Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

A Transformada Discreta de Fourier no Círculo Finito $\mathbb{Z}/n\mathbb{Z}$ [†]

por

Antonio Pereira de Farias Filho

sob orientação do

Prof. Dr. Napoleón Caro Tuesta

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

agosto/2016
João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

F224t Farias Filho, Antonio Pereira de.
A Transformada Discreta de Fourier no círculo finito $\mathbb{Z}/n\mathbb{Z}$ / Antonio Pereira de Farias Filho.- João Pessoa, 2016.
89f.
Orientador: Napoleón Caro Tuesta
Dissertação (Mestrado) - UFPB/CCEN
1. Matemática. 2. Transformada Discreta de Fourier. 3. Anel quociente $\mathbb{Z}/n\mathbb{Z}$ 4. Convolução de funções discretas. 5. Raízes primitivas.

UFPB/BC CDU: 51(043)

A Transformada Discreta de Fourier no Círculo Finito $\mathbb{Z}/n\mathbb{Z}$

por

Antonio Pereira de Farias Filho

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática.

Aprovada por:

Prof. Dr. Napoleón Caro Tuesta -UFPB (Orientador)

Luis A. Alba S.

Prof. Dr. Luis Alberto Alba Sarria - Universidad del Valle, Colômbia

Prof. Dr. Bruno Henrique Carvalho Ribeiro - UFPB

agosto/2016

Agradecimentos

Quero agradecer à todos que me ajudaram a concluir esta jornada, principalmente ao Prof. Dr. Napoleón Caro Tuesta, por ter aceitado o convite para minha orientação e me ajudado a trabalhar esse tema maravilhoso. Faço um agradecimento especial à minha família e amigos por sempre estarem comigo em todos os momentos, sobretudo ao meus pais, Antonio Pereira de Farias e Terezinha Lopes de Farias, por terem me ensinado e ser homem, ao meu filho Alfredo René da Silva Farias e minha esposa Patriciane do Ramo da Silva Farias, por estarem iluminando minha vida a cada dia que se passa.

Dedicatória

Em memória de Severino Ramos de Arruda.

⋆ *05/09/1967*
† *10/03/2015*

Resumo

Faremos, aqui, um estudo teórico sobre a Transformada Discreta de Fourier no círculo finito $\mathbb{Z}/n\mathbb{Z}$. Nosso principal objetivo é verificar se podemos obter propriedades análogas às encontradas nas transformadas de Fourier para o caso contínuo. Nesse trabalho mostraremos que $\mathbb{Z}/n\mathbb{Z}$ tem uma estrutura de anel, dando condições para o desenvolvimento de temas bastante discutidos na Aritmética como, por exemplo, o Teorema Chinês do Resto, função Phi de Euler e raízes primitivas, temas estes que serão tratados no primeiro capítulo. O assunto principal desse estudo é desenvolvido no segundo capítulo, onde definiremos o espaço $L^2(\mathbb{Z}/n\mathbb{Z})$ e provaremos que este é um espaço vetorial com produto interno, dimensão finita e uma base ortonormal. Tal fato será de extrema importância quando estivermos determinando a matriz e demonstrando as propriedades da transformada discreta de Fourier. Também faremos interpretações geométricas do Teorema Chinês do Resto e do círculo finito $\mathbb{Z}/n\mathbb{Z}$ assim como daremos a representação gráfica da DFT de algumas funções que calcularemos. Durante o desenvolvimento desse estudo faremos uso recorrente de definições e resultados tratados na Aritmética, Álgebra e Álgebra Linear.

Palavras-chave: Transformada Discreta de Fourier, Anel Quociente $\mathbb{Z}/n\mathbb{Z}$, Convolução de Funções Discretas, Raízes Primitivas, Grupos Cíclicos.

Abstract

We will do here a theoretical study of the Discrete Fourier Transform on the finite circle $\mathbb{Z}/n\mathbb{Z}$. Our main objective is to see if we can get properties analogous to those found in the Fourier transform for the continuous case. In this work we show that $\mathbb{Z}/n\mathbb{Z}$ has a ring structure, providing conditions for the development of extensively discussed topics in arithmetic, for example, The Chinese Remainder Theorem, Euler's Phi Function and primitive roots, themes these to be dealt with in first chapter. The main subject of this study is developed in the second chapter, which define the space $L^2(\mathbb{Z}/n\mathbb{Z})$ and prove that this is a finite-dimensional inner product vector space, with an orthonormal basis. This fact is of utmost importance when we are determining the matrix and demonstrating the properties of the discrete Fourier transform. We will also make geometric interpretations of the Chinese Remainder Theorem and the finite circle $\mathbb{Z}/n\mathbb{Z}$ as well as give a graphical representation of the DFT of some functions that calculate. During the development of this study we will make recurrent use of definitions and results treated in Arithmetic, Algebra and Linear Algebra.

Keywords: Discrete Fourier Transform, Quotient Ring $\mathbb{Z}/n\mathbb{Z}$, Discrete Convolution Functions, Primitive Roots, Cyclic Groups.

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

No início do século XIX, Fourier publicou um trabalho sobre propagação de calor que mudou a visão dos matemáticos sobre o conceito de função. Ele tentou solucionar o problema para provar que qualquer função definida em um intervalo poderia ser representada por uma série de senos e cossenos, dando origem ao campo de pesquisa da matemática que conhecemos, hoje, como Análise de Fourier. Nesse campo de pesquisa damos uma atenção especial às séries e as transformadas de Fourier.

Uma transformada de Fourier é um operador linear que expressa uma função dada em termos de senos e cossenos. O caso mais conhecido é o da Transformada de Fourier para funções contínuas. Nesse caso, a transformada de Fourier de uma função integrável $f(x)$ qualquer é dada por

$$F(y) = \int_{-\infty}^{+\infty} f(t)e^{-iyt}dt.$$

A transformada definida acima tem algumas propriedades interessantes tais como: inversão, linearidade, convolução, similaridade, teorema de Parseval, translações, dilatações, derivação, etc., e tais vantagens são aplicadas quando tratamos de fenômenos ocorridos em universos infinitos e contínuos.

Na prática, muitos problemas são dados em universos discretos e finitos, e nosso trabalho tem como principal objetivo apresentar uma alternativa para representar funções discretas em termos de seno e cosseno. Estaremos tratando, exclusivamente da Transformada Discreta de Fourier no círculo finito $\mathbb{Z}/n\mathbb{Z}$, pois, além de $\mathbb{Z}/n\mathbb{Z}$ ser um conjunto mais fácil de manipular, esse caso é o que apresenta mais aplicações práticas, como por exemplo, na Teoria dos Números, processamento de sinais, processamento de imagens, na Teoria da Informação, na engenharia, criptografia, etc.

Assumindo que também é possível definir a transformada de Fourier para funções discretas, algumas questões importantes surgem sobre esse assunto: quais as principais propriedades da transformada discreta de Fourier em $\mathbb{Z}/n\mathbb{Z}$? Será que essas propriedades são análogas às do caso contínuo? É possível obter propriedades equivalentes para funções definidas em estruturas algébricas mais gerais?

Esse estudo tem como foco, responder às duas primeiras questões do parágrafo anterior e dar condições para que possamos refletir sobre a última.

No primeiro capítulo desse trabalho, estaremos interessados em construir uma estrutura algébrica para $\mathbb{Z}/n\mathbb{Z}$ de modo que possamos mostrar resultados importantes sobre a Teoria dos Números. Enunciaremos e demonstraremos o Teorema Chinês do Resto e apresentaremos uma interpretação geométrica para um dado sistema de congruência lineares. Também apresentaremos o subgrupo $(\mathbb{Z}/n\mathbb{Z})^*$ das unidades de $\mathbb{Z}/n\mathbb{Z}$, a partir de onde definiremos a Função Phi de Euler. Falaremos sobre grupos cíclicos e raízes primitivas antes de encerrar o capítulo apresentando uma pequena aplicação sobre criptografia de chaves públicas.

O segundo capítulo tratará da Transformada discreta de Fourier no círculo $\mathbb{Z}/n\mathbb{Z}$. Iniciaremos estabelecendo uma base ortonormal para o espaço de funções $L^2(\mathbb{Z}/n\mathbb{Z})$. Em seguida, falaremos um pouco sobre convolução de funções e suas propriedades. A partir daí, teremos as ferramentas necessárias para dar a definição de Transformada Discreta de Fourier (DFT), determinar uma matriz para essa transformada e demonstrar suas principais propriedades. Para algumas dessas propriedades, estaremos apresentando mais de uma demonstração. Finalizaremos o segundo capítulo calculando as transformadas de Fourier para algumas funções e mostrando as respectivas representações gráficas.

Para um entendimento mais eficiente do que iremos expor, são necessários alguns conhecimentos prévios sobre Aritmética, Álgebra e Álgebra Linear. Por esse motivo, resolvemos enunciar alguns conceitos e resultados sobre tais assuntos nos apêndices A, B e C. Alguns dos resultados lá enunciados têm suas demonstrações omitidas pois supomos que tais conhecimentos já tenham sido adquiridos previamente.

Como veremos adiante, $\mathbb{Z}/n\mathbb{Z}$ é um grupo aditivo cíclico de ordem n e isomorfo ao grupo multiplicativo das raízes n-ésimas da unidade complexa. Com isso $\mathbb{Z}/n\mathbb{Z}$ pode ser representado como pontos igualmente espaçados sobre um círculo de raio 1. Também podemos interpretar o anel quociente $\mathbb{Z}/n\mathbb{Z}$ como sendo um produto de gráficos cíclicos, obtendo, assim, o Toro Finito.

A Transformada Discreta de Fourier é calculada sempre que se faz necessário escrever uma série de Fourier clássica de senos e cossenos. Na prática a DFT exprime uma função temporal como a soma de funções sinusoidais, ou seja, em termo de suas frequências. Provavelmente a primeira aplicação da DFT foi feita por Alexis Claude de Clairaut, em 1754, para calcular uma órbita, que pode ser considerada como uma série de Fourier finita de cossenos.

Capítulo 1

Congruências e o Anel Quociente dos Inteiros mod n

Neste capítulo faremos uma breve revisão de alguns tópicos tratados na Teoria Elementar dos Números. Falaremos um pouco sobre congruências mod n e apresentaremos algumas propriedades importantes do anel quociente $\mathbb{Z}/n\mathbb{Z}$. Iremos demonstrar o Teorema Chinês do Resto e faremos algumas aplicações. Apresentaremos certas propriedades importantes da função Phi de Euler. Expressaremos o conceito de Raízes Primitivas, a partir do qual provaremos alguns resultados interessantes e mostraremos uma breve aplicação dos conteúdos estudados na criptografia.

1.1 Congruências

Iniciaremos nossos estudos revendo o conceito de congruência mod n e definindo as operações de adição e multiplicação no anel $\mathbb{Z}/n\mathbb{Z}$. Para um melhor entendimento destes temas é necessário o conhecimento de algumas noções básicas de Aritmética como, por exemplo, divisibilidade de inteiros, divisão euclidiana e unicidade da fatoração de inteiros em números primos. Algumas dessas noções básicas serão apresentadas no Apêndice A e também podem ser consultadas nas Referências Bibliográficas [2], [3] e [4].

Definição 1.1 *Seja n um número inteiro positivo. Dados $a, b \in \mathbb{Z}$, dizemos que a é* congruente *a b módulo n, e escrevemos $a \equiv b \pmod{n}$, se $n \mid a - b$.*

Observação 1.1 *Os seguintes itens são equivalentes à Definição 1.1.*

(a) $a \equiv b \pmod{n} \Leftrightarrow a - b = kn,\ k \in \mathbb{Z}$;

(b) $a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z} =$ *o ideal dos inteiros múltiplos de n;*

(*c*) $a \equiv b \pmod{n} \Leftrightarrow$ *a e b deixam o mesmo resto quando são divididos por n.*

Para que sejamos mais rigorosos, devemos mostrar que a nossa definição para congruência de números inteiros mod n faz sentido. A Proposição 1.1 nos garante que a congruência módulo n é uma relação de equivalência em $\mathbb{Z}$.

Proposição 1.1 *Para quaisquer* $a,\ b,\ c \in \mathbb{Z}$ *e* $n \in \mathbb{Z}^+$ *temos:*

(a) $a \equiv a \pmod{n}$ (reflexividade);

(b) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (simetria);

(c) $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (transitividade).

Demonstração: Suponhamos que a, b, c e n sejam inteiros quaisquer com $n > 0$.

(a) Como $a - a = 0$, temos que $n \mid a - a \Rightarrow a \equiv a \pmod{n}$.

(b) Se $a \equiv b \pmod{n}$ então

$$n \mid a - b \Rightarrow n \mid -(a - b) \Rightarrow n \mid b - a,$$

logo, $b \equiv a \pmod{n}$.

(c) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então

$$n \mid a - b \text{ e } n \mid b - c \Rightarrow n \mid (a - b) + (b - c) \Rightarrow n \mid a - c,$$

portanto, $a \equiv c \pmod{n}$. ∎

Os elementos do conjunto quociente $\mathbb{Z}/n\mathbb{Z}$ são, por definição, as classes de equivalência módulo n, ou seja, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ onde

$$\begin{aligned} \bar{a} &= \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} \\ &= \{x \in \mathbb{Z} \mid x - a \text{ é múltiplo de } n\} \\ &= \{x = a + kn \mid k \in \mathbb{Z}\}. \end{aligned}$$

Neste contexto, quando dois números inteiros são congruentes módulo n, podemos considerá-los como sendo o mesmo objeto. Além disso, podemos fazer uma correspondência injetora entre o conjunto quociente $\mathbb{Z}/n\mathbb{Z}$ e $\{0, 1, 2, \cdots, n-1\} \subset \mathbb{Z}$. Note que, aqui, nós equiparamos 0 com qualquer inteiro múltiplo de n. Assim podemos interpretar geometricamente o anel $\mathbb{Z}/n\mathbb{Z}$ como sendo a reta inteira contornando um círculo infinitas vezes, como mostra a Figura 1.1. Desse modo, podemos considerar $\mathbb{Z}/n\mathbb{Z}$ como sendo um círculo finito.

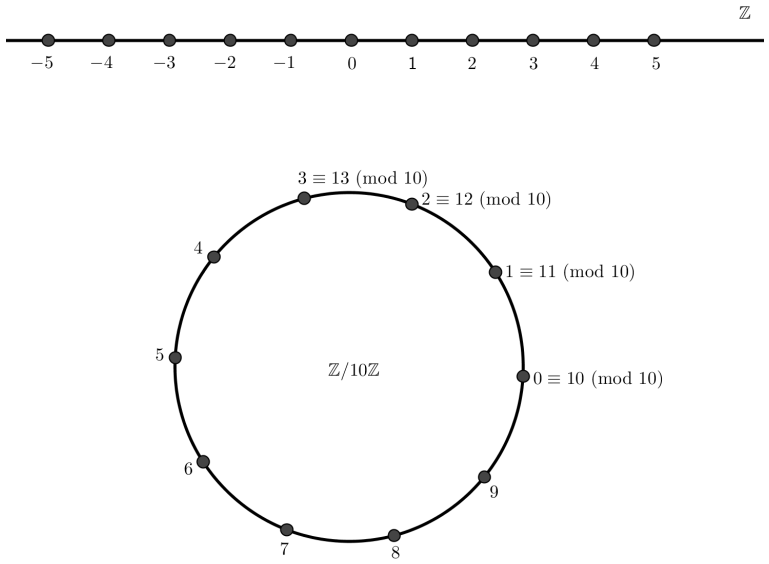

Figura 1.1: Reta inteira contornando o círculo finito.

É possível utilizar outros conjuntos de representantes para $\mathbb{Z}/n\mathbb{Z}$ como, por exemplo, $\{1, 2, 3, \cdots, n\}$ ou $\{-n, -n+1, \cdots, -2, -1\}$. Na verdade, podemos substituir qualquer representante j por $j + an$, onde a é um inteiro qualquer, pois $j \equiv j+an \pmod{n}$. De modo geral, $\{a_1 n,\ 1+a_2 n,\ 2+a_3 n,\ \cdots,\ (n-1)+a_n n\}$ é um conjunto de representantes de $\mathbb{Z}/n\mathbb{Z}$, para qualquer subconjunto $\{a_1, a_2, a_3, \cdots, a_n\}$ de $\mathbb{Z}$.

Definiremos as operações de adição e multiplicação em $\mathbb{Z}/n\mathbb{Z}$ aplicando as operações usuais $+$ e $\cdot$ de $\mathbb{Z}$ e, em seguida, considerando o resto da divisão dos compostos $x + y$ e $x \cdot y$ por n, para qualquer par de elementos $x, y \in \mathbb{Z}/n\mathbb{Z}$. Sendo $\mathbb{Z}/n\mathbb{Z}$ um conjunto finito, é possível escrever as tábuas da adição e multiplicação. Para tanto, devemos posicionar os compostos $i + j$ e $i \cdot j$ nas células pertencentes à i-ésima linha e j-ésima coluna das tábuas da adição e multiplicação, respectivamente.

A Proposição 1.2, abaixo, garante a boa definição das operações de adição e multiplicação em $\mathbb{Z}/n\mathbb{Z}$.

Proposição 1.2 *Sejam $a,\ b,\ c,\ d \in \mathbb{Z}$ e n um número inteiro positivo. Se*

$$a \equiv b \pmod{n} \text{ e } c \equiv d \pmod{n}$$

então

$$a + c \equiv b + d \pmod{n} \text{ e } a \cdot c \equiv b \cdot d \pmod{n}.$$

Demonstração: Suponhamos que $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, ou seja, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a-b = k_1 n$ e $c-d = k_2 n$. Para provar que $a+c \equiv b+d \pmod{n}$ e $a \cdot c \equiv b \cdot d \pmod{n}$ mostraremos que existem $q_1, q_2 \in \mathbb{Z}$ tais que $(a+c)-(b+d) = q_1 n$ e $a \cdot c - b \cdot d = q_2 n$. De fato

$$\begin{aligned} (a+c)-(b+d) &= k_1 n + k_2 n = (k_1+k_2)n \\ &= q_1 n, \text{ onde } k_1 + k_2 = q_1 \in \mathbb{Z} \\ &\Rightarrow a + c \equiv b + d \pmod{n}. \end{aligned}$$

De modo análogo, como $c - d = k_2 n \Rightarrow c = d + k_2 n$, temos

$$\begin{aligned} a \cdot c - b \cdot d &= a \cdot (d + k_2 n) - b \cdot d = ad + ak_2 n - bd = (a-b)d + ak_2 n \\ &= k_1 nd + ak_2 n = (ak_2 + dk_1)n \\ &= q_2 n, \text{ onde } ak_2 + dk_1 = q_2 \in \mathbb{Z} \\ &\Rightarrow a \cdot c \equiv b \cdot d \pmod{n}. \end{aligned}$$

Concluímos, assim, a demonstração. ■

Exemplo 1.1 *Vamos construir a tábua da adição em* $\mathbb{Z}/5\mathbb{Z}$.

Já sabemos que $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, *onde*

- $\overline{0} = \{5k \mid k \in \mathbb{Z}\} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$;
- $\overline{1} = \{1 + 5k \mid k \in \mathbb{Z}\} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$;
- $\overline{2} = \{2 + 5k \mid k \in \mathbb{Z}\} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$;
- $\overline{3} = \{3 + 5k \mid k \in \mathbb{Z}\} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$;
- $\overline{4} = \{4 + 5k \mid k \in \mathbb{Z}\} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$.

Observe que, neste caso,

$$\overline{5} = \{5 + 5k \mid k \in \mathbb{Z}\} = \{5(k+1) \mid k \in \mathbb{Z}\} = \{5K \mid k + 1 = K \in \mathbb{Z}\} = \overline{0}$$

e também que $\overline{6} = \overline{1}$, $\overline{7} = \overline{2}$, $\overline{8} = \overline{3}$, *etc. Em* $\mathbb{Z}/5\mathbb{Z}$ *temos, por exemplo, temos que:*

- $\overline{0} + \overline{2} = \overline{2}$;
- $\overline{3} + \overline{1} = \overline{4}$;
- $\overline{4} + \overline{3} = \overline{7} = \overline{2}$, *pois o resto da divisão de* 7 *por* 5 *é* 2;
- $\overline{3} + \overline{3} = \overline{6} = \overline{1}$, *já que* $6 \equiv 1 \pmod{5}$.

A Tabela 1.1 representa a operação de adição em $\mathbb{Z}/5\mathbb{Z}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Tabela 1.1: Adição em $\mathbb{Z}/5\mathbb{Z}$.

Exemplo 1.2 *Construiremos, agora, a tábua da multiplicação em* $\mathbb{Z}/8\mathbb{Z}$*. Procederemos de modo análogo ao Exemplo 1.1.*

Sabemos que $\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$*, onde*

- $\overline{0} = \{8k \mid k \in \mathbb{Z}\} = \{\ldots, -24, -16, -8, 0, 8, 16, 24, \ldots\}$;
- $\overline{1} = \{1 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -23, -15, -7, 1, 9, 17, 25, \ldots\}$;
- $\overline{2} = \{2 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -22, -14, -6, 2, 10, 18, 26, \ldots\}$;
- $\overline{3} = \{3 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -21, -13, -5, 3, 11, 19, 27, \ldots\}$;
- $\overline{4} = \{4 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -20, -12, -4, 4, 12, 20, 28, \ldots\}$;
- $\overline{5} = \{5 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -19, -11, -3, 5, 13, 21, 29, \ldots\}$;
- $\overline{6} = \{6 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -18, -10, -2, 6, 14, 22, 30, \ldots\}$;
- $\overline{7} = \{7 + 8k \mid k \in \mathbb{Z}\} = \{\ldots, -17, -9, -1, 7, 15, 23, 31, \ldots\}$.

Observe que, neste caso,

$$\overline{8} = \{8 + 8k \mid k \in \mathbb{Z}\} = \{8(k+1) \mid k \in \mathbb{Z}\} = \{8K \mid k + 1 = K \in \mathbb{Z}\} = \overline{0}$$

e também que $\overline{9} = \overline{1}$*,* $\overline{10} = \overline{2}$*,* $\overline{11} = \overline{3}$*, etc. Desse modo obtemos, em* $\mathbb{Z}/8\mathbb{Z}$*:*

- $\overline{0} \cdot \overline{6} = \overline{0}$;
- $\overline{7} \cdot \overline{1} = \overline{7}$;
- $\overline{3} \cdot \overline{2} = \overline{6}$;
- $\overline{4} \cdot \overline{5} = \overline{20} = \overline{4}$*, pois o resto da divisão de* 20 *por* 8 *é* 4;
- $\overline{7} \cdot \overline{7} = \overline{49} = \overline{1}$*, já que* $49 \equiv 1 \pmod 8$.

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{6}$	$\bar{6}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tabela 1.2: Multiplicação em $\mathbb{Z}/8\mathbb{Z}$.

A Tabela 1.2 representa a operação de multiplicação em$\mathbb{Z}/8\mathbb{Z}$.

