denotado por $K_n$, e possui $\begin{pmatrix} n \\ 2 \end{pmatrix} = \frac{n(n-1)}{2}$ arestas.

**Definição 31.** Um grafo é chamado *trivial* se possui $n$ vértices e nenhuma aresta. Denotamos $G = (V, \emptyset)$, e representamos com um conjunto de $n$ pontos no plano.

**Definição 32.** Fixado um vértice $u$ de $G$, denotamos por $N_G(u)$ o conjunto dos vértices adjacentes a $u$:

$$N_G(u) = \{v \in V; uv \in A\}.$$

**Definição 33.** Seja $G = (V, A)$ um grafo. Se $u \in V$, o *grau* de $u$, denotado por $d_G(u)$, é o número de vértices adjacentes a $u$, isto é

$$d_G(u) = |N_G(u)|.$$

**Teorema 2.2.1.** Dado o grafo $G = (V, A)$, a soma dos graus dos vértices é igual ao dobro do número de arestas, ou seja,

$$2|A| = \sum_{u \in V} d_G(u).$$

*Demonstração.* Tomemos a aresta $a = \{u, v\}$ de $G$. Observe que $a$ é contada exatamente duas vezes, uma vez na parcela $d_G(u)$ e outra na parcela de $d_G(v)$. Portanto, $|A|$ deve ser multiplicado por 2, visto que toda aresta contribui exatamente duas vezes na soma $\sum_{u \in V} d_G(u)$. □

**Exemplo 40.** Grafo de palavras: cada vértice é uma palavra da língua portuguesa e duas palavras são adjacentes se diferem em exatamente uma posição. Por exemplo, *rato* e *ralo* são adjacentes, enquanto *ralo* e *rota* não são. Observe o grafo definido pelas seguintes palavras: *caiado, cavado, cavalo, girafa, girava, ralo, ramo, rata, rato, remo, reta, reto, rota, vaiado, varado, virada, virado, virava*, representado na Figura 2.

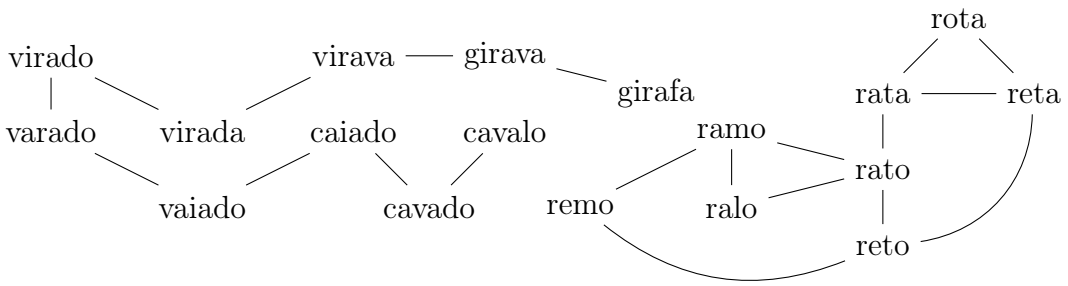


Figura 2 – Grafo de palavras.

Fonte: Autor.

**Exemplo 41.** Um cubo de dimensão $k$, ou $k$-cubo, é o grafo definido da seguinte maneira: os vértices do grafo são todas as sequências $b_1b_2...b_k$ em que cada $b_i$ pertence a $\{0, 1\}$; dois vértices são adjacentes se diferem em exatamente uma posição. Observe o cubo de dimensão 3, o 3-cubo, representado na Figura 3.

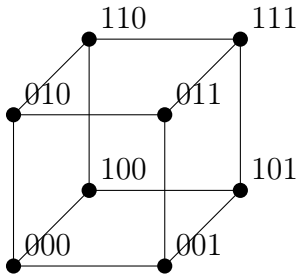


Figura 3 – Grafo do $3-$*cubo*.

Fonte: Autor.

O $k$-cubo possui $2^k$ vértices e $k \cdot 2^{k-1}$ arestas.

**Exemplo 42.** Seja $V$ o conjunto de todos os subconjuntos de $\{1, 2, 3, 4, 5\}$ que têm exatamente 2 elementos. Dois elementos $v$ e $w$ de $V$ são adjacentes se $v \cap w = \emptyset$. Essa relação de adjacência sobre $V$ define o *grafo de Petersen*, representado na Figura 4.

## 2.3 Códigos Corretores de Erros

Podemos dizer que a construção de códigos inspira-se nos idiomas. O alfabeto $A$ da língua portuguesa, por exemplo, é composto de 26 letras, espaço em branco, o c cedilha

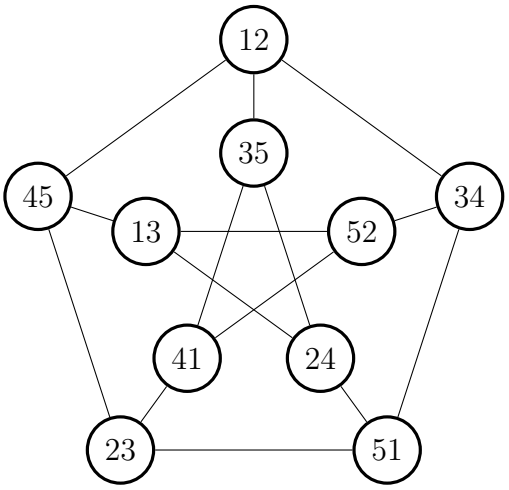


Figura 4 – Grafo de Petersen.

Fonte: Autor.

e as vogais acentuadas. As palavras são sequências de letras, e podem ser consideradas como elementos do conjunto $A^{27}$, onde 27 é o comprimento da palavra mais longa desse idioma. Como nem todas sequências de letras formam palavras, a língua portuguesa pode ser vista como um subconjunto próprio $\mathcal{C}$ de $A^{27}$.

Agora, suponhamos que ao escrever uma palavra, obtemos a sequência de letras "fonre", como essa sequência não pertence a $\mathcal{C}$, é identificado um erro. Neste caso, a correção é simples, pois no conjunto $\mathcal{C}$, existe a palavra "fonte", que é muito próxima da sequência digitada. Este código $\mathcal{C}$ não é muito eficiente, pois se digitarmos a palavra "gato", quando na verdade desejávamos a palavra "rato", nenhum erro será detectado, pois ambas as palavras pertencem a $\mathcal{C}$ e, consequentemente, não haverá uma correção.

Podemos resumir o processo de transmissão de informação da seguinte forma: a informação parte de uma fonte e é destinada a um receptor, através de um meio conhecido como canal, se o canal não tem ruído, a informação recebida será igual a enviada, porém na prática ruído é adicionado à informação resultando na introdução de erros pelo canal. A função do código é detectar e talvez corrigir esses erros.