Observação 1.2 *Em muitas situações desse estudo, estaremos denotando a classe de equivalência $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ simplesmente por seu representante $a \in \mathbb{Z}$. O contexto deixará claro se a representará um número inteiro ou uma classe de $\mathbb{Z}/n\mathbb{Z}$. Nos casos extremos, para evitar confusão, podemos representar a classe $\overline{a}$ por $a \bmod n$.*

As operações de adição e multiplicação que definimos em $\mathbb{Z}/n\mathbb{Z}$ possuem as seguintes propriedades, para quaisquer $x, y, z \in \mathbb{Z}/n\mathbb{Z}$:

- $(x + y) + z = x + (y + z)$ (a adição é associativa em $\mathbb{Z}/n\mathbb{Z}$);
- $x+0 = 0+x$, para todo $x \in \mathbb{Z}/n\mathbb{Z}$ (0 é o elemento neutro da adição em $\mathbb{Z}/n\mathbb{Z}$);
- Para todo $x \in \mathbb{Z}/n\mathbb{Z}$, existe $-x \in \mathbb{Z}/n\mathbb{Z}$ tal que $x + (-x) = -x + x = 0$ (todo elemento de $\mathbb{Z}/n\mathbb{Z}$ possui inverso aditivo);
- $x + y = y + x$ (a adição é comutativa em $\mathbb{Z}/n\mathbb{Z}$);
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (a multiplicação é associativa em $\mathbb{Z}/n\mathbb{Z}$);
- $x \cdot 1 = 1 \cdot x$, para todo $x \in \mathbb{Z}/n\mathbb{Z}$ (1 é o elemento neutro da multiplicação em $\mathbb{Z}/n\mathbb{Z}$);
- $x \cdot y = y \cdot x$ (a multiplicação é comutativa em $\mathbb{Z}/n\mathbb{Z}$);
- $x \cdot (y+x) = x \cdot y + x \cdot z$ e $(y+z) \cdot x = y \cdot x + z \cdot x$ (a multiplicação é distributiva com relação a adição em $\mathbb{Z}/n\mathbb{Z}$).

As propriedades supracitas são consequências imediatas das operações usuais + e $\cdot$ de $\mathbb{Z}$ podendo-se, assim, omitir suas demonstrações. Essas propriedades nos dizem que $\mathbb{Z}/n\mathbb{Z}$ é um anel comutativo com unidade. Consequentemente, $\mathbb{Z}/n\mathbb{Z}$ é

um grupo cíclico aditivo gerado por 1, uma vez que qualquer elemento deste grupo é múltiplo de 1.

Um anel é um conjunto fechado para a adição, subtração e multiplicação mas nem sempre é possível efetuar divisões utilizando as leis habituais tratadas na álgebra. Em outras palavras, nem sempre é possível garantir que todos os elementos não nulos de um anel têm inverso multiplicativo.

O conjunto $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\} = \{1, 2, 3, \cdots, n-1\}$ é um grupo multiplicativo quando todos os seus elementos admitem inverso. A Teorema 1.1 nos mostra em quais condições $\mathbb{Z}/n\mathbb{Z}$ é um grupo multiplicativo. Porém, antes de apresentarmos este teorema vamos relembrar um conceito muito importante. Um anel comutativo com unidade K é denominado um *corpo* se todo elemento não nulo de K possuir inverso multiplicativo.

Teorema 1.1 *O anel $\mathbb{Z}/n\mathbb{Z}$ é um corpo se, e somente se n é um número inteiro primo.*

Demonstração:

($\Rightarrow$) Inicialmente provaremos que se n é um inteiro primo então $\mathbb{Z}/n\mathbb{Z}$ é um corpo. Seja n um inteiro primo positivo. Como $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$ é um anel comutativo com unidade 1, para $\mathbb{Z}/n\mathbb{Z}$ ser um corpo, basta que todos os seus elementos não nulos tenham inverso multiplicativo. Seja $a \in \mathbb{Z}/n\mathbb{Z}$ tal que $a \not\equiv 0 \pmod{n}$. Assim, temos que $1 \leq a \leq n-1$. Sendo n primo, m.d.c.$(a, n) = 1$ e, daí, existem inteiros x, y tais que

$$xa + yn = 1.$$

Como $yn \equiv 0 \pmod{n}$ temos que $xa \equiv 1 \pmod{n}$, ou seja, o inverso multiplicativo de a é x em $\mathbb{Z}/n\mathbb{Z}$. Assim, podemos concluir que $\mathbb{Z}/n\mathbb{Z}$ é um corpo.

($\Leftarrow$) Provaremos, agora, que se $\mathbb{Z}/n\mathbb{Z}$ é um corpo, então n é primo. Esta demonstração será feita por absurdo. Suponhamos que $\mathbb{Z}/n\mathbb{Z}$ é um corpo e n não é primo, logo n pode ser fatorado, ou seja, $n = a \cdot b$ com $1 < a, b < n$. Por hipótese, a possui inverso multiplicativo no corpo $\mathbb{Z}/n\mathbb{Z}$, assim, existe inteiro x tal que $ax \equiv 1 \pmod{n}$, ou seja, $ax - 1$ é um múltiplo de n, logo, $ax - 1 = kn = kab$, onde $k \in \mathbb{Z}$. Portanto,

$$1 = ax - kab \Rightarrow 1 = a(x - kb) \Rightarrow a \mid 1,$$

o que é impossível. Dessa forma, podemos concluir que n é primo. ∎

O Teorema 1.1 nos garante que $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\} = \{1, 2, 3, \cdots, n-1\}$ é um grupo multiplicativo abeliano quando n é primo. Na secção 1.3 definiremos o grupo multiplicativo das unidades de $\mathbb{Z}/n\mathbb{Z}$, denotado por $(\mathbb{Z}/n\mathbb{Z})^*$, e mostraremos algumas condições necessárias e suficientes para que ele seja cíclico.

Em resumo, $\mathbb{Z}/p\mathbb{Z}$ é um corpo finito com p elementos (também chamado $\mathbb{F}_p$) se p é primo. É possível provar que qualquer corpo finito tem $q = p^r$ elementos, para algum primo p e algum inteiro positivo r. A demonstração deste fato não é objetivo do nosso estudo.

O anel quociente $\mathbb{Z}/n\mathbb{Z}$ pode ser comparado com anéis quocientes obtidos a partir de $\mathbb{Q}[x]$ = anel dos polinômios com coeficientes racionais e variável x. Os corpos $\mathbb{Q}[x]/f(x)\mathbb{Q}[x]$, onde $f(x)$ é um polinômio irredutível, são extensões finitas para o corpo $\mathbb{Q}$. Também podemos substituir o corpo dos racionais por um corpo finito e obter outro corpo finito como um quociente de anéis de polinômios sobre $\mathbb{F}_p$.

Agora falaremos um pouco sobre o Teorema Chinês do Resto. De acordo com historiadores, o primeiro problema chinês de análise indeterminada foi encontrado numa obra escrita, por volta do primeiro século d.C, pelo matemático Chinês Sun-Tsï. Tal problema foi a motivação para o que conhecemos hoje por Teorema Chinês do Resto. Esse teorema tem inúmeras aplicações em computação, por exemplo, na criação de programas para multiplicar inteiros grandes.

Definição 1.2 *Definiremos a* soma direta *de dois anéis R e S por*

$$R \oplus S = \{(r, s) \mid r \in R,\ s \in S\}.$$

Consequentemente, definimos as operações de adição *e* multiplicação *em $R \oplus S$ por:*

$$(r, s) + (t, u) = (r + t, s + u),$$

$$(r, s) \cdot (t, u) = (r \cdot t, s \cdot u).$$

Com as operação $+$ e $\cdot$ definidas acima, podemos provar que $R \oplus S$ também é um anel. De modo análogo é possível definir soma direta para qualquer quantidade finita de anéis.

Teorema 1.2 (Teorema Chinês do Resto) *Suponhamos que $m_1,\ m_2,\ \cdots,\ m_r$ sejam inteiros relativamente primos dois a dois, ou seja,* m.d.c.$(m_j, m_k) = 1$*, para $j \neq k$. Seja $m = m_1 \cdot m_2 \cdots m_r$. Então temos o seguinte isomorfismo de anéis:*

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z}).$$

Demonstração: Consideremos a função

$$\psi : \mathbb{Z}/m\mathbb{Z} \longrightarrow (\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z})$$

definida por

$$\psi(x \bmod m) = (x \bmod m_1,\ x \bmod m_2,\ \cdots,\ x \bmod m_r).$$

Devemos mostrar que ψ é um isomorfismo de anéis, ou seja, que ψ é um homomorfismo bijetor. Inicialmente vamos verificar que ψ está bem definida. De fato, o valor de $\psi(x \bmod m)$ independe da escolha do representante da classe $x \bmod m$, pois, se a e b são dois representantes distintos desta classe, então $a \equiv b \pmod m$, ou seja, $m \mid a-b$, portanto, $m_1 \cdot m_2 \cdots m_r \mid a-b$. Mas m.d.c.$(m_j, m_k) = 1$, para $j \neq k$. Isso significa que $m_i \mid a-b$, para todo $i \in \{1,\ 2, \cdots,\ r\}$. Em outros termos $a \equiv b \pmod{m_i}$, logo,

$$(a \bmod m_1,\ a \bmod m_2, \cdots,\ a \bmod m_r) = (b \bmod m_1,\ b \bmod m_2, \cdots,\ b \bmod m_r),$$

donde concluímos que $\psi(a \bmod m) = \psi(b \bmod m)$.

Vamos provar que a função ψ é um homomorfismo de anéis, ou seja, que ψ cumpre as condições (a) e (b) da Definição B.18. Para quaisquer $x, y \in \mathbb{Z}/m\mathbb{Z}$ temos:

$$\begin{array}{rcl}
\psi(x+y \bmod m) & = & (x+y \bmod m_1,\ x+y \bmod m_2,\ \cdots,\ x+y \bmod m_r) \\
& = & (x \bmod m_1,\ x \bmod m_2,\ \cdots,\ x \bmod m_r) \\
& + & (y \bmod m_1,\ y \bmod m_2,\ \cdots,\ y \bmod m_r) \\
& = & \psi(x \bmod m) + \psi(y \bmod m) \quad (\psi \text{ preserva soma});
\end{array}$$

$$\begin{array}{rcl}
\psi(x \cdot y \bmod m) & = & (x \cdot y \bmod m_1,\ x \cdot y \bmod m_2,\ \cdots,\ x \cdot y \bmod m_r) \\
& = & (x \bmod m_1,\ x \bmod m_2,\ \cdots,\ x \bmod m_r) \\
& \cdot & (y \bmod m_1,\ y \bmod m_2,\ \cdots,\ y \bmod m_r) \\
& = & \psi(x \bmod m) \cdot \psi(y \bmod m) \quad (\psi \text{ preserva produto}).
\end{array}$$

Logo, ψ é um homomorfismo de anéis. Resta provar que ψ é uma bijeção ou seja, é injetora e sobrejetora. Como o domínio e o contra-domínio de ψ têm a mesma cardinalidade (ambos têm m elementos), o Princípio das Casas de Pombo [1] nos garante que, se ψ for injetora, então ψ também será sobrejetora. Isto reduz nosso trabalho a provar, apenas, que ψ é injetora. De fato, se $\psi(x \bmod m) = \psi(y \bmod m)$, então $x \equiv y \pmod{m_j}$, para todo j, ou seja,

$$m_1 \mid x-y,\ m_2 \mid x-y,\ \cdots,\ m_r \mid x-y.$$

Como m.d.c.$(m_j, m_k) = 1$, para $j \neq k$, temos que

$$m_1 \cdot m_2 \cdots m_r \mid x-y \Rightarrow m \mid x-y \Rightarrow x \equiv y \pmod m.$$

Fica assim provado que ψ é uma função injetora e, consequentemente, sobrejetora. Como ψ é um homomorfismo sobrejetor de anéis, podemos concluir que ψ é um isomorfismo de $\mathbb{Z}/m\mathbb{Z}$ em $(\mathbb{Z}/m_1\mathbb{Z}) \oplus (\mathbb{Z}/m_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_r\mathbb{Z})$. ∎

[1] O Princípio das Casas de Pombo (PCP) nos diz que se temos $n+1$ pombos e n casas, então existe pelo menos uma casa contendo mais de um pombo.

Observação 1.3 *Apresentamos, anteriormente, uma versão algébrica para o Teorema Chinês do Resto. Geralmente, nosso primeiro contato com esse teorema é por meio de sua versão aritmética, cujo enunciado mostramos a seguir:*

Sejam m_1, m_2, $\cdots$, m_r inteiros positivos tais que m.d.c.$(m_j, m_k) = 1$, para $j \neq k$. O sistema

$$\begin{array}{rcl} x & \equiv & a_1 \pmod{m_1} \\ x & \equiv & a_2 \pmod{m_2} \\ \vdots & \vdots & \vdots \\ x & \equiv & a_r \pmod{m_r} \end{array}$$

tem uma única solução módulo $m = m_1 \cdot m_2 \cdots m_r$. Tal solução pode ser escrita como $x = M_1 y_1 a_1 + M_2 y_2 a_2 + \cdots M_r y_r a_r$, onde $M_i = m/m_i$ e y_i é solução da equação $M_i y \equiv 1 \pmod{m_i}$, com $i \in \{1, 2, \cdots, r\}$.

Podemos consultar uma demonstração aritmética para o Teorema 1.2 nas referências bibliográficas [2], [3] e [4].

Exemplo 1.3 *Vamos resolver o seguinte sistema de congruências.*

$$\begin{array}{rcl} x & \equiv & 2 \pmod{3} \\ x & \equiv & 3 \pmod{5} \\ x & \equiv & 2 \pmod{7}. \end{array}$$

Seguiremos a seguinte sequência: multiplicaremos por 70 *o resto da divisão de* x *por* 3*, multiplicaremos por* 21 *o resto da divisão de* x *por* 5*, e multiplicaremos por* 15 *o resto da divisão de* x *por* 7*. Somaremos os três resultados e, em seguida, consideraremos o resto da divisão da soma por* 105 *encontrando, assim, a menor solução para o sistema,* 23*:*

$$70 \cdot 2 + 21 \cdot 3 + 15 \cdot 7 = 233 = 2 \cdot 105 + 23.$$

Mas, de onde é que vem 70*? É um múltiplo de* 5 *e* 7 *congruente a* 1 *módulo* 3*. De modo análogo,* 21 *é um múltiplo de* 3 *e* 7 *congruente a* 1 *módulo* 5 *e* 15 *é um múltiplo de* 3 *e* 5 *congruente a* 1 *módulo* 7*.*

Em seguida, faremos uma interpretação geométrica do Teorema Chinês do Resto para o caso em que $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Exemplo 1.4 *Suponhamos que exista um computador com problemas que conhece, apenas, os números de* 1 *a* 15*. Podemos melhorá-lo usando o Teorema Chinês do Resto com módulos* 3 *e* 5*. Para tanto, faremos com que cada número de* 1 *a* 15 *ocupe um lugar no retângulo mostrado na Tabela 1.3.*

	1	2	3	4	5
1	1	7	13	4	10
2	11	2	8	14	5
3	6	12	3	9	15

Tabela 1.3: $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Devemos perceber que, na Tabela 1.3, o elemento pertencente a j-ésima linha e k-ésima coluna é um $x \in \mathbb{Z}/15\mathbb{Z}$ *tal que* $x \equiv j \pmod 3$ *e* $x \equiv k \pmod 5$. *Por exemplo:*

- *o elemento pertencente a linha* 2 *e coluna* 4 *é* 14 *pois satisfaz, simultaneamente, as equações* $x \equiv 2 \pmod 3$ *e* $x \equiv 4 \pmod 5$*;*
- *o elemento pertencente a linha* 3 *e coluna* 1 *é* 6 *pois satisfaz, simultaneamente, as equações* $x \equiv 3 \pmod 3$ *e* $x \equiv 1 \pmod 5$*;*

Um modo bem simples de completar a Tabela 1.3 é utilizando uma tábua auxiliar com 15 *linhas e* 15 *colunas, preenchendo sua diagonal principal com os elementos de* $\mathbb{Z}/15\mathbb{Z}$*, como mostra a Tabela 1.4.*

	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1	1														
2		2													
3			3												
1				4											
2					5										
3						6									
1							7								
2								8							
3									9						
1										10					
2											11				
3												12			
1													13		
2														14	
3															15

Tabela 1.4: Tábua auxiliar para a construção da Tabela 1.3.

Na Tabela 1.4 temos, por exemplo, que o elemento 13 *de* $\mathbb{Z}/15\mathbb{Z}$ *pertence a linha que inicia em* 1 *e coluna que inicia em* 3. *Na Tabela 1.3,* 13 *deve ocupar a linha e coluna que iniciam nos respectivos elementos dados na Tabela 1.4. De modo análogo, percebe-se que* $9 \in \mathbb{Z}/15\mathbb{Z}$ *encontra-se na linha que inicia em* 3 *e coluna que inicia em* 4*, nas duas tabelas.*

Iremos, agora, fazer uma interpretação geométrica do anel $\mathbb{Z}/15\mathbb{Z}$ *por meio do Teorema Chinês do Resto. Em vez de um círculo finito ou gráfico cíclico, podemos*

considerar o produto de dois gráficos cíclicos finitos, resultando no gráfico do toro finito. A Figura 1.2 contém a imagem de um toro contínuo obtido enrolando-se um pedaço de material no formato de retângulo. O toro finito é mostrado na Figura 1.3.

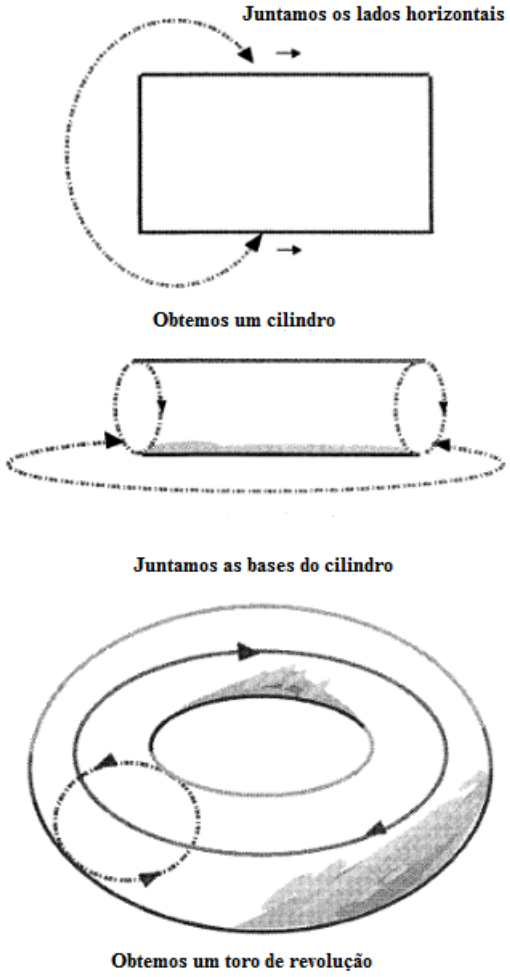

Figura 1.2: Toro contínuo ou de revolução obtido a partir de um retângulo enrolado.

Para finalizar esta secção, faremos uma breve reflexão sobre a seguinte questão: porque os anéis abaixo têm mesma ordem 2^n mas são todos diferentes?

$$\mathbb{Z}/2^n\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^n,\quad \mathbb{F}_{2^n}$$

O grupo aditivo do anel da esquerda é cíclico já que $\mathbb{Z}/2^n\mathbb{Z} = \langle 1 \ (\mod 2^n)\rangle$, em outras palavras, $\mathbb{Z}/2^n\mathbb{Z}$ é gerado por 1. No grupo aditivo do anel $(\mathbb{Z}/2\mathbb{Z})^n$, cada elemento diferente de zero tem ordem 2, o que significa que $2x = 0$ para todo $x \neq 0$. O anel $\mathbb{F}_{2^n}$ é um corpo e, portanto, não tem divisores próprios de zero, ou

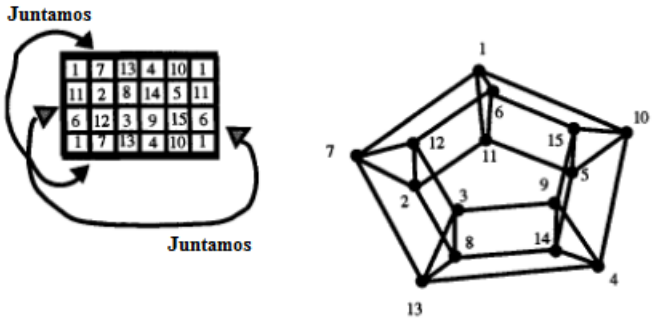

Figura 1.3: Toro finito obtido a partir do gráfico de $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

seja, $ab \neq 0$ para quaisquer a e b não nulos. Mas o outros dois anéis tem divisores próprios de zero.

1.2 Inverso Multiplicativo no Anel $\mathbb{Z}/n\mathbb{Z}$ e Função Phi de Euler

Daremos sequência aos nossos estudos apresentando algumas propriedades do grupo multiplicativo de inteiros $a(\text{mod } n)$, com m.d.c.$(a, n) = 1$. Em seguida, definiremos a Função Phi de Euler e provaremos alguns fatos importantes sobre tal função e, como consequência, mostraremos o Pequeno Teorema de Fermat.

Definição 1.3 *O* grupo das unidades *do anel* $\mathbb{Z}/n\mathbb{Z}$ *é dado por*

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^* &= \{a \bmod n \mid \text{m.d.c.}(a, n) = 1\} \\ &= \{a \bmod n \mid ax \equiv 1 \pmod{n}, \text{ com uma solução } x \in \mathbb{Z}\}.\end{aligned}$$

Devemos observar que $1 \in (\mathbb{Z}/n\mathbb{Z})^*$, já que m.d.c.$(1, n) = 1$. Além disso, para todo $y \in (\mathbb{Z}/n\mathbb{Z})^*$ temos que $1 \cdot y = y \cdot 1 = y$, ou seja, 1 é elemento neutro da multiplicação em $(\mathbb{Z}/n\mathbb{Z})^*$. A Definição 1.3 nos diz que todos os elementos de $(\mathbb{Z}/n\mathbb{Z})^*$ são inversíveis. Também vimos, anteriormente, que a multiplicação em $\mathbb{Z}/n\mathbb{Z}$ é associativa e, consequentemente, tem a mesma propriedade no subconjunto $(\mathbb{Z}/n\mathbb{Z})^*$.

Como a multiplicação é associativa, tem elemento neutro e admite inverso para todos os elementos de $(\mathbb{Z}/n\mathbb{Z})^*$, podemos concluir que $(\mathbb{Z}/n\mathbb{Z})^*$ é um grupo multiplicativo.

Exemplo 1.5 *Vejamos alguns exemplos de grupos das unidades.*

- *O grupo das unidades de* $\mathbb{Z}/8\mathbb{Z}$ *é* $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$*;*

- *O grupo das unidades de* $\mathbb{Z}/12\mathbb{Z}$ *é* $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$*;*
- *Seja* p *é um inteiro primo qualquer. O grupo das unidades de* $\mathbb{Z}/p\mathbb{Z}$ *é* $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, \cdots, p-1\}$.

Definição 1.4 *A* função Phi de Euler *é definida por*

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = \text{ ordem do grupo } (\mathbb{Z}/n\mathbb{Z})^*.$$

Exemplo 1.6 *A seguinte tabela mostra alguns valores da função Phi de Euler.*

n	1	2	3	4	5	6	7	8	9	10	11
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10

Tabela 1.5: Função Phi de Euler.

Teorema 1.3 *Os seguintes fatos sobre a função Phi de Euler são verdadeiros.*

(a) *Se* p *é um primo, então* $\phi(p^n) = p^n - p^{n-1}$.

(b) *Se* m.d.c.$(m, n) = 1$*, então* $\phi(nm) = \phi(n)\phi(m)$*. Isto mostra que a função Phi de Euler é uma função multiplicativa.*

(c)

$$\phi(m) = m \prod_{\substack{p|m \\ p \text{ = primo}}} \left(1 - \frac{1}{p}\right).$$

(d) *Se* x *é um inteiro tal que* m.d.c.$(x, n) = 1$*, então*

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Demonstração:

(a) Seja p um número primo. De acordo com a Definição 1.4, $\phi(p^n)$ é o número de inteiros a compreendidos entre 0 e $p^n - 1$ tais que m.d.c.$(a, p) = 1$. Em outros termos, podemos contar os números a entre 0 e $p^n - 1$ tais que p divide a e subtrair esta quantidade de p^n. Os números a com p dividindo a tais que $0 \leq a \leq p^n - 1$ são

$$0 \cdot p,\ 1 \cdot p,\ 2 \cdot p,\ \cdots,\ (p^{n-1} - 1) \cdot p.$$

Percebendo que a lista acima tem p^{n-1} elementos, podemos concluir que o número de elementos de $(\mathbb{Z}/p^n\mathbb{Z})^*$ é $p^n - p^{n-1}$, ou seja, $\phi(p^n) = p^n - p^{n-1}$.

(b) Sejam n e m inteiros tais que m.d.c.$(m, n) = 1$. Consideremos os anéis $\mathbb{Z}/nm\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ e $\mathbb{Z}/m\mathbb{Z}$. Pelo Teorema Chinês do resto, temos que

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Isso significa que $\mathbb{Z}/nm\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ têm o mesmo número de elementos inversíveis, ou seja, $\phi(nm) = \phi(n)\phi(m)$.

(c) Seja m um número inteiro maior que 1. Pelo Teorema Fundamental da Aritmética, podemos escrever m de modo único como produto de fatores primos. Assim, existem primos $p_1,\ p_2,\ p_3,\ \cdots,\ p_j$ e $n_1,\ n_2,\ n_3,\ \cdots,\ n_j \in \mathbb{N} \cup \{0\}$ tais que

$$m = {p_1}^{n_1} \cdot {p_2}^{n_2} \cdot {p_3}^{n_3} \cdots {p_j}^{n_j}.$$

Aplicando o resultado demonstrado no item (b) temos que:

$$\phi(m) = \phi({p_1}^{n_1} \cdot {p_2}^{n_2} \cdot {p_3}^{n_3} \cdots {p_j}^{n_j}) = \phi({p_1}^{n_1}) \cdot \phi({p_2}^{n_2}) \cdot \phi({p_3}^{n_3}) \cdots \phi({p_j}^{n_j}).$$

No item (a), provamos que $\phi(p^n) = (p^n - p^{n-1})$, para todo p primo e n natural, logo

$$\begin{aligned}
\phi(m) &= ({p_1}^{n_1} - {p_1}^{n_1-1}) \cdot ({p_2}^{n_2} - {p_2}^{n_2-1}) \cdot ({p_3}^{n_3} - {p_3}^{n_3-1}) \cdots ({p_3}^{n_j} - {p_j}^{n_j-1}) \\
&= {p_1}^{n_1}\left(1 - \frac{1}{p_1}\right) \cdot {p_2}^{n_2}\left(1 - \frac{1}{p_2}\right) \cdot {p_3}^{n_3}\left(1 - \frac{1}{p_3}\right) \cdots {p_j}^{n_j}\left(1 - \frac{1}{p_j}\right) \\
&= {p_1}^{n_1}{p_2}^{n_1}{p_3}^{n_3} \cdots {p_j}^{n_j}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \cdots \left(1 - \frac{1}{p_j}\right) \\
&= m \prod_{\substack{p|m \\ p \text{ = primo}}} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

(d) Consideremos um elemento $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ tal que m.d.c.$(x, n) = 1$. Desse modo, $\overline{x}$ pertence ao grupo das unidades de $\mathbb{Z}/n\mathbb{Z}$ e, como $(\mathbb{Z}/n\mathbb{Z})^*$ é um grupo multiplicativo finito de ordem $\phi(n)$, pelo Corolário B.2, podemos concluir que

$$\overline{x}^{\phi(n)} = \overline{1}, \text{ ou seja, } x^{\phi(n)} \equiv 1 \pmod{n}.$$

■

O item (d) do Teorema 1.3 também é conhecido como Teorema de Euler-Fermat. A seguir, provaremos uma consequência importante do *Teorema de Euler-Fermat*.

Corolário 1.1 (Pequeno Teorema de Fermat) *Seja p um número primo qualquer. Então, para todo $a \in \mathbb{Z}$ temos que*

$$a^p \equiv a \pmod{p}.$$

Se p não divide a, então

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração: Consideremos um número primo p e um inteiro a quaisquer. Se $p \mid a$ então $p \mid -a$ e $p \mid a^p$, portanto

$$p \mid (a^p - a) \Rightarrow a^p \equiv a \pmod{p}.$$

Suponhamos, agora, que p não divide a. Assim, m.d.c.$(a, p) = 1$. Como

$$\phi(p) = p^1 - p^{1-1} = p - p^0 = p - 1,$$

o item (d) do Teorema 1.3 nos diz que

$$a^{\phi(p)} \equiv 1 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Além disso, podemos multiplicar a congruência $a^{p-1} \equiv 1 \pmod{p}$ por a para concluir que

$$a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}.$$

■

Observação 1.4 *Se n é um inteiro maior que 2, então $\phi(n) \equiv 0 \pmod{2}$. De fato, se $n = 2^k$, com $k \geq 2$ inteiro, então*

$$\phi(n) = 2^{k-1} \equiv 0 \pmod{2}.$$

Se $n = p^k \cdot a$, onde $a, k \in \mathbb{N}$ e $p > 2$ é um primo tal que $p \nmid a$, temos também

$$\phi(n) = \phi(p^k \cdot a) = \phi(p^k) \cdot \phi(a) = (p^k - p^{k-1})\phi(a) = p^{k-1}(p-1)\phi(a).$$

mas p é um primo ímpar, logo $p - 1$ é par e, portanto, $p^{k-1}(p-1)\phi(a)$ também é par, ou seja

$$\phi(n) = p^{k-1}(p-1)\phi(a) \equiv 0 \pmod{2}.$$

Encerraremos esta secção mostrando mais uma propriedade da função Phi de Euler.

Proposição 1.3 *Para todo número natural m temos que*

$$\sum_{d|m} \phi(d) = m.$$

Demonstração: Seja m um número natural qualquer. Suponhamos que $m = p^n$, com p primo e $n \in \mathbb{N}$. Desse modo temos

$$\begin{aligned}\sum_{d|m} \phi(d) &= \sum_{j=0}^{n} \phi(p^j) = \phi(p^0) + \sum_{j=1}^{n} \phi(p^j) \\ &= 1 + \sum_{j=1}^{n} (p^j - p^{j-1}) = 1 + \sum_{j=1}^{n} p^{j-1}(p-1).\end{aligned}$$

Como $\sum_{j=1}^{n} p^{j-1}(p-1)$ é a soma dos n termos de uma P.G. com primeiro termo $\alpha_1 = p - 1$ e razão $q = p > 1$, temos que

$$\begin{aligned}\sum_{d|m} \phi(d) &= 1 + \alpha_1 \cdot \frac{q^n - 1}{q - 1} = 1 + (p-1) \cdot \frac{p^n - 1}{p - 1} \\ &= 1 + p^n - 1 = p^n = m.\end{aligned}$$

Suponhamos, agora, que m não seja potência de um número primo. Pelo Teorema Fundamental da Aritmética, podemos escrever m de modo único como produto de números primos, assim existem $p_1,\ p_2,\ \cdots,\ p_k$ primos e $n_1,\ n_2,\ \cdots,\ n_k \in \mathbb{N} \cup \{0\}$ tais que

$$m = {p_1}^{n_1} \cdot {p_2}^{n_2} \cdots {p_k}^{n_k}.$$

Logo,

$$\begin{aligned}\sum_{d|m} \phi(d) &= \sum_{j_1=0}^{n_1} \sum_{j_2=0}^{n_2} \cdots \sum_{j_k=0}^{n_k} \phi({p_1}^{j_1} \cdot {p_2}^{j_2} \cdots {p_k}^{j_k}) \\ &= \sum_{j_1=0}^{n_1} \sum_{j_2=0}^{n_2} \cdots \sum_{j_k=0}^{n_k} \phi({p_1}^{j_1}) \cdot \phi({p_2}^{j_2}) \cdots \phi({p_k}^{j_k}) \\ &= \left(\sum_{j_1=0}^{n_1} \phi({p_1}^{j_1})\right) \left(\sum_{j_2=0}^{n_2} \phi({p_2}^{j_2})\right) \cdots \left(\sum_{j_k=0}^{n_k} \phi({p_k}^{j_k})\right) \\ &= \left(\sum_{d_1|p^{n_1}} \phi(d_1)\right) \left(\sum_{d_2|p^{n_2}} \phi(d_2)\right) \cdots \left(\sum_{d_k|p^{n_k}} \phi(d_k)\right) \\ &= {p_1}^{n_1} \cdot {p_2}^{n_2} \cdots {p_k}^{n_k} = m.\end{aligned}$$

■

1.3 Raízes Primitivas

Definição 1.5 *Consideremos um elemento qualquer g pertencente ao grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$. Definimos a* ordem *de g, denotada por $o(g)$, como sendo o número de elementos do subgrupo $\langle g\rangle$ gerado por g. Se a ordem de g for igual à $\phi(n)$, ou seja, for igual ao número de elementos de $(\mathbb{Z}/n\mathbb{Z})^*$, dizemos que g é uma* raiz primitiva módulo n.

Observação 1.5 *Na subsecção B.1.3 do Apêndice B, daremos uma definição mais geral sobre ordem de elementos pertencentes a um grupo multiplicativo e falaremos sobre grupos cíclicos. Para um estudo mais aprofundado sobre esses temas, podemos consultar a referência bibliográfica [5].*

Observação 1.6 *De acordo com a Definição 1.5, quando falamos que g é uma raiz primitiva módulo n também estamos afirmando que g gera o subgrupo $(\mathbb{Z}/n\mathbb{Z})^*$, ou seja, $(\mathbb{Z}/n\mathbb{Z})^* = \langle g\rangle$ é cíclico.*

Exemplo 1.7 *O número 2 não é raiz primitiva módulo 7 pois $\phi(7) = 7 - 1 = 6$, mas, $2^0 = 1$, $2^1 = 2$, $2^2 = 4$ e $2^3 = 8 \equiv 1 \pmod 7$, ou seja, $\langle 2\rangle = \{1, 2, 4\}$ e $o(2) = 3 \neq \phi(7)$. Em outras palavras, 2 não gera $(\mathbb{Z}/7\mathbb{Z})^*$.*

Exemplo 1.8 *O número 5 é raiz primitiva módulo 6 pois*

$$\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = (2 - 1) \cdot (3 - 1) = 1 \cdot 2 = 2.$$

Além disso, $5^0 = 1$, $5^1 = 5$ e $5^2 = 25 \equiv 1 \pmod 6$, ou seja, $\langle 5\rangle = \{1, 5\}$ e, consequentemente, $o(5) = 2 = \phi(6)$. Assim, $(\mathbb{Z}/6\mathbb{Z})^* = \langle 5\rangle$ é um grupo cíclico.

Exemplo 1.9 *Vamos provar que não existe raiz primitiva módulo 12. Devemos perceber, inicialmente, que todos os elementos de $(\mathbb{Z}/3\mathbb{Z})^*$ e $(\mathbb{Z}/4\mathbb{Z})^*$, têm ordem 1 ou 2, ocorrendo o mesmo com os elementos de $(\mathbb{Z}/3\mathbb{Z})^* \oplus (\mathbb{Z}/4\mathbb{Z})^*$. Por outro lado, o Teorema Chinês do Resto nos garante que $(\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \oplus (\mathbb{Z}/4\mathbb{Z})^*$. Assim, todos os elementos de $(\mathbb{Z}/12\mathbb{Z})^*$ têm ordem 1 ou 2 e, portanto, não existe raiz primitiva módulo 12, já que*

$$\phi(12) = \phi(3 \cdot 4) = \phi(3) \cdot \phi(4) = (3 - 1) \cdot (2^2 - 2) = 2 \cdot 2 = 4.$$

Logo, $(\mathbb{Z}/12\mathbb{Z})^*$ não é cíclico.

Exemplo 1.10 *Consideremos o grupo multiplicativo das raízes n-ésimas da unidade complexa definido por*

$$\mathcal{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}.$$

Os elementos desse grupo podem ser escritos na forma $\exp(2k\pi i/n)$, *com* $k = 0, 1, 2, \cdots, n-1$, *onde todos são distintos e têm inverso multiplicativo, já que* $\mathcal{U}_n \subset \mathbb{C} \setminus \{0\}$. *Consideremos* $\omega = \exp(2\pi i/n)$. *É claro que todos os elementos de* $\mathcal{U}_n$ *são potências distintas de* ω, *em outras palavras,* ω *é gerador de* $\mathcal{U}_n$, *ou seja,* $\mathcal{U}_n = \langle\omega\rangle$ *é um grupo cíclico de ordem* n. *Além disso, pelo que veremos na Proposição B.2, os grupos* $(\mathcal{U}_n, \cdot)$ *e* $(\mathbb{Z}/n\mathbb{Z}, +)$ *são isomorfos. Faremos, abaixo, as representações geométricas dos grupos cíclicos* $\mathcal{U}_4$ *e* $\mathcal{U}_6$.

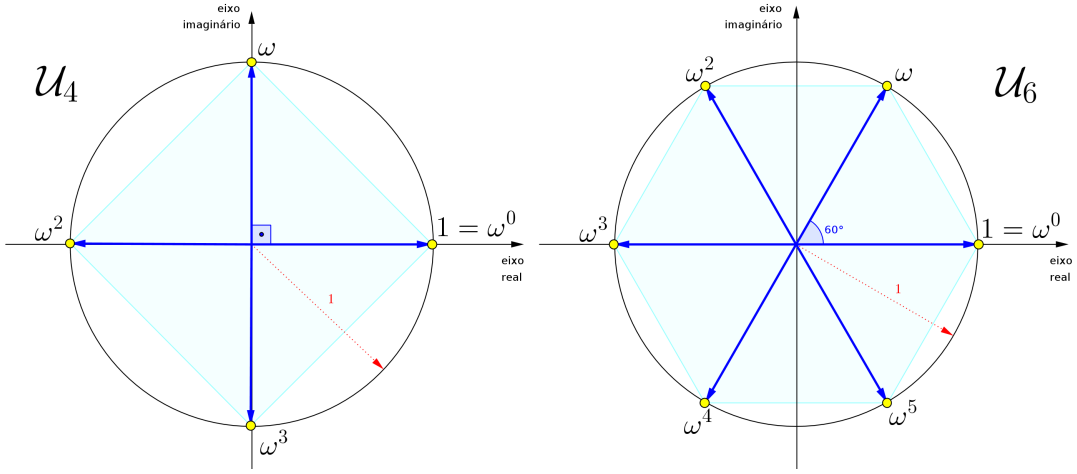

Figura 1.4: Raízes n-enésimas da unidade complexa para $n = 4$ e $n = 6$.

Observação 1.7 *Como* $(\mathbb{Z}/n\mathbb{Z})^*$ *é um grupo finito de ordem* $\phi(n)$, *sendo* a *um elemento qualquer de* $(\mathbb{Z}/n\mathbb{Z})^*$, *o Corolário B.1 nos garante que* $o(a)$ *é um divisor de* $\phi(n)$.

A seguir, provaremos que $(\mathbb{Z}/n\mathbb{Z})^*$ é cíclico se, e somente se, $n = 2,\ 4,\ p^e,\ 2p^e$, para todo p primo e $e \in \mathbb{N}$.

Teorema 1.4 $(\mathbb{Z}/p\mathbb{Z})^*$ *é cíclico para todo* p *primo, ou seja, existe raiz primitiva módulo* p, *para qualquer primo* p.

Demonstração: Devemos provar que $(\mathbb{Z}/p\mathbb{Z})^*$ tem um elemento de ordem $p-1$. Seja d um divisor de $p-1$. Denotaremos por $\psi(d)$ o número de elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ com ordem d. Assim, se $\psi(d) \neq 0$, então existe $x \in \mathbb{Z}/p\mathbb{Z}$ tal que a ordem de x é igual a d, logo, para $0 \leq k < d$, as classes x^k são todas distintas módulo p. É óbvio que o conjunto

$$\langle x\rangle = \{1,\ x,\ x^2,\ x^3,\ \cdots,\ x^{d-1}\}$$

é um subgrupo cíclico de $(\mathbb{Z}/p\mathbb{Z})^*$ com, exatamente, d elementos. Como $\mathbb{Z}/p\mathbb{Z}$ é um corpo, e consequentemente um anel de integridade, a Proposição B.6 nos garante

que a equação $T^d \equiv 1 \pmod{p}$ tem, no máximo, d soluções distintas e tais soluções são, exatamente, os elementos de $\langle x \rangle$, já que $(x^k)^d = 1$, com $0 \leq k < d$. Além disso, se $o(x^k) = d$, então m.d.c.$\{k, d\} = 1$, pois $r = \text{m.d.c.}\{k, d\} > 1$ implica que $(x^k)^{d/r} = (x^d)^{k/r} = 1^{k/r} = 1$, ou seja, $o(x^k) \leq d/r < d$, o que contradiz o fato de que $o(x^k) = d$. Dessa forma, o subgrupo $\langle x \rangle$ contem todos os elementos de $(\mathbb{Z}/p\mathbb{Z})^*$ com ordem d, ou seja, $\psi(d) \leq \phi(d)$. Além disso,a Proposição B.2 nos diz que o grupo cíclico $\langle x \rangle$ é isomorfo ao grupo aditivo $\mathbb{Z}/d\mathbb{Z}$. Por outro lado, para cada elemento $a \in (\mathbb{Z}/p\mathbb{Z})^*$ temos que $o(a) \mid p-1$, assim,

$$\sum_{\substack{0<d \\ d|p-1}} \psi(d) = p - 1.$$

Na Proposição 1.3 vimos que

$$\sum_{\substack{0<d \\ d|p-1}} \phi(d) = p - 1,$$

portanto

$$\psi(d) \leq \phi(d) \quad \Rightarrow \quad \sum_{\substack{0<d \\ d|p-1}} \psi(d) \leq \sum_{\substack{0<d \\ d|p-1}} \phi(d)$$

$$\Rightarrow \quad p - 1 = \sum_{\substack{0<d \\ d|p-1}} \psi(d) \leq \sum_{\substack{0<d \\ d|p-1}} \phi(d) = p - 1,$$

onde podemos concluir que $\psi(d) = \phi(d)$ e, portanto,

$$\langle x \rangle = \{y \in (\mathbb{Z}/p\mathbb{Z})^* \mid o(y) = d\}.$$

Em particular, temos que $p - 1 \mid p - 1$, logo, $\psi(p-1) = \phi(p-1)$, ou seja, existe $x \in \mathbb{Z}/p\mathbb{Z}$ tal que $o(x) = p - 1 = \phi(p)$, logo $(\mathbb{Z}/p\mathbb{Z})^* = \langle x \rangle \neq \emptyset$ e, portanto, $(\mathbb{Z}/p\mathbb{Z})^*$ é cíclico. ∎

Daremos sequência aos nossos estudos lembrando que $(\mathbb{Z}/n\mathbb{Z})^*$ é um grupo finito abeliano. Por outro lado, é possível provar que todo grupo finito abeliano é isomorfo a um produto direto de grupos cíclicos finitos. Nesses casos, o produto direto é análogo à soma direta de anéis que apresentamos no Teorema Chinês do Resto, entretanto, no produto direto de grupos nos preocupamos apenas com uma operação, a multiplicação. Nessas condições, sendo $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$, onde os p_i são primos distintos e os e_i inteiros positivos, o Teorema Chinês do Resto nos diz que

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times (\mathbb{Z}/p_1^{e_2}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{e_k}\mathbb{Z})^*.$$

Aqui o símbolo $\times$ denota o produto direto de grupos multiplicativos.

Proposição 1.4 *Se p é um primo ímpar , então $(\mathbb{Z}/p^e\mathbb{Z})^*$ é cíclico, para qualquer inteiro positivo e.*

Demonstração: Seja p um número primo ímpar. Provaremos, inicialmente, que, que existe raiz primitiva $g \pmod p$ tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. Já vimos no Teorema 1.4 que existe raiz primitiva $x \pmod p$. Se $x^{p-1} \not\equiv 1 \pmod{p^2}$ basta tomar $g = x$. Caso tenhamos $x^{p-1} \equiv 1 \pmod{p^2}$, tomaremos $g = x + p$, que também é raiz primitiva módulo p. Assim

$$\begin{aligned} g^{p-1} &= (x+p)^{p-1} \\ &= \binom{p-1}{0} x^{p-1}p^0 + \binom{p-1}{1} x^{p-2}p^1 + \cdots + \binom{p-1}{p-1} x^0 p^{p-1} \\ &= x^{p-1} + (p-1)\,px^{p-2} + \cdots + p^{p-1} \end{aligned}$$

A partir da terceira parcela da soma anterior, todos os termos são múltiplos de p^2, ou seja, são congruentes a zero módulo p^2. Além disso, $x^{p-1} \equiv 1 \pmod{p^2}$, logo,

$$\begin{aligned} g^{p-1} &= (x+p)^{p-1} \equiv 1 + (p-1)\,px^{p-2} + 0 + \cdots + 0 \pmod{p^2} \\ &\equiv 1 + (p-1)\,px^{p-2} \not\equiv 1 \pmod{p^2}, \end{aligned}$$

já que $(p-1)px^{p-2} \not\equiv 0 \pmod{p^2}$.