Os códigos corretores de erros estão presentes em diversas atividades em nosso dia-a-dia, quando utilizamos redes sem fio, por exemplo, quando falamos ao telefone. Um código desta classe, basicamente, acrescenta dados adicionais a cada informação que deve ser transmitida ou armazenada, de maneira que ao recuperar essa informação, seja possível detectar e corrigir erros. Para ilustrar vamos supor que um robô esta andando sobre um piso quadriculado de modo que ao darmos os comandos Leste, Oeste, Norte ou Sul, ele se desloque conforme o comando. Essas direções codificadas pelos elementos do conjunto $\{0,1\} \times \{0,1\}$ da seguinte maneira:

Suponhamos que desejamos que o robô vá para o Sul, e devido a alguma interferência

| Fonte | | Código de fonte |
|---|---|---|
| Leste | → | 00 |
| Oeste | → | 01 |
| Norte | → | 10 |
| Sul | → | 11 |

o robô receba o comando 10, então se deslocará para o Norte, nenhum erro será detectado e corrigido pois ambas as palavras pertencem ao código. Para evitar esse tipo de problema pode se recodificar as palavras de modo a introduzir redundância que permita detectar e corrigir erros, quando fazemos isso estamos modificando o código de fonte para que se torne um código corretor de erro. Observe a recodificação apresentada a seguir:

| Fonte | | Código de fonte | | Código do Canal |
|---|---|---|---|---|
| Leste | → | 00 | → | 00000 |
| Oeste | → | 01 | → | 01011 |
| Norte | → | 10 | → | 10110 |
| Sul | → | 11 | → | 11101 |

Agora, suponhamos novamente que desejamos que o robô vá para o Sul, ou seja, a informação enviada é 11101, porém a mensagem recebida é 11111. Neste caso identificaríamos o erro, visto que a palavra "11111" não pertence ao código. Além disso, poderíamos corrigir o erro, pois a palavra do código que tem menor número de componentes diferentes da mensagem recebida é 11101, que é a mensagem enviada.

O procedimento realizado anteriormente pode ser esquematizado pelo diagrama dado pela Figura 5, que descreve o funcionamento dos códigos corretores de erros.

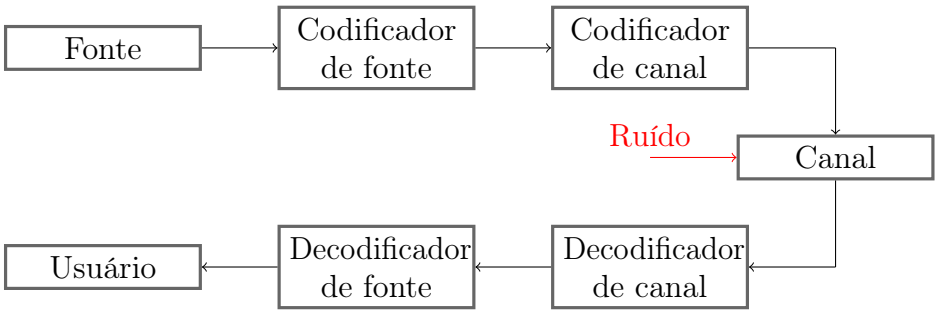


Figura 5 – Diagrama do funcionamento de um sistema de comunicação.

Fonte: Autor.

Podemos definir um código corretor de erros (CCE) da seguinte forma:

**Definição 34.** Considere um conjunto finito $K$ chamado alfabeto. Um *código corretor de erros* $\mathcal{C}$ é um subconjunto próprio qualquer de $K^n$, para algum número natural $n$. Chamamos cada elemento de $\mathcal{C}$ de palavra-código.

A definição de distância entre duas palavras-código $v$ e $w$ pertencentes a um mesmo código $\mathcal{C}$ é dada pela distância de Hamming, que é exatamente o número de posições nas quais duas palavras diferem. Assim, sejam as palavras $\mathbf{v} = \{v_1, v_2, ..., v_n\}$ e $\mathbf{w} = \{w_1, w_2, ..., w_n\} \in \mathcal{C}$, a distância de Hamming é definida por :

$$d(\mathbf{v}, \mathbf{w}) = |\{i;\, v_i \neq w_i, 1 \leq i \leq n\}|,$$

onde $|\{\cdot\}|$ denota a cardinalidade do conjunto $\{\cdot\}$.

**Definição 35.** Um espaço métrico é um par $(M, d)$, onde $M$ é um conjunto e $d : M \times M\mathbb{R}$, uma função, a qual indiquemos por $d(x, y)$ a imagem de um par genérico $(x, y) \in M \times M$ através da função $d$, é tal que, para todo $x$, $y \in M$:

1. $d(x, y) > 0$ se $x \neq y$; $d(x, y) = 0$ se $x = y$;
2. $d(x, y) = d(y, x)$;
3. $d(x, y) \leq d(x, z) + d(y, z)$.

**Teorema 2.3.1.** Dados $u, v, w \in K^n$, valem as seguintes propriedades:

1. Positividade: $d(u, v) \geq 0$. Se $u = v$, $d(u, v) = 0$;
2. Simetria: $d(u, v) = d(v, u)$;
3. Desigualdade triangular: $d(u, v) \leq d(u, w) + d(w, v)$.

*Demonstração.*

1. Positividade: Por definição $d(v, w) = |\{i;\, v_i \neq w_i, 1 \leq i \leq n\}|.$, ou seja, assume apenas valores positivos se $u \neq v$, então é necessário mostrar apena o caso em que $u = v$. Agora, se $u = v$, então $d(u, v) \neq i$, mas temos que $d(u, v) \geq 0$, logo $d(u, v) = 0$.

2. Simetria: Dados $u, v \in K^n$,

$$d(u, v) = |\{i;\, u_i \neq v_i, 1 \leq i \leq n\}| = |\{i;\, v_i \neq u_i, 1 \leq i \leq n\}| = d(v, u).$$

3. Desigualdade triangular: Temos que $d(u, v) = 0$ se $u = v$ e $d(u, v) = |\{i;\, v_i \neq w_i, 1 \leq i \leq n\}|$ se $u \neq v$. No caso em que $d(u, v) = 0$, a desigualdade é verdadeira, visto que $d(u, w) + d(w, v) = 2 \cdot d(u, w)$, como $u \neq w$ a $d(u, w) > 0 \Rightarrow 2 \cdot d(u, w) > 0$. E, no caso em que $u \neq v$, temos que $u \neq w$ e $w \neq v$. Suponhamos que $d(u, w) = n_1$ e $d(w, v) = n_2$, então $d(u, w) + d(w, v) = n_1 + n_2$ no máximo (e no mínimo $|n_1 - n_2|$). Portanto, vale a desigualdade triangular.

□

Pelo Teorema 2.3.1 concluímos também que a distância de Hamming é uma métrica em $K^n$.