Prosseguiremos nossa demonstração provando que, para qualquer raiz primitiva $g \pmod p$ tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$, temos $g^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$, para qualquer que seja o inteiro $e \geq 2$. Faremos esta prova por indução em e.
Se $e = 2$ temos que $g^{p^{2-2}(p-1)} = g^{p-1} \not\equiv 1 \pmod{p^2}$, como vimos anteriormente. Logo, a afirmação é válida para $e = 2$.
Suponhamos que $g^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$ para algum $k > 2$ natural. Devemos mostrar que $g^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$.
Sabemos que $\phi(p^{k-1}) = p^{k-1} - p^{k-2} = p^{k-2}(p-1)$. Aplicando o Teorema de Euler-Fermat obtemos

$$g^{p^{k-2}(p-1)} = g^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}},$$

ou seja, $g^{p^{k-2}(p-1)} = 1 + mp^{k-1}$, onde $p \nmid m$. Desse modo, segue que

$$\begin{aligned} g^{p^{k-1}(p-1)} &= \left[g^{p^{k-2}(p-1)}\right]^p = \left[1+mp^{k-1}\right]^p \\ &= \binom{p}{0}\left(mp^{k-1}\right)^0 + \binom{p}{1}\left(mp^{k-1}\right)^1 + \cdots + \binom{p}{p}\left(mp^{k-1}\right)^p \\ &= 1 + pmp^{k-1} + \cdots + m^p p^{(k-1)p}. \end{aligned}$$

Como, a partir da terceira parcela da última soma, todos os termos são múltiplos de p^{k+1}, ou seja, são congruentes a zero módulo p^{k+1}, obtemos

$$\begin{aligned} g^{p^{k-1}(p-1)} &\equiv 1 + pmp^{k-1} + 0 + \cdots + 0 \pmod{p^{k+1}}, \\ &\equiv 1 + mp^k \not\equiv 1 \pmod{p^{k+1}} \end{aligned}$$

pois $mp^k \not\equiv 0 \pmod{p^{k+1}}$, já que $p \nmid m$.
Por fim, provaremos que qualquer raiz primitiva $g \pmod p$ satisfazendo a condição $g^{p-1} \not\equiv 1 \pmod{p^2}$ é uma raiz primitiva módulo p^e, para todo natural $e \geq 1$. De fato.
Já provamos que, nessas condições, $g^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$, para todo $e \geq 2$. Também sabemos que a ordem de g em $\mathbb{Z}/p^e\mathbb{Z}$ divide $\phi(p^e)$. Denotando a ordem de g por $o_{p^e}(g)$ temos que

$$o_{p^e}(g) \mid \phi(p^e) \Rightarrow o_{p^e}(g) \mid p^{e-1}(p-1).$$

Como $g^{o_{p^e}(g)} \equiv 1 \pmod{p^e}$, segue que $g^{o_{p^e}(g)} \equiv 1 \pmod p$ e, portanto,

$$o_p(g) \mid o_{p^e}(g) \Rightarrow p-1 \mid o_{p^e}(g).$$

Dessa forma, $o_{p^e}(g) = p^\alpha(p-1)$, onde $0 \leq \alpha \leq e-1$. Mas $g^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$, para todo $e \geq 2$, logo, $\alpha = e-1$, portanto,

$$o_{p^e}(g) = p^{e-1}(p-1) = \phi(p^e).$$

Assim, fica provado que g é raiz primitiva módulo p^e, o que conclui nossa demonstração. ∎

Proposição 1.5 *$(\mathbb{Z}/2^e\mathbb{Z})^*$ não é cíclico para $e \geq 3$.*

Demonstração: Provaremos, inicialmente, que para todo inteiro ímpar g e $m \geq 3$, vale $g^{2^{m-2}} \equiv 1 (\text{mod } 2^m)$. Faremos isso por indução. Para $m = 3$ temos que

$$g^{2^{m-2}} \equiv 1 \pmod{2^m} \Rightarrow g^2 \equiv 1 \pmod 8,$$

já que $1^2 = 1 \equiv 1 \pmod 8$, $3^2 = 9 \equiv 1 \pmod 8$, $5^2 = 25 \equiv 1 \pmod 8$ e $7^2 = 49 \equiv 1 \pmod 8$. Suponhamos que $g^{2^{k-2}} \equiv 1 \pmod{2^k}$ seja verdadeiro para algum inteiro $k > 3$. Devemos mostrar que $g^{2^{k-1}} \equiv 1 (\text{mod } 2^{k+1})$. De fato, como $g^{2^{k-2}} \equiv 1 (\text{mod } 2^k) \Rightarrow g^{2^{k-2}} = a \cdot 2^k + 1$, para algum $a \in \mathbb{Z}$, segue que

$$\begin{aligned} g^{2^{k-1}} &= g^{2\cdot 2^{k-2}} = (g^{2^{k-2}})^2 = (a \cdot 2^k + 1)^2 \\ &= a^2 \cdot 2^{2k} + 2 \cdot a \cdot 2^k + 1 \\ &= a^2 \cdot 2^{k+1+k-1} + a \cdot 2^{k+1} + 1 \\ &= (a^2 \cdot 2^{k-1} + a) \cdot 2^{k+1} + 1 \equiv 1 (\text{mod } 2^{k+1}). \end{aligned}$$

Provaremos, agora que $(\mathbb{Z}/2^e\mathbb{Z})^*$ não é cíclico para $e \geq 3$. Como $\phi(2^e) = 2^{e-1}$ temos que

$$g^{\frac{\phi(2^e)}{2}} = g^{\frac{2^{e-1}}{2}} = g^{2^{e-2}} \equiv 1 (\text{mod } 2^e).$$

Logo, $o_{2^e}(g) \leq \dfrac{\phi(2^e)}{2}$, para qualquer inteiro ímpar g. Isso significa que não existe raiz primitiva módulo 2^e ímpar. Como não faz sentido falar em raiz primitiva módulo 2^e par, pois m.d.c.$(g, 2^e) \neq 1$ quando g é par, podemos concluir que $(\mathbb{Z}/2^e\mathbb{Z})^*$ não é cíclico para $e \geq 3$. ∎

Proposição 1.6 *Se $n = ab$, com $a, b > 2$ inteiros tais que* m.d.c.$(a, b) = 1$*, então $(\mathbb{Z}/n\mathbb{Z})^*$ não é cíclico.*

Demonstração: Suponhamos que $n = ab$, com $a, b > 2$ inteiros coprimos, ou seja, com m.d.c.$(a, b) = 1$ e $(\mathbb{Z}/n\mathbb{Z})^*$ seja cíclico. Pelo Teorema Chinês do Resto temos que

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*,$$

logo, $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$ deve ser cíclico. Por outro lado, pelo que vimos na Observação 1.4, $\phi(a)$ e $\phi(b)$ são ambos pares, e portanto, $(\mathbb{Z}/a\mathbb{Z})^*$ e $(\mathbb{Z}/b\mathbb{Z})^*$ têm elemento de ordem 2. Denotemos por $\overline{x}$ e $\overline{y}$ os elementos de ordem 2 pertencentes a $(\mathbb{Z}/a\mathbb{Z})^*$ e $(\mathbb{Z}/b\mathbb{Z})^*$, respectivamente. Desse modo, os pares $(x \mod a,\ 1 \mod b)$ e $(1 \mod a,\ y \mod b)$ tem, ambos, ordem 2 em $(\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$, o que é um absurdo já que, como veremos na Proposição B.4, um grupo cíclico deve ter apenas um elemento de ordem 2. Assim, podemos concluir que $(\mathbb{Z}/n\mathbb{Z})^*$ não é cíclico. ∎

Observação 1.8 *É possível provar que o produto direto $G \times H$ de grupos cíclicos também é cíclico se, e somente se, $|G|$ e $|H|$ são primos entre si. Esse resultado será bastante útil na demonstração do próximo teorema. Ele também poderia ser utilizado na demonstração da Proposição 1.6, já que $(\mathbb{Z}/a\mathbb{Z})^*$ e $(\mathbb{Z}/b\mathbb{Z})^*$ têm, ambos, ordem par.*

O Teorema 1.4 junto com as proposições 1.4, 1.5 e 1.6 nos conduzem ao enunciado do seguinte teorema.

Teorema 1.5 *Existe alguma raiz primitiva módulo n se, e somente se, $n = 2$, $n = 4$, $n = p^e$ ou $n = 2p^e$, onde p é um primo ímpar.*

Demonstração: Já vimos, nas proposições 1.5 e 1.6, que não existem raízes primitivas módulo n quando $n = 2^e$, para $e \geq 3$, e também quando $n = ab$, com $a, b > 2$ inteiros tais que m.d.c.$(a, b) = 1$. É fácil verificar que 1 é raiz primitiva módulo 2 e 3 é raiz primitiva módulo 4. A Proposição 1.4 nos garante que há raiz primitiva módulo p^e para $p > 2$ primo ímpar. Resta mostrar que $(\mathbb{Z}/2p^e\mathbb{Z})^*$ é cíclico. Para tanto, basta lembrar que $(\mathbb{Z}/2p^e\mathbb{Z})^*$ é isomorfo a $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^e\mathbb{Z})^*$ e perceber que este produto direto de grupos cíclicos também é cíclico, pelo que foi exposto na Observação 1.8. ∎

1.4 Uma Pequena Aplicação na Criptografia

Em várias situações do nosso cotidiano se faz necessário enviar algum tipo de mensagem secreta que deve ser decifrada apenas pelo destinatário, como por exemplo, trocar mensagens em redes sociais ou efetuar uma compra via internet. Nessas situações se faz necessário o uso de algoritmos para criptografia de chaves públicas.

Para entendermos como funciona esse método de criptografia, suponhamos que estamos enviando uma mensagem secreta para alguém. Assim, vamos considerar essa mensagem como sendo um número $m \mod pq$, onde p e q são números primos muito grandes, cada um com, pelos menos, 100 algarismos em sua representação decimal. A criptografia de m é dada por $m^t \pmod{pq}$, para algum expoente t. O receptor que deseja descriptografar a mensagem deve determinar outro expoente s tal que $m^{ts} \equiv m \pmod{pq}$.

Pelo que vimos com repeito a $(\mathbb{Z}/n\mathbb{Z})^*$, considerando que p e q não dividem m, vemos que é preciso resolver a equação

$$ts \equiv 1 \pmod{\phi(pq)}.$$

O modo mais fácil de resolver a última congruência linear é fazer

$$ts \equiv t^{\phi(\phi(pq))} \pmod{\phi(pq)} \Rightarrow s \equiv t^{\phi(\phi(pq))-1} \pmod{\phi(pq)}.$$

No entanto, devemos lembrar que $\phi(pq) = (p-1)(q-1)$ e para resolver a congruência é necessário fatorar $\phi(pq)$, o que é computacionalmente complexo, pois devido ao modo como escolhemos os números primos p e q, o tempo estimado para tal tarefa requer alguns anos. Isso faz com que esse algoritmo seja considerado computacionalmente inquebrável.

Abaixo explicitaremos os passos do algoritmo para chaves públicas que estamos apresentando.

1º passo: Escolher, aleatoriamente, dois números primos p e q muito grandes;

2º passo: Calcular pq ;

3º passo: Calcular $\phi(pq) = (p-1)(q-1)$;

4º passo: Escolher um inteiro t tal que $1 < t < \phi(pq)$ e m.d.c.$(t, \phi(pq)) = 1$;

5º passo: Calcular s de forma que $ts \equiv 1 \pmod{\phi(pq)}$.

O par (pq, t) representa uma *chave pública* que pode ser conhecida por todos e utilizada para codificar a mensagem m. Já a terna (p, q, s) representa a *chave privada* que fica guardada em sigilo e serve para decodificar a mensagem criptografada.

Capítulo 2

A Transformada Discreta de Fourier no Círculo Finito $\mathbb{Z}/n\mathbb{Z}$

Daremos continuidade a esse trabalho apresentando a definição de Transformada Discreta de Fourier no circulo finito $\mathbb{Z}/n\mathbb{Z}$. Para isso, iremos definir uma base ortonormal para o espaço de funções complexas $L^2(\mathbb{Z}/n\mathbb{Z})$ e apresentaremos o conceito de convolução de funções. Provaremos que a DFT tem propriedades análogas às do caso contínuo, listaremos as transformadas de certas funções e faremos algumas representações gráficas.

2.1 O que é a Transformada Discreta de Fourier?

Sejam $\mathbb{C}$ corpo dos números complexos e G um grupo finito qualquer. Consideremos o conjunto $L^2(G)$ formado por todas as funções com valores complexos definidas em G, ou seja,

$$L^2(G) := \{f : G \longrightarrow \mathbb{C} \mid f \text{ é uma função}\}.$$

Podemos definir soma e produto por escalar em $L^2(G)$ da seguinte forma:

$$\begin{aligned} (f+g)(x) &= f(x)+g(x); \\ (\lambda f)(x) &= \lambda f(x). \end{aligned}$$

Com essas operações o conjunto $L^2(G)$ é um espaço vetorial complexo, pois as operações aqui definidas têm as propriedades dos itens 3 e 4 da Definição C.1. Além disso, tem dimensão finita (provaremos adiante) e um produto interno definido dado por:

$$\langle f, g\rangle = \sum_{x\in G} f(x)\overline{g(x)}, \text{ para } f, g \in L^2(G). \tag{2.1}$$

Em resumo, $L^2(G)$ é um espaço vetorial sobre o corpo dos complexos com produto interno, ou seja, $L^2(G)$ tem as propriedades da Definição C.10. De fato, sejam $f, g, h \in L^2(G)$ e $\lambda \in \mathbb{C}$:

$$\text{(a) } \langle f, f\rangle = \sum_{x\in G} f(x)\overline{f(x)} = \sum_{x\in G} |f(x)|^2 \Rightarrow \langle f, f\rangle \geq 0.$$

Além disso,

$$\langle f, f\rangle = 0 \Leftrightarrow \sum_{x\in G} |f(x)|^2 = 0 \Leftrightarrow |f(x)| = 0,\ \forall x \in G \Leftrightarrow f = 0.$$

$$\begin{aligned}\text{(b) } \langle f, g\rangle &= \sum_{x\in G} f(x)\overline{g(x)} = \sum_{x\in G} \overline{\overline{f(x)}g(x)} \\ &= \overline{\sum_{x\in G} \overline{f(x)}g(x)} = \overline{\sum_{x\in G} g(x)\overline{f(x)}} = \overline{\langle g, f\rangle}.\end{aligned}$$

$$\begin{aligned}\text{(c) } \langle f+g, h\rangle &= \sum_{x\in G}(f+g)(x)\overline{h(x)} = \sum_{x\in G}[f(x)+g(x)]\overline{h(x)} \\ &= \sum_{x\in G}[f(x)\overline{h(x)} + g(x)\overline{h(x)}] = \sum_{x\in G} f(x)\overline{h(x)} + \sum_{x\in G} g(x)\overline{h(x)} \\ &= \langle f, h\rangle + \langle g, h\rangle.\end{aligned}$$

$$\text{(d) } \langle \lambda f, g\rangle = \sum_{x\in G} \lambda f(x)\overline{g(x)} = \lambda \sum_{x\in G} f(x)\overline{g(x)} = \lambda\langle f, g\rangle.$$

Observação 2.1 *Na demonstração dos itens (a), (b), (c) e (d) acima, foram utilizadas algumas propriedades sobre números complexos que estamos supondo conhecidas e que são fáceis de demonstrar. Vale lembrar também que, de acordo com a Definição C.12, dizemos que duas funções $f, g \in L^2(G)$ são ortogonais quando $\langle f, g\rangle = 0$. Além disso, como $L^2(G)$ é um espaço vetorial com o produto interno dado em (2.1), podemos definir a norma de uma função $f \in L^2(G)$ da seguinte forma:*

$$\|f\| = \langle f, f\rangle^{1/2}. \tag{2.2}$$

Consequentemente, podemos definir uma métrica em $L^2(G)$ por meio da norma (2.2) como sendo $d(f, g) = \|f - g\|$, desse modo, o espaço de funções $L^2(G)$ pode ser tratado como um espaço métrico. Além disso, também é possível provar que ele é um espaço de Hilbert.

A partir daqui, trataremos do espaço de funções complexas definidas sobre o grupo aditivo $\mathbb{Z}/n\mathbb{Z}$, denotado por $L^2(\mathbb{Z}/n\mathbb{Z})$. A seguir, determinaremos uma base ortonormal para esse espaço vetorial.

Consideremos o espaço vetorial complexo $L^2(\mathbb{Z}/n\mathbb{Z})$. Definiremos as funções $\delta_i : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}$, onde $i \in \{0, 1, 2, \cdots, n-1\}$, da seguintes forma:

$$\delta_i(j) \;=\; \begin{cases} 1, & \text{se } i \equiv j \pmod{n} \\ 0, & \text{caso contrário.} \end{cases} \tag{2.3}$$

Proposição 2.1 *O conjunto $\{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$, formado pelas funções definidas em (2.3), constitui uma base ortonormal para o espaço vetorial $L^2(\mathbb{Z}/n\mathbb{Z})$.*

Demonstração: Para mostrar que $\{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$ é uma base ortonormal de $L^2(\mathbb{Z}/n\mathbb{Z})$, devemos provar que este conjunto é ortonormal e gera o espaço de funções.

Por definição, $\delta_i(x) = \begin{cases} 1, & \text{se } i \equiv x \pmod{n} \\ 0, & \text{caso contrário} \end{cases}$, $\forall x \in \mathbb{Z}/n\mathbb{Z}$. Assim, $\overline{\delta_i(x)} = \delta_i(x)$. Desse modo

$$\langle \delta_i, \delta_j \rangle \;=\; \sum_{x=0}^{n-1} \delta_i(x)\overline{\delta_j(x)} = \sum_{x=0}^{n-1} \delta_i(x)\delta_j(x)$$

Se $i \not\equiv j \pmod{n}$ então, para todo $x \in \mathbb{Z}/n\mathbb{Z}$, apenas uma das seguintes alternativas ocorre:

(i) $\delta_i(x) = 1$ e $\delta_j(x) = 0$;
(ii) $\delta_i(x) = 0$ e $\delta_j(x) = 1$;
(iii) $\delta_i(x) = \delta_j(x) = 0$.

Em todos os casos, $\delta_i(x)\delta_j(x) = 0$, logo,

$$\langle \delta_i, \delta_j \rangle = \sum_{x=0}^{n-1} \delta_i(x)\delta_j(x) = 0.$$

Se $i \equiv j \pmod{n}$, então existe $x_0 \in \mathbb{Z}/n\mathbb{Z}$ tal que $x_0 \equiv i \pmod{n}$ e $j \equiv x_0 \pmod{n}$, ou seja, $\delta_i(x_0) = \delta_j(x_0) = 1$. Além disso, para todo $x \in \mathbb{Z}/n\mathbb{Z} \setminus \{x_0\}$ temos que

$$x \not\equiv i \pmod{n} \text{ e } x \not\equiv j \pmod{n} \Rightarrow \delta_i(x) = \delta_j(x) = 0.$$

Assim

$$\langle \delta_i, \delta_j \rangle = \sum_{x=0}^{n-1} \delta_i(x)\delta_j(x) = \delta_i(x_0)\delta_j(x_0) + \sum_{x \in G'} \delta_i(x)\delta_j(x) = 1 + 0 = 1,$$

onde $G' = \mathbb{Z}/n\mathbb{Z} \setminus \{x_0\}$.

Pelo que foi exposto acima, podemos concluir que

$$\langle \delta_i, \delta_j \rangle = \begin{cases} 1, & \text{se } i \equiv j \pmod{n} \\ 0, & \text{caso contrário.} \end{cases} \tag{2.4}$$

A equação (2.4) nos diz que quaisquer duas funções delta distintas são ortogonais, ou seja, $\{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$ é um conjunto de vetores ortogonais em $L^2(\mathbb{Z}/n\mathbb{Z})$, e, pelo Teorema C.3, é um conjunto LI. Além disso, $\|\delta_i\| = \langle \delta_i, \delta_i \rangle = 1$, para todo $i \in \{0,\ 1,\ \cdots,\ n-1\}$, ou seja, $\{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$ é um conjunto de vetores ortonormais. Resta provar que o conjunto das funções delta gera $L^2(\mathbb{Z}/n\mathbb{Z})$, ou seja, que toda função $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ pode ser escrita como combinação linear das funções delta.

Como $\delta_a(x) = 1$ para $a \equiv x \pmod{n}$ e $\delta_a(x) = 0$ para $a \not\equiv x \pmod{n}$, temos que

$$f(0) = f(0)\delta_0(0),\ f(1) = f(1)\delta_1(1), \cdots,\ f(n-1) = f(n-1)\delta_{n-1}(n-1).$$

Assim, fica fácil perceber que

$$f(x) = f(0)\delta_0(x) + f(1)\delta_1(x) + f(n-1)\delta_{n-1}(x),$$

ou seja,

$$f(x) = \sum_{a=0}^{n-1} f(a)\delta_a(x). \tag{2.5}$$

Com isso, concluímos a demonstração da proposição. ∎

Observação 2.2 *A Proposição 2.1, apresentada acima, nos mostra que o conjunto* $\mathscr{B} = \{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$ *é uma base ortonormal do espaço* $L^2(\mathbb{Z}/n\mathbb{Z})$ *e, consequentemente,* $\dim L^2(\mathbb{Z}/n\mathbb{Z}) = n$*, já que essa base possui n elementos. Além disso, a demonstração dessa proposição nos mostra como determinar as coordenadas de uma função* $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ *na base* $\mathscr{B}$ *por meio da equação (2.5).*

Observação 2.3 *Consideremos a transformação* $T : L^2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathbb{C}^n$ *definida por*

$$T(f) = (f(0),\ f(1),\ \cdots,\ f(n-1)).$$

É possível provar que T *é uma transformação linear bijetora, ou seja,* T *é um isomorfismo de* $L^2(\mathbb{Z}/n\mathbb{Z})$ *em* $\mathbb{C}^n$*. Desse modo, esses espaços vetoriais têm as mesmas propriedades algébricas e podem ser representados um pelo outro. No Teorema C.1, do Apêndice C, apresentamos uma prova para esse fato, numa abordagem mais geral.*

Agora, podemos definir convolução para funções de $L^2(\mathbb{Z}/n\mathbb{Z})$ e mostrar algumas propriedades importantes. Nesse caso, iremos tratar $\mathbb{Z}/n\mathbb{Z}$ como um grupo aditivo.

Definição 2.1 *Consideremos duas funções $f, g \in L^2(\mathbb{Z}/n\mathbb{Z})$. A* convolução $f * g$ *é definida da seguinte forma:*

$$(f * g)(x) = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)g(x-y), \text{ para } x \in \mathbb{Z}/n\mathbb{Z}.$$

Notemos, aqui, que a convolução de funções $*$ associa cada par de funções f, g de $L^2(\mathbb{Z}/n\mathbb{Z})$ a uma função $f * g \in L^2(\mathbb{Z}/n\mathbb{Z})$. Em seguida, mostraremos algumas propriedades da convolução de funções.