**Exemplo 43.** Seja $K_3^4 = \{0,1,2\}^4$, então

$$\begin{aligned} d(0101,0001) &= 1 \\ d(0210,0201) &= 2 \\ d(0000,0222) &= 3 \\ d(1210,1210) &= 0. \end{aligned}$$

**Definição 36.** A *distância mínima* de um código $\mathcal{C}$ é dada por

$$\mathbf{d} = \min\{d(v,w); v,w \in C, v \neq w\}.$$

**Definição 37.** O *peso* de um vetor arbitrário não nulo $v \in K^n$ é determinado pela distância de $v$ ao vetor nulo (o vetor nulo é denotado por 0, tal que $0+v=v$, para todo $v \in V$, onde $V$ é um espaço vetorial sobre o corpo $\mathbb{K}$.):

$$\omega(v) := min|\{i : v_i \neq 0\}|.$$

Assim, o peso mínimo de um código é dado por

$$\omega(\mathcal{C}) := min\{\omega(x) : x \in \mathcal{C} - \{0\}\}.$$

A distância mínima $\mathbf{d}$ entre palavras-código distintas é igual ao peso mínimo de todas as palavras-código não nulas de $\mathcal{C}$, isto é, $d = \omega(\mathcal{C})$.

Um código $\mathcal{C}$ pode detectar até $\mathbf{d}-1$ erros e corrigir até $t$ erros, onde $t = \left[\frac{d-1}{2}\right]$, [15]. Observe que quanto maior for a distância mínima do código $\mathcal{C}$, maior será sua capacidade de detecção e correção de erros.

Dado um alfabeto $\mathcal{A} = \mathbb{F}_q$ com $q$ símbolos. O codificador para um código de bloco divide a sequência de informação em blocos de $k$ símbolos, representados por uma $k$-upla $u = (u_1, ..., u_k)$ chamada mensagem. Esse alfabeto possui no total $q^k$ mensagens diferentes. Após a divisão da sequência de informação, o codificador transforma cada mensagem $u$ em uma $n$-upla $v = (v_1, ..., v_n)$, sendo $v$ uma palavra-código. Note que se cada uma das $q^k$ mensagens é transformada em uma palavra-código pelo codificador, então existem $q^k$ palavras-código diferentes em $\mathcal{A}$.

Denominamos esse conjunto formado por $q^k$ palavras-código de comprimento $n$ de código de bloco com parâmetros $(n,k)$ ou $(n,k,d)$, onde $d$ é a distância mínima do código, definida anteriormente. Nos código de bloco o resultado é transmitido, corrompido pelo ruído, e decodificado independentemente dos outros blocos. A principal classe dos códigos de bloco é a dos códigos lineares.

Em geral, $q$ é uma potência de um primo $p$, e o caso mais comum em códigos é quando $q = 2$, conhecido como binário. Neste caso, $\mathbb{F}_2 = \{0, 1\}$, e os elementos 0 e 1 são chamados bits, [15].

Considere um código de bloco com $q^k$ palavras-código e comprimento $n$. Se $k$ e $n$ são relativamente grandes, então teremos dificuldade quanto ao espaço para armazenar essas palavras-código. Nesse sentido, códigos de bloco com uma estrutura linear são mais práticos e reduzem a complexidade do codificador.

**Definição 38.** Um código de bloco de comprimento $n$ com $q^k$ palavras-código é um *código linear* $(n, k)$ se suas $q^k$ palavras-código formam um subespaço de dimensão $k$ do espaço vetorial de todas as $n$-uplas sobre o corpo $\mathbb{F}_q$.

Se $B = \{v_1, v_2, ..., v_k\}$ é uma base ordenada do código $\mathcal{C}$, onde $v_i = \{v_{i1}, ..., v_{in}\}$, a *matriz geradora* G do código $\mathcal{C}$ associada a base $B$, é a matriz onde suas linhas são os vetores da base de $\mathcal{C}$, dada por

$$G = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

Qualquer correspondência um-a-um entre as $k$-uplas e as palavras-código pode ser usada como um procedimento de codificação

$$v = u \cdot G,$$

onde $u$ é uma $k$-upla de símbolos de informação a serem codificadas e a $n$-upla $v$ é a palavra-código correspondente.

Toda matriz geradora G é uma matriz na forma $\mathrm{G} = (I_k \,|\, P)$, onde $I_k$ é a matriz identidade de ordem $k$ e $P$ é uma matriz de ordem $k \times (n - k)$, [15].

Seja $\mathcal{C}$ um subespaço de dimensão $k$, de um espaço vetorial de dimensão $n$, seu complemento ortogonal $\mathcal{C}^\perp$ formado por todos os vetores ortogonais a $\mathcal{C}$, é um espaço vetorial de dimensão $n - k$, e portanto, um código linear. Uma matriz $H$ de ordem $n - k$ cujo espaço linha é $\mathcal{C}^\perp$ pode ser considerada uma matriz geradora para $\mathcal{C}^\perp$. Então uma $n$-upla $v$ é uma palavra-código de $\mathcal{C}$ se, e somente se, é ortogonal a todo vetor linha de $H$, ou seja,

$$vH^T = 0.$$

Podemos verificar se uma palavra-código $v$ pertence a um código $\mathcal{C}$ pela equação anterior, pois $v$ é ortogonal a todo elemento do espaço vetorial $\mathcal{C}^\perp$, então $v \in \mathcal{C}^\perp$.

# 3 Códigos Geometricamente Uniformes

Neste capítulo introduziremos o conceito de códigos geometricamente uniformes no plano Euclidiano e de códigos sobre grafos. Definimos o conceito de códigos perfeitos e quase perfeitos sobre os anéis dos inteiros de Gauss e de Eisenstein-Jacobi e expusemos alguns exemplos destes. As principais referências utilizadas nesse capitulo são [6], [7] e [16].

**Definição 39.** Seja $\mathcal{A}$ um alfabeto e $n$ um número natural. Dizemos que uma função $F : \mathcal{A}^n \to \mathcal{A}^n$ é uma isometria de $\mathcal{A}^n$ se ela preserva distância, ou seja,

$$d(F(x), F(y)) = d(x, y), \forall x, y \in \mathcal{A}^n.$$

**Exemplo 44.** Sejam $\mathbb{F}_2 = 0, 1$ e $n = 3$. A aplicação $F : \mathbb{F}_2 \to \mathbb{F}_2$, definida por $F(x_1, x_2, x_3) = (1x_1, x_2, x_3)$, é uma isometria. De fato, como $1x_1 = 1y_1 \Leftrightarrow x_1 = y_1$ temos que $d(F(x_1, x_2, x_3), F(y_1, y_2, y_3)) = d((1x_1, x_2, x_3), (1y_1, y_2, y_3)) = d((x_1, x_2, x_3), (y_1, y_2, y_3))$

Uma constelação de sinais $S$ é um subconjunto finito de pontos em um espaço métrico $(M, d)$. Essa constelação é um código geometricamente uniforme se, dados $s_1$ e $s_2$ em $S$, existe uma isometria $u_{s_1,s_2}$ que transforma $s_1$ em $s_2$ mantendo $S$ invariante, ou seja,

$$u_{s_1,s_2}(s_1) = s_2, \qquad u_{s_1,s_2}(S) = S. \tag{3.1}$$

Seja $U(S)$ o grupo de simetrias de $S$ em $M$.Assim, $S$ é geometricamente uniforme se o grupo de simetrias $U(S)$ de $S$ age transitivamente em $S$. Se $S$ for finito, dizemos que $S$ é uma constelação uniforme, se $S$ for infinito dizemos que $S$ é um arranjo regular.

Seja $P = \{p_1, p_2, p_3, p_4, ..., p_n\}$ um conjunto de pontos no plano Euclidiano, com $2 \leq n \leq \infty$. Cada ponto $p_i$ tem coordenadas cartesianas $(x_i, y_i)$ e $p_i \neq p_j$ para $i \neq j$, $i$ e $j \in \{1, 2, ..., n\}$. Toma-se um ponto $p$ qualquer do plano Euclidiano com coordenadas $(x, y)$. A distância Euclidiana de $p$ até $p_i$ é dada por:

$$d(p, p_i) = \sqrt{(x - x_i)^2 + (y - y_i)^2}. \tag{3.2}$$

Se $d(p, p_i) \leq d(p, p_j)$, com $j \neq i$, o ponto $p$ é designado para $p_i$ e a região $V(p_i)$, chamada região de Voronoi associada ao ponto $p_i$, é definida por:

$$V(p_i) = \{p \mid d(p, p_i) \leq d(p, p_j), j \neq i\}.$$

A região de Voronoi de $s_0$ em $S$ consiste dos pontos que estão mais próximos de $s_0$ que de qualquer outro ponto de $S$.

Para realizar o processo de decodificação, em códigos geometricamente uniformes, não é necessário saber a região de Voronoi de cada palavra-código; simplesmente basta saber a região de Voronoi associada a uma dessas palavras-código e podem-se determinar as demais regiões a partir de translações da região conhecida. Em um código geometricamente uniforme todas as regiões de Voronoi são congruentes.

## 3.1 Códigos sobre Grafos

**Definição 40.** Seja $\alpha \neq 0$, $\alpha \in \mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = \omega$. A distância sobre $\mathbb{Z}[\rho]_\alpha$ é a distância induzida pelo grafo $G_\alpha$. Assim, se $\eta, \tau \in \mathbb{Z}[\rho]_\alpha$, a distância $D_\alpha$ é dada por:

- $D_\alpha(\eta, \tau) = min\{|x| + |y|\}$, tal que $\tau - \eta \equiv x + yi \ (mod\ \alpha)$, onde $\rho = i$.
- $D_\alpha(\eta, \tau) = min\{|x| + |y| + |z|\}$, tal que $\tau - \eta \equiv x + y\omega + z\omega^2 \ (mod\ \alpha)$, onde $\rho = \omega$.

Podemos definir um grafo gerado por $\alpha$, com $\alpha \in \mathbb{Z}[\rho]$, da seguinte forma:

**Definição 41.** Seja $\alpha \neq 0$, com $\alpha \in \mathbb{Z}[\rho]$, onde $\rho = i$ ou $\rho = \omega$. O grafo gerado por $\alpha$, denotado por $G_\alpha = (V, A)$, é definido por:

- $V = \mathbb{Z}[\rho]_\alpha$ é o conjunto de vértices;
- $A = \{(\eta, \tau) \in V \times V |\ D_\alpha(\eta, \tau) = 1\}$ é o conjunto de arestas.

**Exemplo 45.** Seja $V = \mathbb{Z}[i]_{3+4i}$ o conjunto de vértices definido no Exemplo 37, o conjunto de arestas satisfaz a Definição 41 e sua representação pode ser vista na Figura 6.

Por exemplo, tomando $\mathbb{Z}[i]_{3+4i}$. Se $\eta = -1$ e $\tau = 1+2i$, temos que $\tau-\eta = 2+2i$, logo $D_\alpha(\eta, \tau) = 2+2 = 4$. Se $\eta = -3i$ e $\tau = 1+2i$, temos que $\tau - \eta = 1+5i \equiv -2-i \ (mod\ \alpha)$, logo $D_\alpha(\eta, \tau) = 2+1 = 3$. Como $D_\alpha(\eta, \tau) \neq 1$ não existe uma aresta ligando esses vértices.

**Exemplo 46.** Seja $V = \mathbb{Z}[\omega]_{3+4\omega}$ o conjunto de vértices definido no Exemplo 38, o conjunto de arestas satisfaz a Definição 41 e a sua representação pode ser vista na Figura 7.

Agora, se tomarmos $\mathbb{Z}[\omega]_{3+4\omega}$. Se $\eta = -\omega$ e $\tau = \omega$, temos que $\tau - \eta = 2\omega$, logo $D_\alpha(\eta, \tau) = 2$. Se $\eta = -1$ e $\tau = 1+\omega$, temos que $\tau - \eta = 2+\omega \equiv -2 \ (mod\ \alpha)$, logo $D_\alpha(\eta, \tau) = 2$. Como $D_\alpha(\eta, \tau) \neq 1$ não existe uma arestas ligando esses vértices.

Dado um grafo $G_\alpha$ com conjunto de vértices $V$ e distância $D_\alpha$, um código em $G_\alpha$ é um subconjunto não vazio $\mathcal{C}$ de $G_\alpha$. A região de Voronoi $V_\eta$, com $\eta \in \mathcal{C}$ é o subconjunto formado pelos elementos de $V$ para os quais $\eta$ é o ponto mais próximo em $\mathcal{C}$, ou seja,

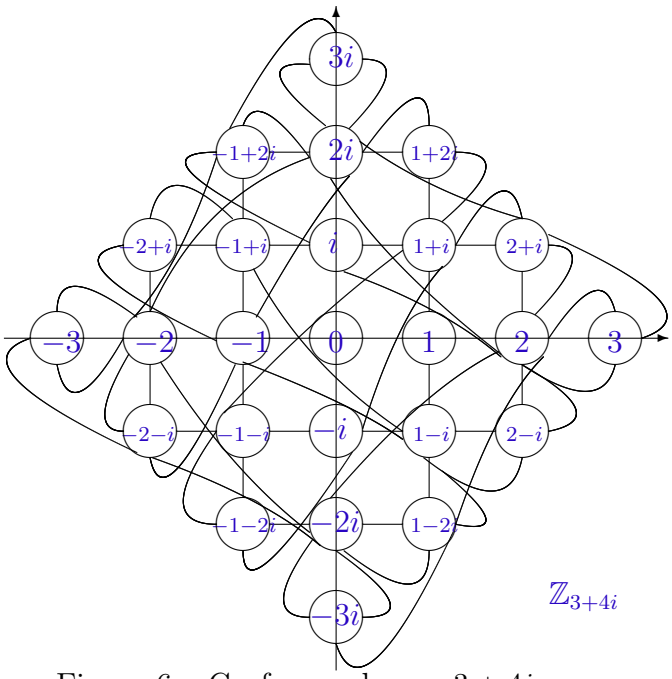


Figura 6 – Grafo gerado por $3 + 4i$.