Proposição 2.2 *Sejam $f, g, h \in L^2(\mathbb{Z}/n\mathbb{Z})$. As seguintes propriedades são verdadeiras.*

(a) $f * g = g * f$ **(comutatividade)**;

(b) $f * (g * h) = (f * g) * h$ **(associatividade)**;

(c) $f * (g + h) = f * g + f * h$ **(distributividade com relação à adição)**;

(d) *se δ_a e δ_b são funções delta definidas em (2.3), então:*

$$\begin{aligned} \delta_a * \delta_b &= \delta_{a+b \pmod n}; \\ (f * \delta_a)(x) &= f(x-a). \end{aligned}$$

Demonstração:

$$\begin{aligned} (a)\ (f * g)(x) &= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)g(x-y), \text{ para } x \in \mathbb{Z}/n\mathbb{Z} \\ &= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} g(x-y)f(y), \text{ tomando } x - y \equiv z \pmod n \\ &= \sum_{z \in \mathbb{Z}/n\mathbb{Z}} g(z)f(x-z) = (g * f)(x). \\ (b)\ [f * (g * h)](x) &= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)(g * h)(x-y), \text{ para } x \in \mathbb{Z}/n\mathbb{Z} \\ &= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y) \sum_{z \in \mathbb{Z}/n\mathbb{Z}} g(z)(h)(x-y-z). \end{aligned}$$

Sabendo que $y + z \equiv w \pmod{n} \Rightarrow z \equiv w - y \pmod{n}$ temos

$$\begin{aligned}
[f * (g * h)](x) &= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y) \sum_{w \in \mathbb{Z}/n\mathbb{Z}} g(w-y)(h)(x-w) \\
&= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \sum_{w \in \mathbb{Z}/n\mathbb{Z}} f(y) g(w-y)(h)(x-w) \\
&= \sum_{w \in \mathbb{Z}/n\mathbb{Z}} \left[\sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y) g(w-y) \right] (h)(x-w) \\
&= \sum_{w \in \mathbb{Z}/n\mathbb{Z}} (f * g)(w)(h)(x-w) \\
&= [(f * g) * h](x).
\end{aligned}$$

$$\begin{aligned}
(c)\ [f * (g + h)](x) &= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)(g+h)(x-y), \text{ para } x \in \mathbb{Z}/n\mathbb{Z} \\
&= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)[g(x-y) + h(x-y)] \\
&= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} [f(y)g(x-y) + f(y)h(x-y)] \\
&= \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)g(x-y) + \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)h(x-y) \\
&= (f * g)(x) + (f * h)(x).
\end{aligned}$$

(d) Provaremos, inicialmente, que $\delta_a * \delta_b = \delta_{a+b \pmod{n}}$. Sabemos que $(\delta_a * \delta_b)(x) = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \delta_a(y)\delta_b(x-y)$. Da equação (2.3), temos que

$$\sum_{y \in \mathbb{Z}/n\mathbb{Z}} \delta_a(y)\delta_b(x-y) = 1 \text{ ou } \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \delta_a(y)\delta_b(x-y) = 0.$$

O primeiro caso ocorre se, e somente se, uma das parcelas do somatório não for nula, o que é verdade se, e somente se, $a \equiv y \pmod{n}$ e $b \equiv x - y \pmod{n}$, para algum par $x, y \in \mathbb{Z}/n\mathbb{Z}$, o que nos dá, por meio da soma das equivalências, $a + b \equiv x \pmod{n}$.

Do contrário, $(\delta_a * \delta_b)(x) = 0$. Em resumo

$$(\delta_a * \delta_b)(x) = \begin{cases} 1, & \text{se } a+b \equiv x \pmod{n} \\ 0, & \text{caso contrário} \end{cases} \Rightarrow \delta_a * \delta_b = \delta_{a+b \pmod{n}}.$$

Resta provar que $(f * \delta_a)(x) = f(x-a)$. De fato, como $\delta_a(x-y) = 1$ se, e somente se, $a \equiv x - y \pmod{n}$, e sabendo que a última equivalência implica em $y \equiv x - a \pmod{n}$, podemos concluir que

$$(f * \delta_a)(x) = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y)\delta_a(x-y) = f(x-a)\delta_a(a) = f(x-a) \cdot 1 = f(x-a).$$

■

Exemplo 2.1 *Vamos determinar a convolução para as funções* $f = \delta_4 + \delta_5 + \delta_6$ *e* $g = \delta_{-3} + \delta_{-1} + \delta_0$ *em* $L^2(\mathbb{Z}/15\mathbb{Z})$. *Para isso, iremos aplicar os itens (a), (c) e (d) da Proposição 2.2. Vejamos:*

$$\begin{aligned} f * g &= f * (\delta_{-3} + \delta_{-1} + \delta_0) \\ &= f * \delta_{-3} + f * \delta_{-1} + f * \delta_0 \\ &= \delta_{-3} * f + \delta_{-1} * f + \delta_0 * f \\ &= \delta_{-3} * (\delta_4 + \delta_5 + \delta_6) + \delta_{-1} * (\delta_4 + \delta_5 + \delta_6) + \delta_0 * (\delta_4 + \delta_5 + \delta_6) \\ &= \delta_{-3} * \delta_4 + \delta_{-3} * \delta_5 + \delta_{-3} * \delta_6 + \delta_{-1} * \delta_4 + \delta_{-1} * \delta_5 + \delta_{-1} * \delta_6 \\ &+ \delta_0 * \delta_4 + \delta_0 * \delta_5 + \delta_0 * \delta_6 \\ &= \delta_{-3+4} + \delta_{-3+5} + \delta_{-3+6} + \delta_{-1+4} + \delta_{-1+5} + \delta_{-1+6} + \delta_{0+4} + \delta_{0+5} + \delta_{0+6} \\ &= \delta_1 + \delta_2 + \delta_3 + \delta_3 + \delta_4 + \delta_5 + \delta_4 + \delta_5 + \delta_6 \\ &= \delta_1 + \delta_2 + 2\delta_3 + 2\delta_4 + 2\delta_5 + \delta_6. \end{aligned}$$

Vejamos a representação gráfica das funções f, g *e* $f * g$.

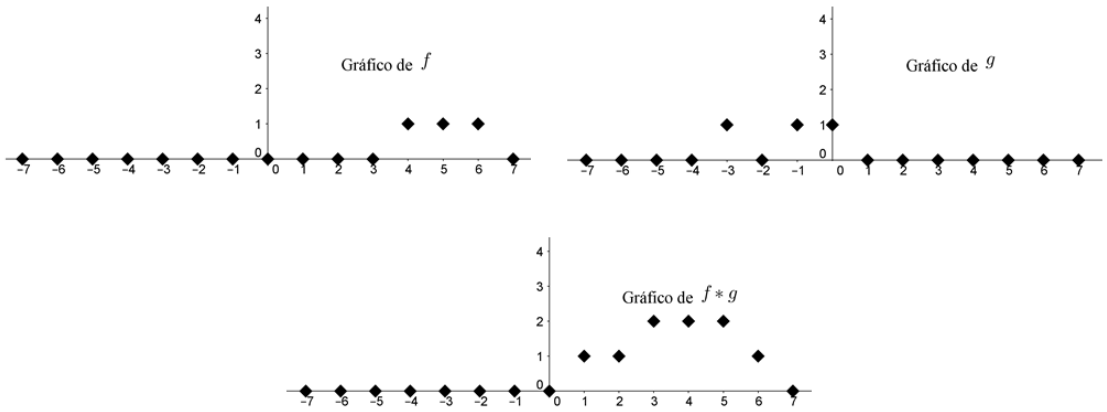

Figura 2.1: Exemplo de convolução discreta para funções de $L^2(\mathbb{Z}/15\mathbb{Z})$.

Observação 2.4 *No Exemplo 2.1, como* $-1 \equiv 14 \pmod{15}$ *e* $-3 \equiv 12 \pmod{15}$*, temos que* $\delta_{-1} = \delta_{14}$ *e* $\delta_{-3} = \delta_{12}$*.*

Continuaremos nossa discussão relembrando que podemos obter uma relação entre as funções exponenciais e as funções trigonométricas através da fórmula de Euler:

$$e^{ix} = \cos x + i\,\mathrm{sen}x, \text{ onde } i^2 = -1 \text{ e } x \in \mathbb{R}.$$

A seguir, consideremos o subgrupo multiplicativo dos números complexos de módulo 1, isto é,

$$\mathbb{T} := \{z \in \mathbb{C} \mid |z| = 1\}.$$

Proposição 2.3 *Seja* $a \in \mathbb{Z}/n\mathbb{Z}$*. A função* $e_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{T}$ *definida por*

$$e_a(x) = \exp\left(\frac{2\pi i a x}{n}\right)$$

é um homomorfismo do grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ *no grupo multiplicativo* $\mathbb{T}$*.*

Demonstração: De acordo com a Definição B.4 devemos mostrar que, para quaisquer $x, y \in \mathbb{Z}/n\mathbb{Z}$, $e_a(x+y) = e_a(x) \cdot e_a(y)$. De fato

$$\begin{aligned} e_a(x+y) &= \exp\left(\frac{2\pi i a(x+y)}{n}\right) = \exp\left(\frac{2\pi i a x + 2\pi i a y}{n}\right) \\ &= \exp\left(\frac{2\pi i a x}{n} + \frac{2\pi i a y}{n}\right) \\ &= \exp\left(\frac{2\pi i a x}{n}\right) \cdot \exp\left(\frac{2\pi i a y}{n}\right) \\ &= e_a(x) \cdot e_a(y). \end{aligned}$$

Portanto, e_a é um homomorfismo de grupos. ∎

Observação 2.5 *Os homomorfismos apresentados na Proposição 2.3 são, usualmente, chamados* caracteres *de* $\mathbb{Z}/n\mathbb{Z}$*.*

Para encerrar esta secção, iremos definir a Transformada discreta de Fourier no círculo finito $\mathbb{Z}/n\mathbb{Z}$.

Definição 2.2 *A* transformada discreta de Fourier (ou simplesmente DFT) *de uma função* $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ *é definida por*

$$\mathscr{F}_n f(x) = \mathscr{F} f(x) = \hat{f}(x) = \sum_{y \in \mathbb{Z}/n\mathbb{Z}} f(y) e_x(-y).$$

Aqui, e_x *é a exponencial tratada na Proposição 2.3.*

O seguinte fato é uma consequência imediata da Definição 2.2:

$$\mathscr{F}f(x) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)e_x(-y) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\overline{e_x(y)} = \langle f, e_x\rangle.$$

Observação 2.6 *Na próxima secção mostraremos algumas propriedades da DFT em $L^2(\mathbb{Z}/n\mathbb{Z})$. Em tais demonstrações faremos uso, na maioria dos casos, da Definição 2.2, de propriedades dos números complexos, de funções exponenciais e faremos algumas mudanças nos índices dos somatórios. Porém, os seguinte fato pode nos fornecer um outro ponto de vista sobre a DFT em $L^2(\mathbb{Z}/n\mathbb{Z})$. De acordo com as definições de DFT e convolução em $L^2(\mathbb{Z}/n\mathbb{Z})$ temos que*

$$\mathscr{F}f(x) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)e_x(-y) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)e_x(0-y) = f * e_x(0). \tag{2.6}$$

Um exercício interessante é tentar provar algumas das propriedades que veremos na próxima secção utilizando o fato mostrado na equação (2.6). Nesse caso, podemos utilizar as propriedades da convolução.

2.2 As Propriedades da DFT em $\mathbb{Z}/n\mathbb{Z}$

Iniciaremos esta secção determinando a matriz da transformada discreta de Fourier no círculo finito $\mathbb{Z}/n\mathbb{Z}$ com relação à base das funções $\mathscr{B} = \{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$ em $L^2(\mathbb{Z}/n\mathbb{Z})$.

Seja f uma função qualquer de $L^2(\mathbb{Z}/n\mathbb{Z})$. Pela equação (2.5), podemos escrever f como combinação linear das funções delta da seguinte forma:

$$f(x) = \sum_{a=0}^{n-1} f(a)\delta_a(x).$$

Assim, a matriz da função f com relação à base $\mathscr{B}$ é:

$$[f]_{\mathscr{B}} = \begin{pmatrix} f(0) \\ f(1) \\ \vdots \\ f(n-1). \end{pmatrix}.$$

De modo análogo, como $\mathscr{F}f$ também é uma função de $L^2(\mathbb{Z}/n\mathbb{Z})$, sua matriz com relação à base $\mathscr{B}$ é:

$$[\mathscr{F}f]_{\mathscr{B}} = \begin{pmatrix} \mathscr{F}f(0) \\ \mathscr{F}f(1) \\ \vdots \\ \mathscr{F}f(n-1) \end{pmatrix}.$$

Por outro lado, a Definição 2.2 nos diz que

$$\begin{aligned}\mathscr{F}f(x) &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)e_x(-y) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\exp\left(\frac{2\pi ix(-y)}{n}\right)\\ &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\left[\exp\left(\frac{2\pi i}{n}\right)\right]^{-xy} = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\omega^{-xy}.\end{aligned} \tag{2.7}$$

onde $\omega = \exp(2\pi i/n)$ é a e-ésima raiz primitiva da unidade complexa, como vimos no Exemplo 1.10. Atribuindo valores para x na equação (2.7) temos:

$$\left\{\begin{array}{rl} \mathscr{F}f(0) &= \displaystyle\sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\omega^{-0\cdot y}\\ \mathscr{F}f(1) &= \displaystyle\sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\omega^{-1\cdot y}\\ &\vdots\\ \mathscr{F}f(n-1) &= \displaystyle\sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)\omega^{-(n-1)\cdot y}\end{array}\right. \Rightarrow$$

$$\Rightarrow \left\{\begin{array}{rl} \mathscr{F}f(0) &= f(0)\omega^{-0\cdot 0} + f(1)\omega^{-0\cdot 1} + \cdots + f(n-1)\omega^{-0\cdot(n-1)}\\ \mathscr{F}f(1) &= f(0)\omega^{-1\cdot 0} + f(1)\omega^{-1\cdot 1} + \cdots + f(n-1)\omega^{-1\cdot(n-1)}\\ &\vdots\\ \mathscr{F}f(n-1) &= f(0)\omega^{-(n-1)\cdot 0} + f(1)\omega^{-(n-1)\cdot 1} + \cdots + f(n-1)\omega^{-(n-1)\cdot(n-1)}\end{array}\right. \tag{2.8}$$

O sistema de equações (2.8) pode ser representado por matrizes da seguinte forma:

$$\begin{pmatrix} \mathscr{F}f(0)\\ \mathscr{F}f(1)\\ \vdots\\ \mathscr{F}f(n-1)\end{pmatrix} = \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-0\cdot 1} & \cdots & \omega^{-0\cdot(n-1)}\\ \omega^{-1\cdot 0} & \omega^{-1\cdot 1} & \cdots & \omega^{-1\cdot(n-1)}\\ \vdots & \vdots & \ddots & \vdots\\ \omega^{-(n-1)\cdot 0} & \omega^{-(n-1)\cdot 1} & \cdots & \omega^{-(n-1)\cdot(n-1)}\end{pmatrix}\begin{pmatrix} f(0)\\ f(1)\\ \vdots\\ f(n-1)\end{pmatrix}.$$

Com isso, podemos concluir que a matriz da DFT na base $\{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$ é

$$F_n = \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-0\cdot 1} & \cdots & \omega^{-0\cdot(n-1)}\\ \omega^{-1\cdot 0} & \omega^{-1\cdot 1} & \cdots & \omega^{-1\cdot(n-1)}\\ \vdots & \vdots & \ddots & \vdots\\ \omega^{-(n-1)\cdot 0} & \omega^{-(n-1)\cdot 1} & \cdots & \omega^{-(n-1)\cdot(n-1)}\end{pmatrix},$$

onde $\omega = \exp(2\pi i/n)$ é uma raiz e-ésima primitiva da unidade complexa. Essa matriz ainda pode ser representada por:

$$F_n = \left(\omega^{-(j-1)(k-1)}\right)_{1\leq j,k\leq n} \tag{2.9}$$

onde j e k representam, respectivamente, a j-ésima linha e k-ésima coluna da matriz F_n.

Exemplo 2.2 *Vamos determinar a matriz da DFT no caso em que $n = 4$, ou seja, em $L^2(\mathbb{Z}/4\mathbb{Z})$. De acordo com a equação (2.9),*

$$F_4 = \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-0\cdot 1} & \omega^{-0\cdot 2} & \omega^{-0\cdot 3} \\ \omega^{-1\cdot 0} & \omega^{-1\cdot 1} & \omega^{-1\cdot 2} & \omega^{-1\cdot 3} \\ \omega^{-2\cdot 0} & \omega^{-2\cdot 1} & \omega^{-2\cdot 2} & \omega^{-2\cdot 3} \\ \omega^{-3\cdot 0} & \omega^{-3\cdot 1} & \omega^{-3\cdot 2} & \omega^{-3\cdot 3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} \\ 1 & \omega^{-2} & \omega^{-4} & \omega^{-6} \\ 1 & \omega^{-3} & \omega^{-6} & \omega^{-9} \end{pmatrix},$$

onde $\omega = \exp(2\pi i/4) = \exp(\pi i/2)$. Assim

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{-\frac{\pi i}{2}} & e^{-\frac{2\pi i}{2}} & e^{-\frac{3\pi i}{2}} \\ 1 & e^{-\frac{2\pi i}{2}} & e^{-\frac{4\pi i}{2}} & e^{-\frac{6\pi i}{2}} \\ 1 & e^{-\frac{3\pi i}{2}} & e^{-\frac{6\pi i}{2}} & e^{-\frac{9\pi i}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{-\frac{\pi i}{2}} & e^{-\pi i} & e^{-\frac{3\pi i}{2}} \\ 1 & e^{-\pi i} & e^{-2\pi i} & e^{-3\pi i} \\ 1 & e^{-\frac{3\pi i}{2}} & e^{-3\pi i} & e^{-\frac{9\pi i}{2}} \end{pmatrix}. \tag{2.10}$$

Aplicando a fórmula de Euler nos elementos da matriz (2.10) obtemos

$$\begin{array}{rcrcr} e^{-\frac{\pi i}{2}} & = & \cos\left(-\frac{\pi}{2}\right) + i\,\mathrm{sen}\left(-\frac{\pi}{2}\right) & = & -i; \\ e^{-\frac{3\pi i}{2}} & = & \cos\left(-\frac{3\pi}{2}\right) + i\,\mathrm{sen}\left(-\frac{3\pi}{2}\right) & = & i; \\ e^{-\frac{9\pi i}{2}} & = & \cos\left(-\frac{9\pi}{2}\right) + i\,\mathrm{sen}\left(-\frac{9\pi}{2}\right) & = & -i; \\ e^{-\pi i} & = & \cos(-\pi) + i\,\mathrm{sen}(-\pi) & = & -1; \\ e^{-2\pi i} & = & \cos(-2\pi) + i\,\mathrm{sen}(-2\pi) & = & 1; \\ e^{-3\pi i} & = & \cos(-3\pi) + i\,\mathrm{sen}(-3\pi) & = & -1. \end{array}$$

Portanto,

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

O seguinte lema nos mostrará as relações de ortogonalidade dos caracteres de $\mathbb{Z}/n\mathbb{Z}$.

Lema 2.1 *Seja $e_a(b) = \exp(2\pi iab/n)$, para $a, b \in \mathbb{Z}/n\mathbb{Z}$. Então:*

$$\langle e_x, e_y\rangle = \left\{ \begin{array}{ll} n, & \text{se } x \equiv y \pmod{n} \\ 0, & \text{caso contrário} \end{array} \right\} = n\delta_x(y).$$

Em particular,

$$\langle e_a, e_0\rangle = \left\{ \begin{array}{ll} n, & \text{se } a \equiv 0 \pmod{n} \\ 0, & \text{caso contrário} \end{array} \right\} = n\delta_0(a).$$

Demonstração: De acordo com a equação (2.1) temos que

$$\begin{aligned} \langle e_x, e_y\rangle &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}} e_x(b)\overline{e_y(b)} = \sum_{b\in\mathbb{Z}/n\mathbb{Z}} e_x(b)e_y(-b) \\ &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i x b}{n}\right)\exp\left(\frac{-2\pi i y b}{n}\right) \\ &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i (x-y) b}{n}\right). \end{aligned}$$

Se $x \equiv y \pmod{n}$, então $x - y \equiv 0 \pmod{n}$, logo

$$\langle e_x, e_y\rangle = \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i \cdot 0 \cdot b}{n}\right) = \sum_{b=0}^{n-1} e^0 = \sum_{b=0}^{n-1} 1 = n.$$

Suponhamos, agora, que $x \not\equiv y \pmod{n}$ e seja $S = \displaystyle\sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(x-y)b}{n}\right)$.

$$\begin{aligned} \exp\left(\frac{2\pi i(x-y)}{n}\right) S &= \exp\left(\frac{2\pi i(x-y)}{n}\right) \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(x-y)b}{n}\right) \\ &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(x-y)}{n}\right) \cdot \exp\left(\frac{2\pi i(x-y)b}{n}\right) \\ &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(x-y)}{n} + \frac{2\pi i(x-y)b}{n}\right) \\ &= \sum_{b\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(x-y)(b+1)}{n}\right) \\ &= \sum_{d\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(x-y)d}{n}\right), \text{ tomando } b+1 \equiv d \pmod{n} \\ &= S. \end{aligned}$$

Acabamos de mostrar que $\exp\left(\frac{2\pi i(x-y)}{n}\right) S = S$. Como $x \not\equiv y \pmod{n}$, ou seja, $x - y$ não é múltiplo de n, temos que

$$\exp\left(\frac{2\pi i(x-y)}{n}\right) = \cos\left(\frac{2\pi(x-y)}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi(x-y)}{n}\right) \neq 1,$$

portanto

$$\exp\left(\frac{2\pi i(x-y)}{n}\right)S = S \Rightarrow \left[\exp\left(\frac{2\pi i(x-y)}{n}\right) - 1\right]S = 0 \Rightarrow S = 0.$$

Logo

$$\langle e_x, e_y\rangle = \left\{ \begin{array}{ll} n, & \text{se } x \equiv y \pmod{n} \\ 0, & \text{caso contrário} \end{array} \right\} = n\delta_x(y).$$

Particularmente, temos que

$$\langle e_a, e_0\rangle = \left\{ \begin{array}{ll} n, & \text{se } a \equiv 0 \pmod{n} \\ 0, & \text{caso contrário} \end{array} \right\} = n\delta_0(a).$$

■

O seguinte teorema nos mostra algumas propriedades básicas da DFT no círculo finito.

Teorema 2.1 *Consideremos a função* $\mathscr{F} : L^2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow L^2(\mathbb{Z}/n\mathbb{Z})$ *dada por*

$$\mathscr{F}f(x) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)e_x(-y).$$

As seguintes propriedades são verdadeiras:

(a) $\mathscr{F}$ *é uma transformação linear bijetora;*

(b) $\mathscr{F}(f * g)(x) = \mathscr{F}f(x) \cdot \mathscr{F}g(x)$ **(convolução)**;

(c) $f(x) = \dfrac{1}{n}\mathscr{F}\mathscr{F}f(-x) = \dfrac{1}{n}\displaystyle\sum_{y\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(y)\exp\left(\frac{2\pi ixy}{n}\right)$ **(inversão)**;

(d) $\langle f, f\rangle = \dfrac{1}{n}\langle \hat{f}, \hat{f}\rangle$ **(Teorema de Plancherel ou Igualdade de Parseval)**.

Demonstração:

(a) Provaremos, inicialmente, que $\mathscr{F}$ é uma transformação linear. Para tanto, consideremos $f, g \in L^2(\mathbb{Z}/n\mathbb{Z})$ e $\lambda \in \mathbb{C}$ quaisquer.

$$\begin{aligned} \mathscr{F}(\lambda f + g)(x) &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} (\lambda f + g)(y)e_x(-y) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} [\lambda f(y) + g(y)]e_x(-y) \\ &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \lambda f(y)e_x(-y) + g(y)e_x(-y) \\ &= \lambda \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(y)e_x(-y) + \sum_{y\in\mathbb{Z}/n\mathbb{Z}} g(y)e_x(-y) \\ &= \lambda\mathscr{F}f(x) + \mathscr{F}g(x). \end{aligned}$$

O fato de que $\mathscr{F}$ é bijetora será demonstrado no item (c), onde explicitaremos uma fórmula para o cálculo da transformada inversa.