Fonte: QUEIROZ (2011, p.70)

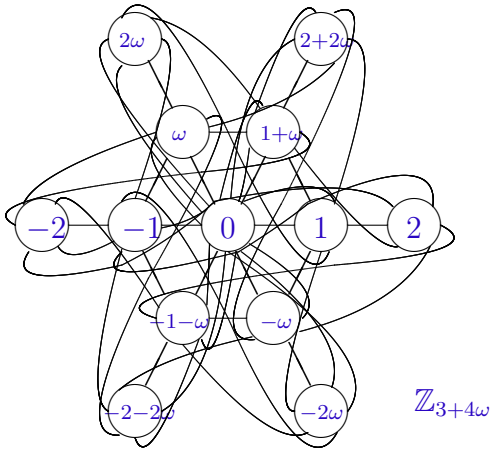


Figura 7 – Grafo gerado por $3 + 4\omega$.

Fonte: QUEIROZ (2011, p.70)

$V_\eta = \{\tau \in V |\ D_\alpha(\eta, \tau) = D_\alpha(\eta, \mathcal{C})\}$. O número $t = max\{D_\alpha(\eta, \mathcal{C})\}$ é chamado raio de cobertura do código. O raio de cobertura é o menor número $t$ tal que as bolas de raio $t$, cujo os centro são pontos do código corretor $\mathcal{C}$, dadas por $B_t(\eta) = \{\tau \in V |\ D_\alpha(\eta, \tau) \leq t\}$ cobrem $V$.

**Definição 42.** Um vértice $\eta$ de um grafo $G$ é dito $t$-dominar outro vértice $\tau$ se $D(\eta, \tau) \leq t$, onde $D$ denota a distância do grafo. Então, um subconjunto $S$ de vértices é chamado um

conjunto $t$-dominante se todo vértice de $G$ é $t$-dominado por um único vértice em $S$.

## 3.2 Códigos Perfeitos

Um código $\mathcal{C}$ é chamado *perfeito* se as bolas de raio $t$ centradas nos pontos de $\mathcal{C}$ particionam o conjunto de pontos $V$, ou seja, é um código que corrige todos os padrões com até t erros e nenhum padrão com $t+1$ erros ou mais. Assim ao recebermos um ponto da constelação de sinal que esta dentro de uma bola de raio $t$, poderemos detecta-lo como um erro e corrigi-lo para o ponto central da bola, que é um ponto do código.

O próximo teorema fornece um procedimento para a obtenção destes conjuntos no caso do anel dos inteiros de Gauss.

**Teorema 3.2.1.** Dado $\alpha \neq 0 \in \mathbb{Z}[i]$ e $t$ um inteiro positivo. Temos que:

1. Se $\beta = t + (t+1)i$ divide $\alpha$, então o ideal $S = [\beta] \subseteq \mathbb{Z}[i]_\alpha$ forma um código perfeito que corrige todos os padrões com até $t$ erros;
2. Se $\overline{\beta} = t - (t+1)i$ divide $\alpha$, então o ideal $S = [\overline{\beta}] \subseteq \mathbb{Z}[i]_\alpha$ forma um código perfeito que corrige todos os padrões com até $t$ erros.

Dado $\beta$, a norma $N(\beta) = 2t^2 + 2t + 1$ resulta no número de pontos da região de Voronoi, a qual chamamos de esfera de Lee de raio $t$, onde cada ponto do grafo é um célula da esfera.

A demonstração do Teorema 3.2.1 pode ser encontrada em [16].

Nos exemplos a seguir serão apresentados códigos perfeito sobre o anel dos inteiros de Gauss.

**Exemplo 47.** Dado $\alpha = 3 + 4i$, temos $N(\alpha) = 3^2 + 4^2 = 25$. Portanto, $\mathbb{Z}[i]_{3+4i}$ tem 25 elementos. Podemos reescrever $\alpha$ como $3 + 4i = (1 - 2i)(-1 + 2i)$, e se tomarmos $\bar{\beta} = 1 - 2i$ temos o gerador do conjunto perfeito t-dominante, assim o ideal $[\bar{\beta}] = [1 - 2i]$ é um conjunto perfeito 1-dominante em $G_{3+4i}$. Portanto, o código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros, possui $N(\alpha)/N(\beta) = \frac{25}{5} = 5$ elementos, é dado por $S = [\bar{\beta}] = \{0, 1 - 2i, -2 - i, 2 + i, -1 + 2i\}$ e é identificado no grafo a seguir pelos pontos que estão duplamente circulados, formando os baricentros dos 5 polígonos fundamentais, com 5 elementos, que recobrem a constelação de sinais, contendo 25 elementos de $\mathbb{Z}_{3+4i}$ (Figura 8).

**Exemplo 48.** Dado $\alpha = 6 + 7i$, temos $N(\alpha) = 6^2 + 7^2 = 85$. Portanto, $\mathbb{Z}[i]_{6+7i}$ tem 85 elementos. Podemos reescrever $\alpha$ como $6 + 7i = (-i)(1 + 2i)(1 + 4i)$, e se tomarmos $\beta = 1 + 2i$ temos o gerador do conjunto perfeito t-dominante, assim o ideal $[\beta] = [1 + 2i]$ é

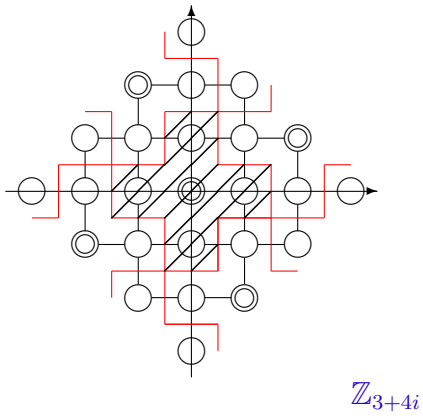


Figura 8 – Código Perfeito 1-dominante em $G_{3+4i}$

Fonte: Autor.

um conjunto perfeito 1-dominante em $G_{6+7i}$. Portanto, o código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros, possui $N(\alpha)/N(\beta) = \frac{85}{5} = 17$ elementos, é dado por $S = [\beta] = \{0, 1+2i, 2+4i, -3-i, -2+i, -1+3i, 5i, -5, -4+2i, -1-2i, -2-4i, 3+i, 2-i, 1-3i, -5i, 5, 4-2i\}$ e é identificado no grafo abaixo pelos pontos que estão duplamente circulados, formando os baricentros dos 17 polígonos fundamentais, com 5 elementos, que recobrem a constelação de sinais, contendo 85 elementos de $\mathbb{Z}_{6+7i}$ (Figura 9).

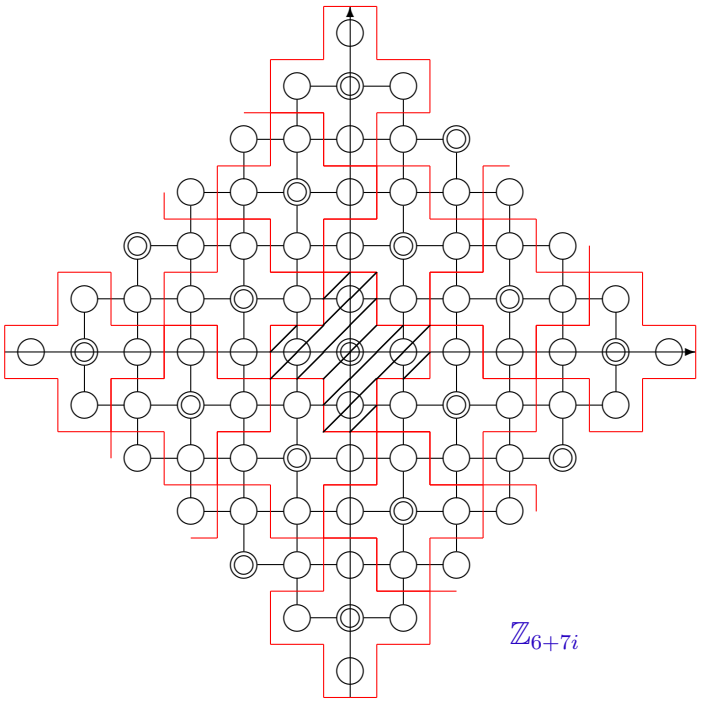


Figura 9 – Código Perfeito 1-dominante em $G_{6+7i}$

Fonte: QUEIROZ (2011, p.72)

Assim como para os inteiros de Gauss, podemos obter um procedimento para o caso do anel dos inteiros de Eisenstein-Jacobi,

**Teorema 3.2.2.** Seja $0 \neq \alpha \in \mathbb{Z}[\omega]$ e $t$ um inteiro positivo. Temos que:

1. Se $\beta = t + (2t+1)\omega$ divide $\alpha$, então o ideal $S = [\beta] \subseteq \mathbb{Z}[\omega]_\alpha$ é um conjunto perfeito $t$-dominante em $G_\alpha$;

2. Se $-\bar{\beta} = (t+1) + (2t+1)\omega$ divide $\alpha$, então o ideal $S = [-\bar{\beta}] = [\bar{\beta}] \subseteq \mathbb{Z}[\omega]_\alpha$ é um conjunto perfeito $t$-dominante em $G_\alpha$.

A demonstração do Teorema 3.2.2 pode ser encontrada em [16].

Dado $\beta$ como definido anteriormente, sua norma $N(\beta) = 3t^2 + 3t + 1$ resulta no número de pontos da região de Voronoi, que agora será vista como hexágonos de raio $t$.

**Exemplo 49.** Dado $\alpha = -8 - 3\omega$, temos $N(\alpha) = (-8)^2 + (-3)^2 - 24 = 49$. Portanto, $\mathbb{Z}[\omega]_{-8-3\omega}$ tem 49 elementos. Podemos reescrever $\alpha$ como $-8-3\omega = (1+3\omega)^2$, e se tomarmos $\beta = 1+3\omega$ obtemos o gerador do conjunto perfeito $t$-dominante. Assim, o ideal $[\beta] = [1+3\omega]$ é um conjunto perfeito 1-dominante em $G_{-8-3\omega}$. Portanto, o código perfeito que corrige todos os padrões com 1 erro e nenhum padrão com 2 ou mais erros, possui $N(\alpha)/N(\beta) = \frac{49}{7} = 7$ elementos, é dado por $S = [\beta] = \{0, 1+3\omega, -3-2\omega, -2+\omega, 2-\omega, 3+2\omega, -1-3\omega\}$

e é identificado no grafo pelos pontos duplamente circulados, formando os baricentros dos 7 polígonos fundamentais,com 7 elementos, que recobrem a constelação de sinais, que contem 49 elementos de $\mathbb{Z}_{-8-3\omega}$ (Figura 10).

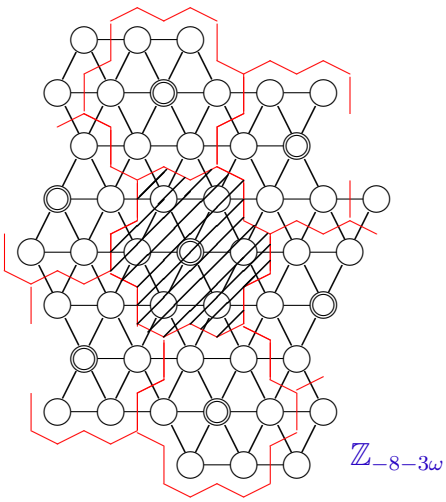


Figura 10 – Código Perfeito 1-dominante em $G_{-8-3\omega}$.

Fonte: QUEIROZ (2011, p.73)

Observe que os procedimentos para obtenção de códigos perfeitos sobre os anéis dos inteiros de Gauss e de Eisenstein-Jacobi são semelhantes e assim podem ser estendidos para outros anéis de inteiros, obtendo novas constelações.

## 3.3 Códigos Quase Perfeitos

Um código é dito *quase-perfeito* se é capaz de corrigir todos os padrões com até $t$ erros e alguns padrões com $t+1$ erros.

Ao escolhermos $\beta = t \pm (t+1)i$ divisor de $\alpha$ obtemos um código perfeito, e a constelação de pontos é coberta por regiões cujo raio de cobertura tem valor máximo $t$, ou seja, as regiões fundamentais são constituídas por esferas de Lee de raio $t$. Portanto, códigos perfeitos são obtidos através de translações de esferas de Lee de raio $t$, e uma esfera de Lee de raio $t$ em $\mathbb{Z}^2$ possui $2t^2+2t+1$ pontos, visto que obtemos o número de pontos da região de Voronoi calculando a norma $N(\beta) = 2t^2+2t+1$. Mas, se tomarmos um $\beta$ divisor de $\alpha$ diferentes dos definidos acima, ou seja $\beta \neq t \pm (t+1)i$ , deixamos de ter um código perfeito, mas obtemos um novo código que cobre a constelação de pontos por regiões fundamentais idênticas, e mantendo as propriedades de um código geometricamente uniforme.

**Teorema 3.3.1.** Seja $\alpha \neq 0 \in \mathbb{Z}[i]$ e $t$ um inteiro positivo. Temos que:

1. Se $\beta = (t-c) + (t+(c+1))i$ divide $\alpha$, então o ideal $S = [\beta] \subseteq \mathbb{Z}[i]_\alpha$ forma um código quase perfeito que corrige todos os padrões com até $t$ erros e $2c^2 + 2c$ padrões com $t+1$ erros em $G_\alpha$;

2. Se $\overline{\beta} = (t-c) - (t+(c+1))i$ divide $\alpha$, então o ideal $S = [\overline{\beta}] \subseteq \mathbb{Z}[i]_\alpha$ forma um código quase perfeito que corrige todos os padrões com até $t$ erros e $2c^2 + 2c$ padrões com $t+1$ erros em $G_\alpha$.