(b) Sejam f e g funções quaisquer em $L^2(\mathbb{Z}/n\mathbb{Z})$.

$$\begin{aligned}\mathscr{F}(f*g)(x) &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} (f*g)(y)e_x(-y) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} (f*g)(y)\exp\left(\frac{-2\pi ixy}{n}\right)\\ &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}}\sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)g(y-z)\exp\left(\frac{-2\pi ixy}{n}\right).\end{aligned}$$

Sabendo que $y - z \equiv w \pmod{n} \Rightarrow y \equiv z + w \pmod{n}$, obtemos

$$\begin{aligned}\mathscr{F}(f*g)(x) &= \sum_{w\in\mathbb{Z}/n\mathbb{Z}}\sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)g(w)\exp\left(\frac{-2\pi ix(z+w)}{n}\right)\\ &= \sum_{z\in\mathbb{Z}/n\mathbb{Z}}\sum_{w\in\mathbb{Z}/n\mathbb{Z}} f(z)g(w)\exp\left(\frac{-2\pi ixz}{n}+\frac{-2\pi ixw}{n}\right)\\ &= \sum_{z\in\mathbb{Z}/n\mathbb{Z}}\sum_{w\in\mathbb{Z}/n\mathbb{Z}} f(z)g(w)\exp\left(\frac{-2\pi ixz}{n}\right)\exp\left(\frac{-2\pi ixw}{n}\right)\\ &= \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\exp\left(\frac{-2\pi ixz}{n}\right)\cdot\sum_{w\in\mathbb{Z}/n\mathbb{Z}} g(w)\exp\left(\frac{-2\pi ixw}{n}\right)\\ &= \mathscr{F}f(x)\cdot\mathscr{F}g(x).\end{aligned}$$

(c) Vamos provar, inicialmente, que a fórmula para a inversão de $\mathscr{F}$ é válida para as funções $\{\delta_0,\ \delta_1,\ \cdots,\ \delta_{n-1}\}$. A transformada de Fourier para uma função δ_a é

$$\mathscr{F}\delta_a(x) = \hat{\delta}_a(x) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \delta_a(y)e_x(-y),\ \text{para } a, x \in \mathbb{Z}/n\mathbb{Z}.$$

Logo

$$\mathscr{F}\delta_a(x) = \delta_a(a)\exp\left(\frac{-2\pi ixa}{n}\right) = 1\cdot\exp\left(\frac{-2\pi ixa}{n}\right) = \exp\left(\frac{-2\pi ixa}{n}\right).$$

Portanto,

$$\begin{aligned}
\mathscr{F}\mathscr{F}\delta_a(-x) &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \hat{\delta}_a(-x)e_{-x}(-y) \\
&= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi i(-x)a}{n}\right)\exp\left(\frac{-2\pi i(-x)y}{n}\right) \\
&= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{-2\pi ixa}{n}\right)\exp\left(\frac{2\pi ixy}{n}\right) \\
&= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{-2\pi ixa}{n}+\frac{2\pi ixy}{n}\right) \\
&= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \exp\left(\frac{2\pi ix(y-a)}{n}\right),
\end{aligned}$$

onde concluímos, por meio do Lema 2.1, que

$$\mathscr{F}\mathscr{F}\delta_a(-x) = n\delta_a(x) \Rightarrow \delta_a(x) = \frac{1}{n}\mathscr{F}\mathscr{F}\delta_a(-x).$$

Consideremos, agora, uma função qualquer $f \in L^2(\mathbb{Z}/n\mathbb{Z})$. Pela equação (2.5) podemos escrever f como combinação linear das funções delta da seguinte forma

$$\begin{aligned}
f(x) &= \sum_{a=0}^{n-1} f(a)\delta_a(x) = f(0)\delta_0(x) + f(1)\delta_1(x) + \cdots + f(n-1)\delta_{n-1}(x) \\
&= f(0)\frac{1}{n}\mathscr{F}\mathscr{F}\delta_0(-x) + f(1)\frac{1}{n}\mathscr{F}\mathscr{F}\delta_1(-x) + \cdots + f(n-1)\frac{1}{n}\mathscr{F}\mathscr{F}\delta_{n-1}(-x).
\end{aligned}$$

Como $\mathscr{F}$ é linear, temos:

$$\begin{aligned}
f(x) &= \frac{1}{n}[\mathscr{F}\mathscr{F}f(0)\delta_0(-x) + \mathscr{F}\mathscr{F}f(1)\delta_1(-x) + \cdots + \mathscr{F}\mathscr{F}f(n-1)\delta_{n-1}(-x)] \\
&= \frac{1}{n}\mathscr{F}\mathscr{F}[f(0)\delta_0(-x) + f(1)\delta_1(-x) + \cdots + f(n-1)\delta_{n-1}(-x)] \\
&= \frac{1}{n}\mathscr{F}\mathscr{F}f(-x).
\end{aligned}$$

Portanto,

$$f(x) = \frac{1}{n}\mathscr{F}\mathscr{F}f(-x) = \frac{1}{n}\sum_{y\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(y)\exp\left(\frac{2\pi ixy}{n}\right).$$

(d) Para demonstrar o Teorema de Plancherel (ou Igualdade de Parseval) utilizaremos um método que consiste em provar o resultado mais geral que segue

$$\langle f, g\rangle = \frac{1}{n}\langle \hat{f}, \hat{g}\rangle, \text{ para } f, g \in L^2(\mathbb{Z}/n\mathbb{Z}). \tag{2.11}$$

Para quaisquer $a \in \mathbb{Z}/n\mathbb{Z}$ e $g \in L^2(\mathbb{Z}/n\mathbb{Z})$ temos que

$$\langle \delta_a, g \rangle = \sum_{x=0}^{n-1} \delta_a(x)\overline{g(x)} = \delta_a(a)\overline{g(a)} = \overline{g(a)}.$$

Pelo item (c) do Teorema 2.1 temos que

$$\begin{aligned} \langle \delta_a, g \rangle &= \overline{g(a)} = \frac{1}{n} \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \overline{\hat{g}(y)}\ \overline{\exp\left(2\pi i a y/n\right)} \\ &= \frac{1}{n} \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \exp\left(-2\pi i a y/n\right)\ \overline{\hat{g}(y)}. \end{aligned}$$

Na demonstração do item (c) vimos que $\exp\left(-2\pi i a y/n\right) = \hat{\delta}_a(y)$, logo,

$$\langle \delta_a, g \rangle = \frac{1}{n} \sum_{y \in \mathbb{Z}/n\mathbb{Z}} \hat{\delta}_a(y)\ \overline{\hat{g}(y)} = \frac{1}{n}\langle \hat{\delta}_a, \hat{g} \rangle.$$

Agora, consideremos uma função $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ qualquer. Sabemos que

$$f(x) = \sum_{a=0}^{n-1} f(a)\delta_a(x)$$

e que o produto interno de funções da Definição 2.1 é linear. Dessa forma

$$\begin{aligned} \langle f, g \rangle &= \left\langle \sum_{a=0}^{n-1} f(a)\delta_a,\ g \right\rangle = \sum_{a=0}^{n-1} f(a)\langle \delta_a, g \rangle \\ &= \sum_{a=0}^{n-1} f(a)\frac{1}{n}\langle \mathscr{F}\delta_a,\ \mathscr{F}g \rangle = \frac{1}{n}\left\langle \sum_{a=0}^{n-1} f(a)\mathscr{F}\delta_a,\ \mathscr{F}g \right\rangle \\ &= \frac{1}{n}\left\langle \sum_{a=0}^{n-1} \mathscr{F}f(a)\delta_a,\ \mathscr{F}g \right\rangle = \frac{1}{n}\left\langle \mathscr{F}\sum_{a=0}^{n-1} f(a)\delta_a,\ \mathscr{F}g \right\rangle \\ &= \frac{1}{n}\langle \mathscr{F}f,\ \mathscr{F}g \rangle = \frac{1}{n}\left\langle \hat{f}, \hat{g} \right\rangle. \end{aligned}$$

Acabamos de provar a equação (2.11). Tomando $g = f$ podemos concluir que

$$\langle f, f \rangle = \frac{1}{n}\langle \hat{f}, \hat{f} \rangle.$$

■

Para encerrar esta secção, mostraremos as propriedades de translação e dilatação da DFT no círculo finito $\mathbb{Z}/n\mathbb{Z}$.

Teorema 2.2 (Translação) *Seja a um elemento qualquer de $\mathbb{Z}/n\mathbb{Z}$. Consideremos a função $T_a : L^2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow L^2(\mathbb{Z}/n\mathbb{Z})$ definida por $T_a f(x) = f(x-a)$, então*

$$\mathscr{F}(T_a f)(x) = \exp(-2\pi i a x/n)\,\mathscr{F} f(x).$$

Demonstração: Sejam $a \in \mathbb{Z}/n\mathbb{Z}$ e $f \in L^2(\mathbb{Z}/n\mathbb{Z})$ quaisquer. O item (d) da Proposição 2.2 nos diz que

$$T_a f(x) = f(x-a) = (\delta_a * f)(x),\ \forall x \in \mathbb{Z}/n\mathbb{Z}.$$

Dessa forma

$$\begin{aligned}\mathscr{F}(T_a f)(x) &= \mathscr{F}(\delta_a * f)(x)\\ &= \mathscr{F}\delta_a(x)\cdot\mathscr{F} f(x), \qquad \text{(item (b) do Teorema 2.1)}\\ &= \exp(-2\pi i a x/n)\,\mathscr{F} f(x).\end{aligned}$$

■

Teorema 2.3 (Dilatação) *Seja a um elemento qualquer do grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$. Consideremos a função $D_a : L^2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow L^2(\mathbb{Z}/n\mathbb{Z})$ definida por $D_a f(x) = f(ax)$, então*

$$\mathscr{F}(D_a f)(x) = D_{a^{-1}}\mathscr{F} f(x).$$

Demonstração: Sejam $a \in (\mathbb{Z}/n\mathbb{Z})^*$ e $f, g \in L^2(\mathbb{Z}/n\mathbb{Z})$ quaisquer. Como a é um elemento inversível de $\mathbb{Z}/n\mathbb{Z}$, é certo que existe $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ tal que $a \cdot a^{-1} = 1$. Assim,

$$\begin{aligned}\mathscr{F} D_a f(x) &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} D_a f(y) e_x(-y) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(ay)\exp\left(\frac{-2\pi i x y}{n}\right)\\ &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(ay)\exp\left(\frac{-2\pi i a^{-1} x a y}{n}\right) = \sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(ay) e_{a^{-1}x}(-ay).\end{aligned}$$

Tomando $z \equiv ay \pmod{n}$ obtemos

$$\mathscr{F} D_a f(x) = \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z) e_{a^{-1}x}(-z) = \mathscr{F} f(a^{-1}x) = D_{a^{-1}}\mathscr{F} f(x).$$

■

2.3 Outras demonstrações para as propriedades da DFT em $\mathbb{Z}/n\mathbb{Z}$

Nesta secção apresentaremos outras demonstrações para o Lema 2.1 e para os itens (a), (c) e (d) do Teorema 2.1.

2.3.1 Segunda Demonstração para o Lema 2.1.

Sejam x e y elementos quaisquer de $\mathbb{Z}/n\mathbb{Z}$. Se $x \equiv y \pmod{n}$, então $\langle e_x, e_y\rangle = n$ e a demonstração é feita do mesmo modo que apresentamos na secção anterior.

Suponhamos que $x \not\equiv y \pmod{n}$

$$\begin{aligned}
\langle e_x, e_y\rangle &= \sum_{a=0}^{n-1} e_x(a)\overline{e_y(a)} = \sum_{a=0}^{n-1} e_x(a)e_y(-a), \text{ para } a \in \mathbb{Z}/n\mathbb{Z}, \\
&= \sum_{a=0}^{n-1} \exp(2\pi ixa/n)\exp(-2\pi iya/n) \\
&= \sum_{a=0}^{n-1} \exp(2\pi ixa/n)\exp(-2\pi iya/n) \\
&= \sum_{a=0}^{n-1} \exp\left(\frac{2\pi i(x-y)a}{n}\right) = \sum_{a=0}^{n-1} \exp\left(\frac{2\pi i(x-y)}{n}\right)^a.
\end{aligned}$$

Sabemos que $\displaystyle\sum_{a=0}^{n-1} \exp\left(\frac{2\pi i(x-y)}{n}\right)^a$ é a soma dos n termos de uma progressão geométrica com primeiro termo $\alpha_1 = 1$ e razão $q = \exp\left(\frac{2\pi i(x-y)}{n}\right) \neq 1$, já que, por hipótese, n não divide $x - y$. Dessa forma

$$\langle e_x, e_y\rangle = \alpha_1 \cdot \frac{1-q^n}{1-q} = \frac{1-q^n}{1-q}.$$

Por outro lado,

$$\begin{aligned}
q^n &= [\exp(2\pi i(x-y)/n)]^n = \exp(2\pi i(x-y)n/n) \\
&= e^{2\pi(x-y)i} = \cos[2\pi(x-y)] + i\,\mathrm{sen}[2\pi(x-y)] = 1.
\end{aligned}$$

Portanto,

$$\langle e_x, e_y\rangle = \frac{1-q^n}{1-q} = \frac{1-1}{1-q} = \frac{0}{1-q} = 0.$$

Em resumo,

$$\langle e_x, e_y\rangle = \left\{ \begin{array}{ll} n, & \text{se } x \equiv y \pmod{n} \\ 0, & \text{caso contrário} \end{array} \right\} = n\delta_x(y).$$

2.3.2 Segunda Demonstração para item (a) do Teorema 2.1

Faremos, aqui, outra demonstração para o fato de que $\mathscr{F}$ é bijetora. Para isso, iremos provar um resultado mais geral sobre a matriz de Vandermonde.

Definição 2.3 *Seja V uma matriz $m \times n$ cujos elementos pertencem a um corpo K. Dizemos que V é uma matriz de Vandermonde quando os termos de cada uma de suas linhas estão em progressão geométrica. Uma matriz de Vandermonde tem a seguinte forma geral:*

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^{n-1} \end{pmatrix}$$

onde $x_i \in K$.

Vimos, na equação (2.9), que a matriz da DFT pode ser representada por

$$F_n = \left(\omega^{-(j-1)(k-1)}\right)_{1\leq j,k\leq n} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \cdots & \omega^{-(n-1)^2} \end{pmatrix},$$

onde $\omega = \exp(2\pi i/n)$ é uma raiz e-ésima primitiva de $\mathbb{T}$. É fácil perceber que F_n é uma matriz $n \times n$ de Vandermonde, com $x_r \neq x_s$, para $r \neq s$.

Seja V_n o determinante da matriz $n \times n$ de Vandermonde V. Provaremos, por indução, que $V_n = \prod_{1\leq r<s\leq n} (x_s - x_r)$.

Para $n = 2$ temos que

$$F_2 = \det \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \end{pmatrix} = 1 \cdot x_2 - 1 \cdot x_1 = x_2 - x_1 = \prod_{1\leq r<s\leq 2} (x_s - x_r).$$

Suponhamos que a fórmula para o determinante seja válido para matrizes de Vandermonde $n-1 \times n-1$ (hipótese de indução). Assim

$$V_n = \det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_m & x_m^2 & \cdots & x_m^{n-1} \end{pmatrix}.$$

Agora, a partir da segunda coluna, iremos somar cada coluna com a da esquerda multiplicada por $-x_1$, logo

$$
\begin{aligned}
V_n &= \det \begin{pmatrix} 1 & x_1 - x_1 \cdot 1 & x_1^2 - x_1 x_1 & \cdots & x_1^{n-1} - x_1 x_1^{n-2} \\ 1 & x_2 - x_1 \cdot 1 & x_2^2 - x_1 x_2 & \cdots & x_2^{n-1} - x_1 x_2^{n-2} \\ 1 & x_3 - x_1 \cdot 1 & x_3^2 - x_1 x_3 & \cdots & x_3^{n-1} - x_1 x_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n - x_1 \cdot 1 & x_n^2 - x_1 x_n & \cdots & x_n^{n-1} - x_1 x_n^{n-2} \end{pmatrix} \\
&= \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{n-2}(x_2 - x_1) \\ 1 & x_3 - x_1 & x_3(x_3 - x_1) & \cdots & x_3^{n-2}(x_3 - x_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n - x_1 & x_n(x_n - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{pmatrix}.
\end{aligned}
$$

Aplicando o Teorema de Laplace [1] obtemos:

$$
\begin{aligned}
V_n &= (-1)^{1+1} \cdot 1 \cdot \det(M_{11}) + (-1)^{1+2} \cdot 0 \cdot \det(M_{12}) + \cdots + (-1)^{1+n} \cdot 0 \cdot \det(M_{1n}) \\
&= \det(M_{11}) = \det \begin{pmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{n-2}(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) & \cdots & x_3^{n-2}(x_3 - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_1 & x_n(x_n - x_1) & \cdots & x_n^{n-2}(x_n - x_1) \end{pmatrix} \\
&= \det(M_{11}) = (x_2 - x_1)(x_3 - x_1)(x_n - x_1) \det \begin{pmatrix} 1 & x_2 & \cdots & x_2^{n-2} \\ 1 & x_3 & \cdots & x_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-2} \end{pmatrix}.
\end{aligned}
$$

Aplicando a hipótese de indução temos que

$$
\begin{aligned}
V_n &= (x_2 - x_1)(x_3 - x_1) \cdots (x_n - x_1) \prod_{2 \le r < s \le n} (x_s - x_r) \\
&= \prod_{1 \le r < s \le n} (x_s - x_r).
\end{aligned}
$$

Após essa demonstração é imediato perceber que, para obtermos $V_n \neq 0$, é necessário ter $x_r \neq x_s$, para $r \neq s$. Dessa forma, podemos concluir que o determinante

[1] O Teorema de Laplace no diz que o determinante de uma matriz $A \in M_{n \times n}(K)$, onde K é um corpo, é dado por $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(M_{ij})$, em que $M_{i,j}$ representa a matriz que se obtém da matriz original pela eliminação da i-ésima linha e da j-ésima coluna.

da matriz da DFT não é nulo, ou seja, $\det(F_n) \neq 0$. Portanto, F_n é inversível e, consequentemente, a função $\mathscr{F}$ também é. Assim, $\mathscr{F}$ é bijetora.

2.3.3 Segunda Demonstração para item (c) do Teorema 2.1

Faremos uma demonstração calculando, diretamente, a dupla soma representada por $\mathscr{F}\mathscr{F}f$.

$$\begin{aligned}
\mathscr{F}\mathscr{F}f(-x) &= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \hat{f}(y)\exp\left(\frac{-2\pi i(-x)y}{n}\right) \\
&= \sum_{y\in\mathbb{Z}/n\mathbb{Z}} \left[\sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\exp\left(\frac{-2\pi iyz}{n}\right)\right]\exp\left(\frac{2\pi ixy}{n}\right) \\
&= \sum_{z\in\mathbb{Z}/n\mathbb{Z}}\sum_{y\in\mathbb{Z}/n\mathbb{Z}} f(z)\exp\left(\frac{-2\pi izy}{n}\right)\exp\left(\frac{2\pi ixy}{n}\right) \\
&= \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\sum_{y\in\mathbb{Z}/n\mathbb{Z}} e_z(y)e_x(-y) \\
&= \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\sum_{y\in\mathbb{Z}/n\mathbb{Z}} e_z(y)\overline{e_x(y)} \\
&= \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\langle e_z, e_x\rangle = \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\overline{\langle e_x, e_z\rangle}.
\end{aligned}$$

Pelo Lema 2.1 temos que $\langle e_x, e_z\rangle = n\delta_x(z)$, logo

$$\begin{aligned}
\mathscr{F}\mathscr{F}f(-x) &= \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\ \overline{n\delta_x(z)} \ = \sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\ n\delta_x(z) \\
&= n\sum_{z\in\mathbb{Z}/n\mathbb{Z}} f(z)\delta_x(z) \\
&= nf(x).
\end{aligned}$$

Portanto,

$$f(x) = \frac{1}{n}\mathscr{F}\mathscr{F}f(-x).$$

2.3.4 Segunda Demonstração para item (d) do Teorema 2.1

Consideremos o conjunto $\mathcal{U} = \{u_0,\ u_1,\ \cdots,\ u_{n-1}\}$, onde $u_a = n^{-1/2}e_a$, para $a \in \{0, 1, \cdots, n-1\}$. Provaremos que $\mathcal{U}$ é uma base ortonormal do espaço $L^2(\mathbb{Z}/n\mathbb{Z})$, ou seja, $\mathcal{U}$ é um conjunto de vetores ortonormais que gera $L^2(\mathbb{Z}/n\mathbb{Z})$. Para tanto, devemos lembrar que $\dim L^2(\mathbb{Z}/n\mathbb{Z}) = n$ e provar que $\langle u_a, u_b\rangle = 0$, para $a \not\equiv b \pmod n$, $\langle u_a, u_a\rangle = 1$, ou seja, $\mathcal{U}$ é um conjunto ortonormal.

Sejam u_a e u_b elementos quaisquer de $\mathcal{U}$. Assim

$$\langle u_a, u_b\rangle = \langle n^{-1/2}e_a, n^{-1/2}e_b\rangle = n^{-1/2}\cdot n^{-1/2}\langle e_a, e_b\rangle = n^{-1}\langle e_a, e_b\rangle.$$

Pelo Lema 2.1 temos que $\langle e_a, e_b\rangle = n\delta_a(b)$, logo

$$\langle u_a, u_b\rangle = n^{-1}\cdot n\cdot \delta_a(b) \Rightarrow \langle u_a, u_b\rangle = \delta_a(b),$$

onde podemos concluir que $\langle u_a, u_b\rangle = 0$, para $a \not\equiv b \pmod n$ e $\langle u_a, u_a\rangle = 1 = \|u_a\|$, logo, $\mathcal{U} = \{u_0,\ u_1,\ \cdots,\ u_{n-1}\}$ é um conjunto ortonormal de vetores em $L^2(\mathbb{Z}/n\mathbb{Z})$ co n elementos e, portanto, uma base para $L^2(\mathbb{Z}/n\mathbb{Z})$. Além disso, aplicando o Corolário C.1 obtemos

$$f(x) = \sum_{a=0}^{n-1}\frac{\langle f, u_a\rangle}{\|u_a\|^2}u_a(x) = \sum_{a=0}^{n-1}\frac{\langle f, u_a\rangle}{1^2}u_a(x) = \sum_{a=0}^{n-1}\langle f, u_a\rangle u_a(x). \tag{2.12}$$

Provaremos, agora, a fórmula de Parseval

$$\langle f,\ f\rangle = \frac{1}{n}\langle \hat{f},\ \hat{f}\rangle.$$

Sabemos que

$$\langle f,\ f\rangle = \sum_{a=0}^{n-1} f(a)\ \overline{f(a)} = \sum_{a=0}^{n-1}|f(a)|^2.$$

Por outro lado,

$$\begin{aligned}
\langle \hat{f},\ \hat{f}\rangle &= \sum_{a=0}^{n-1}|\hat{f}(a)|^2 \ = \ \sum_{a=0}^{n-1}|\langle f,\ e_a\rangle|^2 \\
&= \sum_{a=0}^{n-1}\left|\langle f, n^{1/2}\cdot u_a\rangle\right|^2 \ = \ \sum_{a=0}^{n-1}\left|\langle f,\ n^{1/2}u_a\rangle\right|^2 \\
&= \left(n^{1/2}\right)^2\sum_{a=0}^{n-1}|\langle f,\ u_a\rangle|^2 \ = \ n\sum_{a=0}^{n-1}|\langle f,\ u_a\rangle|^2,
\end{aligned}$$

ou seja,

$$\langle \hat{f},\ \hat{f}\rangle = n\sum_{a=0}^{n-1}|\langle f,\ u_a\rangle|^2 \Rightarrow \frac{1}{n}\langle \hat{f},\ \hat{f}\rangle = \sum_{a=0}^{n-1}|\langle f,\ u_a\rangle|^2 .$$

Para concluir a demonstração resta provar que

$$\sum_{a=0}^{n-1}|f(a)|^2 = \sum_{a=0}^{n-1}|\langle f,\ u_a\rangle|^2 . \tag{2.13}$$

De fato, aplicando o resultado obtido em (2.12) temos que

$$\begin{aligned}\sum_{a=0}^{n-1}|f(a)|^2 &= \langle f,f\rangle = \left\langle \sum_{a=0}^{n-1}\langle f,u_a\rangle u_a(x),\ \sum_{b=0}^{n-1}\langle f,u_b\rangle u_b(x)\right\rangle \\ &= \sum_{a=0}^{n-1}\langle f,u_a\rangle \left\langle u_a(x),\ \sum_{b=0}^{n-1}\langle f,u_b\rangle u_b(x)\right\rangle \\ &= \sum_{a=0}^{n-1}\langle f,u_a\rangle \sum_{b=0}^{n-1}\overline{\langle f,u_b\rangle}\,\langle u_a,\ u_b\rangle\end{aligned}$$

Como $\langle u_a,\ u_b\rangle = \delta_a(b)$ temos que

$$\sum_{b=0}^{n-1}\overline{\langle f,u_b\rangle}\,\langle u_a,\ u_b\rangle = \sum_{b=0}^{n-1}\overline{\langle f,u_b\rangle}\delta_a(b) = \overline{\langle f,u_a\rangle}.$$

Desse modo,

$$\begin{aligned}\sum_{a=0}^{n-1}|f(a)|^2 &= \sum_{a=0}^{n-1}\langle f,u_a\rangle \sum_{b=0}^{n-1}\overline{\langle f,u_b\rangle}\,\langle u_a,\ u_b\rangle \\ &= \sum_{a=0}^{n-1}\langle f,u_a\rangle\ \overline{\langle f,u_a\rangle} = \sum_{a=0}^{n-1}|\langle f,u_a\rangle|^2,\end{aligned}$$

e, portanto,

$$\langle f,\ f\rangle = \sum_{a=0}^{n-1}|f(a)|^2 = \sum_{a=0}^{n-1}|\langle f,u_a\rangle|^2 = \frac{1}{n}\langle \hat{f},\ \hat{f}\rangle.$$

2.4 Alguns Exemplos

Nesta secção mostraremos alguns exemplos com o cálculo e a representação gráfica da DFT de funções em $L^2(\mathbb{Z}/n\mathbb{Z})$ e listaremos todas as transformadas determinadas neste estudo.