A demonstração do Teorema 3.3.1 pode ser encontrada em [16].

**Exemplo 50.** Dado $\alpha = 6 + 7i$, temos que $N(\alpha) = 6^2 + 7^2 = 85$. Portanto, $\mathbb{Z}[i]_{6+7i}$ possui 85 elementos. Podemos reescrever $\alpha$ como $6 + 7i = (-i)(1 + 2i)(1 + 4i)$. Agora, se tomarmos $\beta = 1 + 4i$ como gerador do ideal, ele tem a forma $\beta = (t-1) + (t+2)i$, e obtemos um código quase-perfeito que corrige todos os padrões com até $t = 2$ erros e $2c^2 + 2c = 2 \cdot 1^2 + 2 \cdot 1 = 4$ padrões com $t + 1 = 3$ erros, pois temos $N(\beta) = 17$ e a maior esfera de Lee contida em 17 pontos possui 13 pontos com raio de cobertura 2 (lembrando que uma esfera de raio Lee possui $2r^2 + 2r + 1$ pontos), logo restam 4 pontos para completarmos os 17. Assim, obtemos uma região de Voronoi que cobre 17 pontos. $S = [\beta]$ tem ordem $N(\alpha)/N(\beta) = \frac{85}{17} = 5$ e o código quase-perfeito, que corrige todos os padrões com 2 erros e 4 padrões com 3 erros, dado por $S = \{0, 1+4i, -4+i, 4-i, -1-4i\}$ é identificado no grafo a seguir pelos pontos que estão duplamente circulados, formando os baricentros dos 5 polígonos fundamentais, com 17 elementos, que recobrem a constelação de sinais, contendo 85 elementos de $\mathbb{Z}_{6+7i}$ (Figura 11).

Assim como para o anel dos inteiros de Gauss, se tomarmos $\beta = t + (2t+1)\omega$ ou $\beta = (t+1) + (2t+1)\omega$, divisor de $\alpha$, obtemos um código perfeito, e a constelação de pontos é coberta por regiões de Voronoi cujo raio de cobertura tem valor no máximo $t$, ou seja, as regiões de Voronoi são agora constituídas por hexágonos de raio $t$. Portanto os códigos perfeitos são obtidos através de translações de hexágonos de raio $t$, onde $t \leq r$, e um hexágono de raio $r$ possui $3r^2 + 3r + 1$ pontos. Mas, se tomarmos $\beta$ divisor de $\alpha$ diferente dos definidos para códigos perfeitos, obtemos um novo código, não mais perfeito, mas que cobre a constelação de pontos por regiões de Voronoi idênticas, e mantendo as propriedades de um código geometricamente uniforme.

**Teorema 3.3.2.** Seja $0 \neq \alpha \in \mathbb{Z}[\omega]$ e $t$ um inteiro positivo. Temos que:

1. Se $\beta = (t + 2c + 1) + (2t+1)\omega$ ou $\beta = (t-2c) + (2t+1)\omega$ divide $\alpha$, então o ideal $S = [\beta] \subseteq \mathbb{Z}[\omega]_\alpha$ forma um código quase-perfeito que corrige todos os padrões com até $t$ erros e $4c^2 + 2c$ padrões com $t+1$ erros em $G_\alpha$;

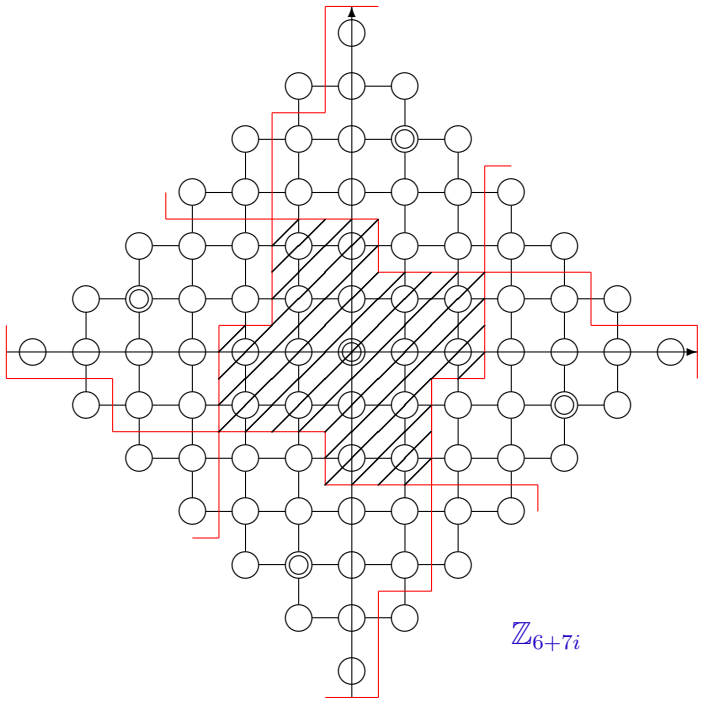


Figura 11 – Código quase perfeito sobre $\mathbb{Z}_{6+7i}$

Fonte: QUEIROZ (2011, p.75)

2. Se $\bar{\beta} = (t+2c) + (2t+1)\omega$ ou $\beta = (t-2c+1) + (2t+1)\omega$ divide $\alpha$, então o ideal $S = [\bar{\beta}] \subseteq \mathbb{Z}[\omega]_\alpha$ forma um código quase-perfeito capaz de corrigir todos os padrões com até $t$ erros e $4c^2 - 2c$ padrões com $t+1$ erros em $G_\alpha$.

A demonstração do Teorema 3.3.2 pode ser encontrada em [16].

**Exemplo 51.** Dado $\alpha = -5+2\omega$, temos que $N(\alpha) = (-5)^2+2^2-[(-5)\cdot 2] = 39$. Portanto, $\mathbb{Z}_{-5+2\omega}$ tem 39 elementos. Podemos reescrever $\alpha$ como $-5+2\omega = (1+2\omega)(3+4\omega)$ e se tomarmos $\beta = 3+4\omega$ como gerador do ideal, ele tem a forma de $\beta = (t+2+1)+(2t+1)\omega$, e obtemos um código quase perfeito que corrige todos os padrões com $t = 1$ erro e $4c^2+2c = 6$ padrões com 2 erros, visto que $N(\beta) = 13$ resulta no número de pontos da região de Voronoi, que neste caso são os hexágonos de raio $t$, e o maior hexágono contido em 13 pontos possui 7 pontos com raio de cobertura 1, logo restam 6 pontos para completarmos os 13. Assim, obtemos uma região de Voronoi que cobre 13 pontos. $S = [\beta]$ tem ordem $N(\alpha)/N(\beta) = \frac{39}{13} = 3$ e o código quase perfeito, que corrige todos os padrões com 1 erro e 6 padrões com 2 erros, dado por $S = \{0, 3+4\omega, -3-4\omega\}$ é identificado no grafo pelos pontos duplamente circulados, formando os baricentros dos 3 polígonos fundamentais, com 13 elementos, que recobrem a constelação de sinais, contendo 39 elementos de $\mathbb{Z}_{-5+2\omega}$ (Figura 12).

Observe que se tomarmos $c = 0$ nos Teoremas 3.3.1 e 3.3.2 obtemos $\beta$ como definido

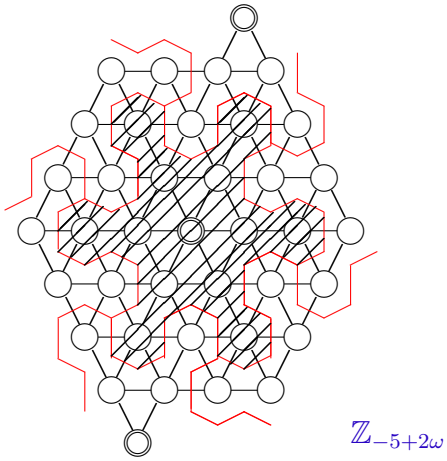


Figura 12 – Código quase perfeito sobre $\mathbb{Z}_{-5+2\omega}$.

Fonte: QUEIROZ (2011, p.79)

para códigos perfeitos nos Teoremas 3.2.1 e 3.2.2 . Assim, temos que os códigos perfeitos são um caso particular dos códigos quase-perfeitos. Mais ainda, assim como para os códigos perfeitos, os procedimentos adotados para a obtenção dos códigos perfeitos sobre anéis de inteiros de Gauss e de Eisenstei-Jacobi podem ser facilmente estendidos para outros tipos de anéis, obtendo assim formas para a construção de outros códigos quase-perfeitos sobre novas constelações de sinais.

# 4 Conclusão

Neste trabalho foram estudados conceitos fundamentais de álgebra, o que permitiu relembrar diversos conceitos trabalhado no decorrer do curso. Também foram apresentados conceitos sobre grafos, códigos corretores e códigos geometricamente uniformes, mais especificadamente códigos perfeitos e quase-perfeitos, com um foco principal desses códigos sobre os anéis de inteiros Gaussianos e de Einsentein-Jacobi.

Comparando os resultados obtidos, vimos que ambos os códigos são geometricamente uniformes, mas os códigos quase-perfeitos são capazes de corrigir mais erros que os códigos perfeitos, porém o número de vértices obtidos é menor que nos códigos perfeitos. Além disso vimos que os códigos perfeitos são um caso particular dos códigos quase-perfeitos, conforme apresentado por [6].

O estudo dos códigos corretores de erros contribuiu para a complementação na formação matemática da discente, possibilitando a sua aproximação da área matemática de interesse, além de maiores condições para prosseguir com a formação acadêmica na área almejada. Além disso, este trabalho pode servir como base para outros estudantes, em nível de graduação, que também se interessem pela área.

# Referências

1 SHANNON, C. E. A Mathematical Theory of Communication, **The Bell System Technical Journal**, v. 27, p. 379-423, 1948. Citado na página 15.

2 SLEPIAN, D. Group Codes for the Gaussian Channel, **The Bell System Technical Journal**, v. 37, p. 575-602, 1968. Citado na página 15.

3 FORNEY, G. D. Geometrically Uniform Codes. **IEEE Trans. On Inform. Theory**, v.37 N.5, p. 1241-1260, 1991 Citado na página 15.

4 UNGERBOECK, G.Trellis Coded Modulation with redundadat signal sets - Part I: Introduction. **IEEE Communications Magazine**, v. 25 n. 2, 1987. Citado na página 15.

5 MARTÍNEZ, C., BEIVIDE, R., GABIDULIN, E. Perfect codes from metrics induced by circulant graphs, **IEEE Trans. On Inform. Theory**, v. 53 n. 9, p. 3042-3052, 2007. Citado na página 15.

6 QUILLES, C., PALAZZO, R. Quasi-perfect geometrically uniform codes derived from graphs over Gaussian integer rings, **Proc. IEEE Intl. Symp. Information Theory**, Austin, Texas, U.S.A. p. 1158-1162, 2010. Citado 4 vezes nas páginas 15, 16, 65 e 75.

7 QUILLES QUEIROZ, C., CAMARERO, C., MARTÍNEZ, C, PALAZZO JR, R. Quasi-Perfect Codes from Cayley Graphs over Integer Rings, **IEEE Trans. On Inform. Theory**, v. 59 n. 9, p. 5905-5916, 2013. Citado 3 vezes nas páginas 15, 16 e 65.

8 MILIES, C. P. **Breve introdução à Teoria dos Códigos Corretores de Erros**.Colóquio de Matemática da Região Centro-Oeste, 2009. Citado na página 16.

9 NOGUEIRA, J. A. P. **Aplicações Matemáticas em Códigos Corretores de Erros**. 2019. 81f. Dissertação (Mestrado em Matemática) - Programa de Pós Graduação em Matemática, Universidade Federal do Cariri, Juazeiro do Norte, 2019. Citado na página 16.

10 DOMINGUES, H. H., IEZZI, G. **Álgebra moderna**. 4. ed. ref. São Paulo: Atual, 2003. Citado 4 vezes nas páginas 16, 17, 20 e 28.

11 DIAS, I. **Teoria de Anéis - Notas de Aulas**, ICMC - USP, 2001, Disponível em: <https://sites.icmc.usp.br/iresdias/material/sma306.pdf> Citado 2 vezes nas páginas 16 e 17.

12 SAMUEL, P. **Algebraic Theory of Numbers**, Herman, Paris, 1967. Citado 3 vezes nas páginas 16, 17 e 56.

13 FEOFILOFF, P., KOHAYAKAWA, Y., WAKABAYASHI, Y. **Uma Introdução Sucinta à Teoria dos Grafos**. SBM, 2011. Citado na página 16.

14 MELO, G. S. de. **Introdução à Teoria dos Grafos**. Tese(Doutorado em Engenharia Elétrica)- Mestrado Profissional em Matemática em Rede Nacional PROFMAT, Universidade Federal da Paraíba. Paraíba, p. 1-6. 2014. Citado na página 16.

15 ALBUQUERQUE, C. D. **Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais**. 2009. 139f. Tese (Doutorado em Engenharia Elétrica)- Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, São Paulo, 2009. Citado 3 vezes nas páginas 16, 63 e 64.

16 QUEIROZ, C. R. O. Q. **Códigos geometricamente uniformes derivados de grafos sobre anéis quocientes de inteiros e de ordens dos quatérnios**. 2011. 108 p. Tese (doutorado) - Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, 2011. Citado 7 vezes nas páginas 16, 55, 65, 68, 70, 72 e 73.