Exemplo 2.3 *Vamos determinar a DFT da função constante $f(x) = 1$, para todo $x \in \mathbb{Z}/n\mathbb{Z}$.*

$$\begin{aligned}
\mathscr{F}f(x) &= \sum_{y\in\ \mathbb{Z}/n\mathbb{Z}} f(y)e_x(-y) \;=\; \sum_{y=0}^{n-1} 1\cdot\exp(-2\pi ixy/n) \\
&= \sum_{y=0}^{n-1} \exp(2\pi i0\cdot y/n)\cdot\exp(-2\pi ixy/n) \\
&= \sum_{y=0}^{n-1} e_0(y)\cdot e_x(-y) \\
&= \sum_{y=0}^{n-1} e_0(y)\cdot\overline{e_x(y)} \;=\; \langle e_0, e_x\rangle.
\end{aligned}$$

Pelo Lema 2.1, podemos concluir que $\langle e_x, e_0\rangle = n\delta_0(x)$, portanto

$$\mathscr{F}f(x) = \langle e_0, e_x\rangle = \overline{\langle e_x, e_0\rangle} = \overline{n\delta_0(x)} = n\delta_0(x).$$

A seguir, faremos a representação gráfica da função constante $f(x) = 1$ e sua DFT $\hat{f}(x) = n\delta_0(x)$.

Observação 2.7 *Pelo que foi visto no exemplo anterior, se definirmos a probabilidade uniforme por $P_U(x) = 1/n$, para todo $x \in \mathbb{Z}/n\mathbb{Z}$, então sua DFT é*

$$\mathscr{F}p_U(x) = \mathscr{F}(1/n) = \frac{1}{n}\mathscr{F}(1) = \frac{1}{n}\cdot n\delta_0 = \delta_0.$$

Aplicando a fórmula da inversão da DFT temos que

$$\mathscr{F}\delta_0 = \mathscr{F}\mathscr{F}p_U(x) = np_U(x),$$

ou seja, a DFT da função delta em zero é a probabilidade uniforme multiplicada por n.

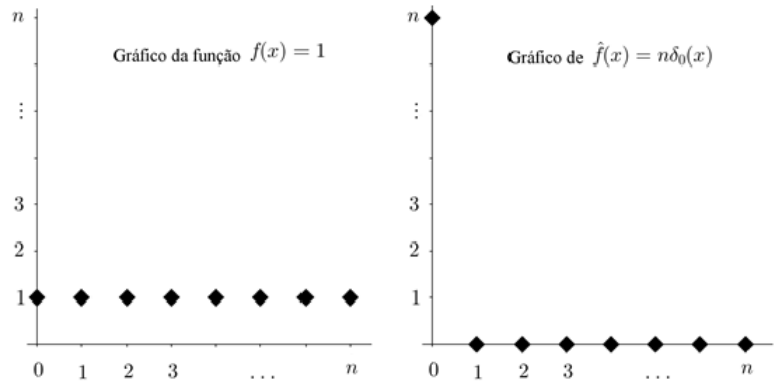

Figura 2.2: Uma função constante e sua DFT.

Exemplo 2.4 *Definiremos a função* $f(x) = \frac{1}{2}[\delta_1(x)+\delta_{-1}(x)]$ *em* $L^2(\mathbb{Z}/n\mathbb{Z})$. *Vamos mostrar que*

$$\hat{f}(x) = \cos\left(\frac{2\pi x}{n}\right).$$

Sabemos que $\mathscr{F}$ *é linear e já provamos que* $\mathscr{F}\delta_a(x) = \hat{\delta}_a(x) = e_a(-x)$. *Assim*

$$\begin{aligned}
\mathscr{F}f(x) &= \mathscr{F}\frac{1}{2}[\delta_1(x) + \delta_{-1}(x)] = \frac{1}{2}[\mathscr{F}\delta_1(x) + \mathscr{F}\delta_{-1}(x)] \\
&= \frac{1}{2}[e_1(-x) + e_{-1}(-x)] = \frac{1}{2}[\exp(-2\pi ix/n) + \exp(2\pi ix/n)] \\
&= \frac{1}{2}[\cos(-2\pi x/n) + i\,\mathrm{sen}(-2\pi x/n) + \cos(2\pi x/n) + i\,\mathrm{sen}(2\pi x/n)] \\
&= \frac{1}{2}[\cos(2\pi x/n) - i\,\mathrm{sen}(2\pi x/n) + \cos(2\pi x/n) + i\,\mathrm{sen}(2\pi x/n)] \\
&= \cos\left(\frac{2\pi x}{n}\right).
\end{aligned}$$

A Figura 2.3, a seguir, nos fornece uma representação geométrica das funções f *e* $\hat{f}$ *definidas neste exemplo, para* $n = 15$.

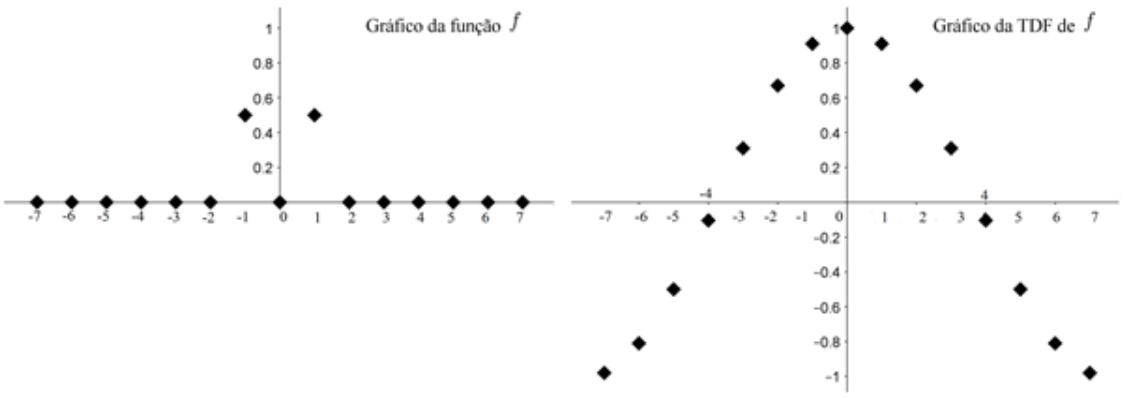

Figura 2.3: Gráficos das funções f e $\hat{f}$ dadas no Exemplo 2.4.

Exemplo 2.5 *Consideremos função* $f(x) = \frac{1}{3}[\delta_1(x) + \delta_0(x) + \delta_{-1}(x)]$ *pertencente ao espaço* $L^2(\mathbb{Z}/n\mathbb{Z})$. *Vamos determinar* $\hat{f}(x)$.

$$\begin{aligned}
\mathscr{F}f(x) &= \mathscr{F}\frac{1}{3}[\delta_1(x) + \delta_0(x) + \delta_{-1}(x)] = \frac{1}{3}[\mathscr{F}\delta_1(x) + \mathscr{F}\delta_0(x) + \mathscr{F}\delta_{-1}(x)] \\
&= \frac{1}{3}[e_1(-x) + e_0(-x) + e_{-1}(-x)] \;=\; \frac{1}{3}[\exp(-2\pi ix/n) + 1 + \exp(2\pi ix/n)] \\
&= \frac{1}{3}[\cos(-2\pi x/n) + i\,\mathrm{sen}(-2\pi x/n) + 1 + \cos(2\pi x/n) + i\,\mathrm{sen}(2\pi x/n)] \\
&= \frac{1}{3}[\cos(2\pi x/n) - i\,\mathrm{sen}(2\pi x/n) + 1 + \cos(2\pi x/n) + i\,\mathrm{sen}(2\pi x/n)] \\
&= \frac{1}{3}\left[1 + 2\cos\left(\frac{2\pi x}{n}\right)\right].
\end{aligned}$$

Veremos, abaixo, a representação gráfica de $f(x) = \frac{1}{3}[\delta_1(x) + \delta_0(x) + \delta_{-1}(x)]$ *e sua DFT para* $n = 15$.

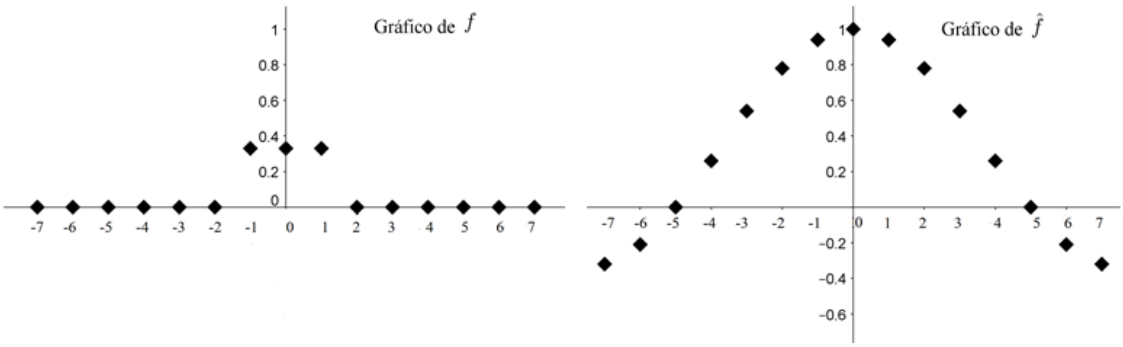

Figura 2.4: A DFT de $f(x) = \frac{1}{3}[\delta_1(x) + \delta_0(x) + \delta_{-1}(x)]$ para $n = 15$.

Exemplo 2.6 *Seja* $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}$ *a função definida por* $f(x) = \frac{1}{2}[\delta_0(x) + \delta_1(x)]$. *Vamos calcular* $\mathscr{F}f(x)$.

$$\begin{aligned}
\mathscr{F}f(x) &= \mathscr{F}\frac{1}{2}[\delta_0(x) + \delta_1(x)] = \frac{1}{2}[\mathscr{F}\delta_0(x) + \mathscr{F}\delta_1(x)] \\
&= \frac{1}{2}[e_0(-x) + e_1(-x)] = \frac{1}{2}[\exp(0) + \exp(-2\pi ix/n)] \\
&= \frac{1}{2}[1 + \cos(-2\pi x/n) + i\,\mathrm{sen}(-2\pi x/n)].
\end{aligned}$$

Aplicando as identidades $\cos(2a) = 2\cos^2(a) - 1$ *e* $\mathrm{sen}(2a) = 2\,\mathrm{sen}(a)\cos(a)$ *obtemos:*

$$\begin{aligned}
\mathscr{F}f(x) &= \frac{1}{2}[1 + 2\cos^2(-\pi x/n) - 1 - 2i\,\mathrm{sen}(-\pi x/n)\cos(-\pi x/n)] \\
&= \cos^2(-\pi x/n) - i\,\mathrm{sen}(-\pi x/n)\cos(-\pi x/n) \\
&= [\cos(-\pi x/n) + i\,\mathrm{sen}(-\pi x/n)]\cos(\pi x/n) \\
&= \exp\left(-\frac{\pi ix}{n}\right)\cos\left(\frac{\pi x}{n}\right).
\end{aligned}$$

Mostraremos, a seguir, uma tabela listando todas as transformadas de Fourier determinadas neste estudo.

$f(x)$	$\mathscr{F} f(y)$
1	$n\delta_0(y)$
$e_a(x)$	$n\delta_a(y)$
$\delta_a(x)$	$e_a(-y)$
$\frac{1}{2}(\delta_1 + \delta_{-1})(x)$	$\cos\left(\frac{2\pi y}{n}\right)$
$\frac{1}{3}(\delta_1 + \delta_0 + \delta_{-1})(x)$	$\frac{1}{3}\left[1 + 2\cos\left(\frac{2\pi y}{n}\right)\right]$
$\frac{1}{2}(\delta_0 + \delta_1)(x)$	$\exp\left(-\frac{\pi i y}{n}\right)\cos\left(\frac{\pi y}{n}\right)$

Tabela 2.1: Uma pequena tabela com transformadas discretas de Fourier.

Apêndice A

Conceitos Básicos da Aritmética

Faremos, nesse apêndice, um breve resumo sobre alguns temas tratados na Aritmática que são importantes para esse estudo. As demonstrações omitidas aqui podem ser consultadas nas referências bibliográficas [2], [3] e [4].

Definição A.1 *Dados dois números inteiros a e b, dizemos que a* divide *b quando existir um $k \in \mathbb{Z}$ tal que $b = ka$. Denotaremos por $a \mid b$ e podemos dizer também que a é um* divisor *de b ou, ainda, que b é um* múltiplo *de a ou que b é* divisível *por a.*

Na maioria dos casos, um número inteiro a não divide o número inteiro b. Nessas situações, às vezes, se faz necessário utilizar um fato que garante a possibilidade de efetuar a divisão de b por a com resto. Esse resultado, que enunciaremos abaixo, foi apresentado pela primeira vez na obra "Os Elementos", escrita por Euclides por volta de 300 a.C.. Esse teorema é o resultado central da Aritmética.

Teorema A.1 (Algoritmo da Divisão) *Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$b = aq + r, \ \text{com } 0 \leq r < |a|.$$

A seguir, apresentaremos o conceito de m.d.c. e provaremos um resultado interessante sobre ele.

Definição A.2 *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. O* Máximo Divisor Comum *de a e b, denotado por* m.d.c.(a, b)*, é um inteiro positivo d que satisfaz as seguintes condições:*

(a) $d \mid a$ e $d \mid b$;
(b) se $c \mid a$ e $c \mid b$ então $c \mid d$.

O seguinte teorema nos mostra que é sempre possível escrever o m.d.c. de dois números inteiros como combinação linear destes, com coeficientes inteiros.

Teorema A.2 *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Então existem $x, y \in \mathbb{Z}$ tais que*

$$ax + by = \text{m.d.c.}(a, b).$$

Demonstração: Sejam $a, b \in \mathbb{Z}$. Suponhamos, sem perda de generalidade, que $a \neq 0$ e consideremos o conjunto S de todas as combinações lineares positivas de a e b:

$$S = \{ax + by \mid ax + by > 0;\ x, y \in \mathbb{Z}\}.$$

Vamos provar, inicialmente, que S não é vazio. De fato, $0 < |a| = ax + b \cdot 0 \in S$, onde tomamos $x = 1$ ou $x = -1$ conforme a seja positivo ou negativo. Pelo Princípio da Boa Ordenação[1], S possui um elemento mínimo d. Provaremos, agora, que $d = \text{m.d.c.}(a, b)$, ou seja, d satisfaz as condições (a) e (b) da Definição A.2. De acordo com a definição de S, existem $x, y \in \mathbb{Z}$ tais que $ax + by = d$. Aplicando o Algoritmo da Divisão de Euclides podemos encontrar números inteiros q e r tais que $a = qd + r$, com $0 \leq r < d$. Logo, podemos escrever r na forma

$$\begin{aligned} r &= a - qd = a - q(ax + by) \\ &= a(1 - qx) + b(-qy) \\ &= aX + bY, \text{ onde } 1 - qx = X \in \mathbb{Z} \text{ e } -qy = Y \in \mathbb{Z}. \end{aligned}$$

Se $r > 0$, então r é um elemento de S, o que é uma contradição, pois d é o elemento mínimo de S e $r < d$, portanto, devemos ter $r = 0$. Deste modo,

$$a = qd + r \Rightarrow a = qd \Rightarrow d \mid a.$$

Analogamente podemos provar que $d \mid b$. Em resumo, $d \mid a$ e $d \mid b$. Agora, se c é um inteiro positivo onde $c \mid a$ e $c \mid b$, então, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = k_1 c$ e $b = k_2 c$, logo,

$$\begin{aligned} d &= ax + by = k_1 cx + k_2 cy = (k_1 x + k_2 y)c \\ &\Rightarrow d = kc, \text{ onde } k_1 x + k_2 y = k \in \mathbb{Z} \\ &\Rightarrow c \mid d, \end{aligned}$$

ou seja, se $c \mid a$ e $c \mid b$ então $c \mid d$. Como d satisfaz as condições da Definição A.2 podemos concluir que $d = \text{m.d.c.}(a, b)$. ∎

Como consequência imediata do Teorema A.2 temos que se $\text{m.d.c.}(a, b) = 1$, então existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$.

[1] O Princípio da Boa Ordenação (PBO) garante que todo subconjunto não vazio de elementos de $\mathbb{Z}_+$ tem um elemento mínimo.

Definição A.3 *Seja p um inteiro maior que* 1*. Dizemos que p é um número* primo *quando ele tiver apenas dois divisores.*

Por fim, enunciaremos o Teorema Fundamental da Aritmética, que nos garante a possibilidade de decompor em fatores primos, de modo único, qualquer número inteiro diferente de -1, 0, e 1.

Teorema A.3 (Teorema Fundamental da Aritmética) *Todo número natural maior que* 1 *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

De posse do Teorema A.3, é possível provar que, para qualquer inteiro m diferente de -1, 0, e 1, existem $p_1, p_2, \cdots, p_k$ primos e $n_1, n_2, \cdots, n_k \in \mathbb{N} \cup \{0\}$, univocamente determinados, de modo que

$$m = \pm\, p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

Apêndice B

Álgebra

B.1 Grupos

B.1.1 Definição e Exemplos

Definição B.1 *Sejam G um conjunto não vazio e $*$ uma operação definida em G. Dizemos que G é um* grupo *com relação à operação $*$ quando forem verificadas as seguintes propriedades:*

(a) $x * (y * z) = (x * y) * z$ para quaisquer $x, y, z \in G$ (associatividade);

(b) existe $e \in G$ tal que $x * e = e * x = x$ para todo $x \in G$ (existência de elemento neutro);

(c) para todo $x \in G$, existe $x^{-1} \in G$ tal que $x * x^{-1} = x^{-1} * x = e$ (existência de inverso).

Observação B.1 *Quando, além das três propriedades da Definição B.1, a operação $*$ for comutativa, ou seja, se $x * y = y * x$ para quaisquer $x, y \in G$, dizemos que G é um* grupo abeliano *(ou comutativo). Se a operação $*$ for uma* adição*, então diremos que G é um* grupo aditivo*. Se $*$ for uma* multiplicação*, diremos que G é um* grupo multiplicativo*.*

Exemplo B.1 *São exemplos de grupos aditivos: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ desde que $+$ represente a adição usual nos conjuntos numéricos. São exemplos de grupos multiplicativos: $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ e $(\mathbb{C} \setminus \{0\}, \cdot)$ desde que $\cdot$ represente a multiplicação usual nos conjuntos numéricos. Nesse trabalho estamos dando uma atenção especial aos seguintes grupos multiplicativos:*

- *grupo das classes de equivalência módulo p primo dado por $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$;*

- *o grupo dos números complexos de módulo* 1*, ou seja,* $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$*;*
- *o grupo* $\mathcal{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ *das raízes n-ésimas da unidade complexa.*

Os grupos listados neste exemplo são todos abelianos.

Definição B.2 *Seja* $(G, *)$ *um grupo finito com n elementos. A* ordem de G *é definida como sendo o número de elementos distintos de* G *e é denotada por* $|G|$ *ou por* $o(G)$*. Quando* G *for infinito, dizemos que a* ordem de G é infinita.

Exemplo B.2 *Consideremos* $A = \{1, -1\}$ *e a operação* $*$ *de multiplicação dada na seguinte tábua.*

$\cdot$	1	-1
1	1	-1
-1	-1	1

Neste caso, $(A, \cdot)$ *é um grupo abeliano de ordem 2, ou seja,* $|A| = 2$*.*

Definição B.3 *Seja* $(G, *)$ *um grupo. Um subconjunto não vazio* $S \subset G$ *que seja fechado com relação à operação* $*$ *é denominado um* subgrupo *de* G *quando* $(S, *)$ *também for um grupo.*

Observação B.2 *Todo grupo* G *admite pelo menos dois subgrupos triviais:* $S_1 = G$ *e* $S_2 = \{e\}$*, onde* e *é o elemento neutro de* G*.*

A seguinte proposição nos fornece uma ferramente muito útil quando estamos interessados em provar que certo subconjunto S é subgrupo de $(G, *)$. Sua demonstração pode ser consultada na reverência bibliográfica [5].

Proposição B.1 *Sejam* $(G, *)$ *um grupo e* S *um subconjunto de* G*. As seguintes condições são equivalentes:*

(a) S *é um subgrupo de* G*;*

(b) (i) $e \in S$*;*
(ii) $x * y \in S$*, para quaisquer* $x, y \in S$*;*
(iii) $x^{-1} \in S$*, para todo* $x \in S$*;*

(c) $S \neq \emptyset$ *e* $x * y^{-1} \in S$*, para quaisquer* $x, y \in S$*.*

Exemplo B.3 *Sejam* $G = (\mathbb{R} \setminus \{0\}, \cdot)$ *o grupo multiplicativo dos reais não nulos e* $S \subset G$ *o conjunto de todas as potências de expoente inteiro de 2:*

$$S = \{2^k \mid k \in \mathbb{Z}\} = \left\{\cdots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \cdots\right\}$$

Sejam x *e* y *dois elementos quaisquer de* S*. Assim,* x *e* y *são potências de* 2*, ou seja,* $x = 2^m$ *e* $y = 2^n$ *com* $m, n \in \mathbb{Z}$*. Desse modo,* $x \cdot y^{-1} = (2^m) \cdot (2^n)^{-1} = 2^m \cdot 2^{-n} = 2^{m-n}$*. Como* $m - n \in \mathbb{Z}$*, temos* $2^{m-n} \in S$*, portanto,* S *é subgrupo de* G*.*

B.1.2 Homomorfismo e Isomorfismo de Grupos

Definição B.4 *Dados dois grupos $(G, *)$ e $(J, \star)$ uma função $\psi : G \longrightarrow J$ é denominada um* homomorfismo *de G em J quando*

$$\psi(x * y) = \psi(x) \star \psi(y)$$

para quaisquer $x, y \in G$.

Exemplo B.4 *Sejam $G = (\mathbb{R}, +)$ e $J = (\mathbb{R}\backslash\{0\}, \cdot)$, respectivamente,o grupo aditivo e o grupo multiplicativo dos reais. Consideremos um número real positivo a. A função $\psi : G \longrightarrow J$ definida por $\psi(x) = a^x$ é um homomorfismo de G em J pois para quaisquer $x, y \in G$ temos*

$$\psi(x + y) = a^{x+y} = a^x \cdot a^y = \psi(x) \cdot \psi(y).$$

Definição B.5 *Sejam G e J grupos. Um* isomorfismo $\psi : G \longrightarrow J$ *é um homomorfismo de grupos que é também uma função bijetora. Quando existir um isomorfismo de grupos $\psi : G \longrightarrow J$, diremos que G é* isomorfo *a J e denotamos por $G \cong J$.*

Exemplo B.5 *Sejam $G = (\mathbb{R}^+, \cdot)$ o grupo multiplicativo dos reais positivos e $J = (\mathbb{R}, +)$. A função $\psi : G \longrightarrow J$ definida por $\psi(x) = \log(x)$ é um isomorfismo de grupos pois:*

(i) ψ é bijetora;

(ii) ψ é um homomorfismo já que

$$\psi(x \cdot y) = \log(x \cdot y) = \log(x) + \log(y) = \psi(x) + \psi(y).$$

Portanto $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +)$.

Observação B.3 *Se dois grupos G e J são isomorfos, então eles têm as mesmas propriedades algébricas. Por exemplo, se G for abeliano, então J também será abeliano, se G for finito e de ordem n, então J também será finito e de ordem n, se G é cíclico, então J também será cíclico, se determinada equação tem solução em G, então também terá solução em J, etc.*

B.1.3 Grupos Cíclicos e Teorema de Lagrange

Definição B.6 *Um grupo multiplicativo G é denominado* cíclico *quando existir um elemento $g \in G$ tal que todo elemento de G seja igual a alguma potência de g, ou seja, $G = \{g^n \mid n \in \mathbb{Z}\}$. Neste caso, o elemento g é denominado um* gerador *de G e escrevemos $G = [g]$ ou $G = \langle g \rangle$.*

Exemplo B.6 *O grupo* $S = \left\{\ldots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\right\}$ *dado no Exemplo B.3 é um grupo cíclico gerado por* 2*, ou seja,* $S = \langle 2\rangle$*. Notemos, neste caso, que* $\frac{1}{2}$ *também é gerador de* S*, ou seja,* $S = \langle \frac{1}{2}\rangle$*. Já foi visto, no Exemplo 1.10, que o grupo* $\mathcal{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ *é cíclico, gerado por* $\omega = \exp(2\pi i/n)$*.*

Exemplo B.7 *O grupo multiplicativo* $G = (\mathbb{Q}^+, \cdot)$ *não é cíclico porque não é possível encontramos um número racional positivo cujas potências gerem todos os elementos de* G*.*

Definição B.7 *Seja* g *pertencente a um grupo multiplicativo* G*, se existir um menor número inteiro positivo* n *tal que* $g^n = e =$ *elemento neutro de* G*, então* n *é denominado a* ordem *de* g*. Se não existir o menor inteiro positivo* n *tal que* $g^n = e$*, então dizemos que* g *tem* ordem zero*. A ordem de um elemento* g *é denotada por* $o(g)$*.*

Observação B.4 *A ordem de um elemento* g *pertencente a um grupo multiplicativo* G *também pode ser definida como sendo o número de elementos do grupo cíclico* $\langle g\rangle$*.*

Exemplo B.8 *Consideremos o grupo multiplicativo* $(\mathbb{Z}/7\mathbb{Z}) \setminus \{0\}$ *e seja* $\bar{2} \in \mathbb{Z}/7\mathbb{Z}$*. Assim,* $\bar{2}^1 = \bar{2}$*,* $\bar{2}^2 = \bar{4}$*,* $\bar{2}^3 = \bar{1}$*. Portanto,* $o(\bar{2}) = 3$*.*

Exemplo B.9 *No grupo multiplicativo das potências de* 2 *no exemplo B.6, observemos que* $2^1 = 2$*,* $2^2 = 4$*,* $2^3 = 8$*,* $2^4 = 16$*, ... e as potências não se repetem. Portanto, não existe um menor inteiro positivo* n *tal que* $2^n = 1$*, logo,* $o(2) = 0$*.*

Proposição B.2 *Seja* G *um grupo cíclico finito de ordem* n*. Então,* G *é isomorfo ao grupo aditivo* $\mathbb{Z}/n\mathbb{Z}$*.*

Demonstração: Suponhamos que G seja um grupo cíclico gerado por g, ou seja, $G = \{e, g^2, g^3, \cdots, g^{n-1}\}$. Consideremos a função $\psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ definida por $\psi(\bar{x}) = g^x$ e ilustrada abaixo.

$$\begin{array}{rccccccc} \mathbb{Z}/n\mathbb{Z} = & \{\bar{0}, & \bar{1}, & \bar{2}, & \cdots, & \overline{n-1}\} \\ \downarrow \psi & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ G = & \{e, & g, & g^2, & \cdots, & g^{n-1}\} \end{array}$$

Vamos provar que ψ é um isomorfismo de grupos. De fato, a função ψ é claramente sobrejetora. Por outro lado, para quaisquer $\bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$, temos que

$$\bar{x} = \bar{y} \Leftrightarrow x \equiv y \pmod{n} \Leftrightarrow x - y = nk, k \in \mathbb{Z} \Leftrightarrow g^{x-y} = g^{nk} = (g^n)^k = e \Leftrightarrow g^x = g^y,$$

logo, ψ também é injetora. Além disso,

$$\psi(\bar{x} + \bar{y}) = \psi(\overline{x+y}) = g^{x+y} = g^x \cdot g^y = \psi(\bar{x}) \cdot \psi(\bar{y})$$

e portanto, fica mostrado que ψ é um homomorfismo bijetor de G em $\mathbb{Z}/n\mathbb{Z}$, ou seja, $G \cong \mathbb{Z}/n\mathbb{Z}$. ∎

Definição B.8 *Sejam H um subgrupo de um grupo $(G, *)$ e $x \in G$ um elemento qualquer. A* classe lateral à esquerda, módulo H, definida por x, *denotada por $x*H$, é definida como sendo o seguinte subconjunto de G:*

$$x * H = \{x * h \mid h \in H\}.$$

Analogamente, a classe lateral à direita, módulo H, definida por x, *denotada por $H * x$, é definida como sendo o seguinte subconjunto de G:*

$$H * x = \{h * x \mid h \in H\}.$$

Observação B.5 *Quando G for um grupo abeliano os conceitos de classes laterais à esquerda e à direita coincidem, ou seja, $x * H = H * x$.*

Na Proposição B.3 a seguir, consideremos G um grupo multiplicativo e H um dos seus subgrupos. Por simplicidade, ao tratarmos de grupos multiplicativos, denotaremos suas classes laterais por xH ou Hx. Omitiremos a demonstração dessa proposição e sugerimos a consulta da referência bibliográfica [5].

Proposição B.3 *$x, y \in G$, $x \equiv y \pmod{H} \Leftrightarrow xy^{-1} \in H$ define uma relação de equivalência no grupo G.*

Nas condições da Proposição B.3, consideremos uma classe de equivalência $\overline{x} = \{y \in G \mid x \equiv y \ (\mod H)\}$. Desse modo

$$y \in \overline{x} \Leftrightarrow x \equiv y \ (\mod H) \Leftrightarrow yx^{-1} \in H \Leftrightarrow yx^{-1} = h,$$

para algum $h \in H$, ou seja, $y = hx$. Assim é fácil ver que $Hx = \{hx \mid h \in H\} = \overline{x}$ (um argumento análogo nos leva à uma conclusão semelhante para classes laterais à esquerda). Com isso, o conjunto quociente G/H, formado por todas as classes de equivalência $\overline{x}$ módulo H em G, é dado por $G/H = \{Hx \mid x \in G\}$.

Vamos supor, agora, que G/H tem, exatamente, n classes laterais distintas, ou seja, $G/H = \{Hx_1, Hx_2, \cdots, Hx_n\}$, onde $x_1, x_2, \cdots, x_n \in G$. Como G/H é uma partição de G, temos que $Hx_i \cap Hx_j = \emptyset$ se $i \neq j$. Além disso,

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n \text{ (união disjunta).}$$

Definição B.9 *Sendo G um grupo finito e H um subgrupo de G, o* índice de H em G *é o número de classes laterais distintas módulo H em G e é denotado por $(G : H)$.*

Teorema B.1 (Teorema de Lagrange) *Se G for um grupo finito e H for um subgrupo de G, então a ordem de H divide a ordem de G e $|G| = |H|(G : H)$.*

Demonstração: Vamos mostra, inicialmente, que toda classe lateral Hx tem a mesma quantidade de elementos que H. De fato, Seja $\psi : H \longrightarrow Hx$ definida por $\psi(h) = hx$. Temos que:

- Se $\psi(h_1) = \psi(h_2)$, então $h_1x = h_2 \cdot x \Rightarrow h_1xx^{-1} = h_2xx^{-1} \Rightarrow h_1 = h_2$. Logo, ψ é injetora.
- Se $y \in Hx$, então existe $h_1 \in H$ tal que $y = h_1x$ e daí $\psi(h_1) = h_1x = y$. Logo, ψ é sobrejetora.

Como ψ é uma bijeção de H em Hx, podemos concluir que $|H| = |Hx|$.

Daremos prosseguimento a nossa demonstração lembrando que

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n,$$

onde classes laterais distintas não têm elemento em comum. Assim

(i) $(G : H) = n$;

(ii) $|Hx_i| = |H|$ para todo $i \in \{1, 2, \cdots, n\}$;

(iii) $|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_n| = \overbrace{|H| + \cdots + |H|}^{n \text{ parcelas}} = n|H|$.

Dos itens (i) e (ii) concluímos que $|G| = |H|(G : H)$. ∎

Corolário B.1 *Se G é um grupo finito e $x \in G$, então $o(x)$ é um divisor de $|G|$.*

Demonstração: Basta lembrar que $|\langle x\rangle| = o(x)$ assim, pelo Teorema de Lagrange, $|\langle x\rangle|$ divide $|G|$. ∎

Corolário B.2 *Se G é um grupo finito, com elemento neutro e, e $x \in G$, então $x^{|G|} = e$.*

Demonstração: Seja $H = \langle x\rangle$. Então $|H| = o(x)$ e, como $|G| = |H|(G : H)$, temos $|G| = o(x)(G : H) \Rightarrow x^{|G|} = x^{o(x)(G:H)} = (x^{o(x)})^{(G:H)} = e^{(G:H)} = e$. ∎

Corolário B.3 *Todo grupo finito G de ordem prima é cíclico e seus únicos subgrupos são $\{e\}$ e G.*

Demonstração: Suponhamos $|G| = p$ primo e H um subgrupo de G. Como $|H|$ é um divisor de $|G|$, temos $|H| = 1$ ou $|H| = p$. Se $|H| = 1$, então $H = \{e\}$. Caso tenhamos $|H| = p$, então $H = G$. Logo, os únicos subgrupos de G são os subgrupos triviais $\{e\}$ e G.

Se $G = \{e\} = [e]$ então G é cíclico e é gerado por e; se G contiver algum elemento $x \neq e$, então $H = \langle x\rangle \Rightarrow H \neq \{e\} \Rightarrow H = G$, ou seja $G = \langle x\rangle$ é gerado por x. Em qualquer caso, G é cíclico. ∎

B.1.4 Grupos-Quocientes

Sendo G um grupo, um subgrupo N de G é denominado *normal* quando $xN = Nx$ para todo $x \in G$. Neste caso, N *subgrupo normal de* G é denotado por $N \lhd G$.

Exemplo B.10 *É claro que se G for abeliano, então todo subgrupo de G é normal porque as classes laterais à esquerda e à direita coincidem. Por exemplo, se $G = (\mathbb{R}, +)$ e $H = (\mathbb{Z}, +)$, então $H \lhd G$.*

Sejam N um subgrupo normal de um grupo G e xN e yN duas classes laterais módulo N quaisquer. Podemos definir uma operação de multiplicação $\cdot$ sobre o conjunto de todas as classes laterais módulo N do seguinte modo:

$$(xN) \cdot (yN) = (x \cdot y)N. \tag{B.1}$$

Definição B.10 *Consideremos $N \lhd G$. O conjunto de todas as classes laterais módulo N com a operação definida em (B.1) é denominado* grupo quociente *de G por N e é denotado por G/N:*

$$G/N = \{xN \mid \ x \in G\}.$$

É fácil provar que $(G/N, \cdot)$ tem, realmente, todas as propriedades de grupo. Além disso, quando G for um grupo finito, o Teorema de Lagrange nos garante que

$$|G/N| = (G : N) = \frac{|G|}{|N|}.$$

Antes de encerrar essa secção iremos enunciar um resultado utilizado nesse trabalho.

Proposição B.4 *Se G é um grupo cíclico de ordem n e $d \mid n$, então existe um único subgrupo S de G (que também é cíclico) de ordem d.*

Particularmente, se n é igual a 2, então G tem apenas um elemento de ordem 2.

B.2 Anéis

B.2.1 Definição e Exemplos

Definição B.11 *Consideremos um conjunto $A \neq \emptyset$ no qual estão definidas duas operações: uma adição $(+)$ e uma multiplicação $(\cdot)$. Dizemos que $(A, +, \cdot)$* é um anel *(ou simplesmente que A* é um anel*) quando forem verificadas as seguintes propriedades:*

(a) $\forall x, y, z \in A$, $x + (y + z) = (x + y) + z$ *(associatividade da adição);*

(b) $\forall x, y \in A$, $x + y = y + x$ *(comutatividade da adição);*

(c) *Existe* $0 \in A$ *tal que* $x + 0 = x$, $\forall x \in A$ *(elemento neutro da adição);*

(d) *Para todo* $x \in A$, *existe* $(-x) \in A$ *tal que* $x + (-x) = 0$ *(inverso aditivo);*

(e) $\forall x, y, z$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(associatividade da multiplicação);*

(f) $\forall x, y, z \in A$, $x \cdot (y + z) = x \cdot y + x \cdot z$ *e* $(x + y) \cdot z = x \cdot z + y \cdot z$ *(distributividade da adição com relação à multiplicação).*

Exemplo B.11 *Os conjuntos numéricos* $\mathbb{Z}$ $\mathbb{Q}$, $\mathbb{R}$ *e* $\mathbb{C}$ *são anéis com relação às operações de adição e multiplicação usuais.*

Definição B.12 *Seja* $(A, +, \cdot)$ *um anel e* $S \neq \emptyset$ *um subconjunto de* A. *Dizemos que* S *é um* subanel *de* A *quando* $(S, +, \cdot)$ *também for um anel com as operações de* A *restritas ao conjunto* S.

Exemplo B.12 *O conjunto dos múltiplos de* 5, $5\mathbb{Z}$, *é um subanel de* $\mathbb{Z}$ *com as operações de adição e multiplicação de inteiros usuais. Em geral,* $(n\mathbb{Z}, +, \cdot)$ *é um subanel de* $(\mathbb{Z}, +, \cdot)$ *para qualquer inteiro positivo* n.

A proposição a seguir fornece um critério bastante útil para se determinar se um conjunto é subanel de um anel.

Proposição B.5 *Sejam* $(A, +, \cdot)$ *e* S *um subconjunto de* A. *Então,* S *é um subanel de* A *se, e somente se,* $0 \in S$ *e* $x - y \in S$ *e* $x \cdot y \in S$ *para quaisquer* $x, y \in S$, *ou seja,* S *for fechado com relação à subtração e à multiplicação de* A.

Definição B.13 *Um anel* $(A, +, \cdot)$ *é denominado* comutativo *se a sua multiplicação for comutativa, ou seja, se* $x \cdot y = y \cdot x$, $\forall x, y \in A$.

Definição B.14 *Um* anel com unidade *é um anel* A *cuja multiplicação possui elemento neutro, denotado por* 1_A *ou simplesmente por* 1, *e denominado a* unidade *do anel.*

Exemplo B.13 *O anéis* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *e* $\mathbb{C}$, *com as operações usuais de adição e multiplicação, são exemplos de anéis comutativos com unidade.*

Definição B.15 *Dizemos que* $x \neq 0$ *e* $y \neq 0$ *em um anel* A *são* divisores próprios de zero *quando* $x \cdot y = 0$.

Definição B.16 *Um anel comutativo com unidade A é denominado* anel de integridade *quando*

$$\forall x, y \in A,\ x \cdot y = 0 \Rightarrow x = 0 \text{ ou } y = 0.$$

Pelo que vimos nas definições B.16 e B.15, um anel de integridade é um anel comutativo com unidade que não possui divisores próprios do zero.

Exemplo B.14 *No anel dos inteiros $\mathbb{Z}$, se $x, y \in \mathbb{Z}$ são tais que $x \cdot y = 0$, então temos que $x = 0$ ou $y = 0$. Logo, $\mathbb{Z}$ é um anel de integridade. Também são anéis de integridade: $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.*

Exemplo B.15 *Consideremos o anel $\mathbb{Z}/10\mathbb{Z}$. Os elementos $\bar{5}$ e $\bar{6}$ são diferentes de $\bar{0}$, mas $\bar{5} \cdot \bar{6} = \bar{30} = \bar{0}$. Logo, $\bar{5}$ e $\bar{6}$ são divisores próprios do zero em $\mathbb{Z}/10\mathbb{Z}$ e, consequentemente, $\mathbb{Z}/10\mathbb{Z}$ não é anel de integridade.*

Definição B.17 *Um anel comutativo com unidade K é denominado um* corpo *se todo elemento não nulo de K possuir inverso multiplicativo, ou seja, $\forall x \in K$, $x \neq 0 \Rightarrow \exists x^{-1} \in K$ tal que $x \cdot x^{-1} = 1$.*

Exemplo B.16 *Os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos. No entanto, $\mathbb{Z}$ não é um corpo, porque nem todo número inteiro possui inverso multiplicativo. No Teorema 1.1 vimos que $\mathbb{Z}/p\mathbb{Z}$ é uma corpo para qualquer primo p.*

B.2.2 Homomorfismo e Isomorfismo de Anéis

Definição B.18 *Uma função $\psi : A \longrightarrow B$ de um anel A em um anel B é denominada* homomorfismo de anéis *quando forem verificadas as seguintes propriedades, para quaisquer $x, y \in A$:*

(a) $\psi(x + y) = \psi(x) + \psi(y)$ (ψ preserva soma);

(b) $\psi(x \cdot y) = \psi(x) \cdot \psi(y)$ (ψ preserva produto).

Um isomorfismo *de um anel A em um anel B é uma função $\psi : A \longrightarrow B$ que é um homomorfismo bijetor. Nesse caso, dizemos que A e B são anéis* isomorfos *e denotamos por $A \cong B$.*

Exemplo B.17 *Seja $A = (\mathbb{Q} \oplus \mathbb{R}, +, \cdot)$ e $B = (\mathbb{R} \oplus \mathbb{Q}, +, \cdot)$, onde $+$ e $\cdot$ são as operações dadas na* Definição 1.2. *Mostraremos que a função $\psi : A \longrightarrow B$ definida por $(x, y) = (y, x)$ é um isomorfismo de anéis.*

Sejam $\alpha = (x, y)$ e $\beta = (z, w)$ dois elementos quaisquer de A. Dessa forma temos que:

$$\begin{aligned}(a)\ \psi(\alpha+\beta) &= \psi((x,y)+(z,w)) = \psi(x+z, y+w) = (y+w, x+z)\\ &= (y,x)+(w,z) = \psi(x,y)+\psi(z,w)\\ &= \psi(\alpha)+\psi(\beta) \qquad (\psi \text{ preserva soma});\end{aligned}$$

$$\begin{aligned}(b)\ \psi(\alpha\cdot\beta) &= \psi((x,y)\cdot(z,w)) = \psi(x\cdot z, y\cdot w) = (y\cdot w, x\cdot z)\\ &= (y,x)\cdot(w,z) = \psi(x,y)\cdot\psi(z,w)\\ &= \psi(\alpha)\cdot\psi(\beta) \qquad (\psi \text{ preserva produto}).\end{aligned}$$

Logo, ψ é um homomorfismo de anéis. Resta provar que ψ é uma bijeção. Como

$$\psi(\alpha) = \psi(\beta) \Rightarrow \psi(x,y) = \psi(z,w) \Rightarrow (y,x) = (w,z) \Rightarrow x = z \text{ e } y = w \Rightarrow \alpha = \beta,$$

temos que ψ é injetora. Além disso, para todo par $b = (r, s) \in B$ existe um par $a = (s, r) \in A$ tal que $\psi(a) = b$, logo, ψ também é sobrejetora e, portanto, bijetora. Assim ψ é um isomorfismo de anéis.

Observação B.6 *De modo análogo ao isomorfismo de grupos, se dois anéis A e B são isomorfos então eles têm as mesmas propriedades algébricas.*

B.2.3 Ideais e Anéis-Quocientes

Definição B.19 *Sejam A um anel comutativo e I um subconjunto não vazio de A. Dizemos que I é um* ideal *em A quando ele tem as seguintes propriedades:*

(a) $x - y \in I$, $\forall x, y \in I$;

(b) $a \cdot x \in I$, $\forall x \in I$ e $\forall a \in A$

Exemplo B.18 *Sejam $A = \mathbb{Z}$ e $I = 7\mathbb{Z}$ = conjunto dos inteiros múltiplos de 7. Sabemos que $I = 7\mathbb{Z}$ não é vazio. Além disso:*

(a) se $x, y \in I$, então $x = 7m$ e $y = 7n$ com $m, n \in \mathbb{Z}$. Daí, temos que $x - y = 7m - 7n = 7(m - n) \in I$;

(b) se $a \in A$, então $a \cdot x = a \cdot (7m) = 7(a \cdot m) \in I$.

Dessa forma, podemos concluir que $7\mathbb{Z}$ é um ideal em $\mathbb{Z}$. De modo geral, temos que $n\mathbb{Z}$ é um ideal em $\mathbb{Z}$ para todo inteiro n.

Observação B.7 *Todo anel A possui pelo menos dois ideais: o próprio anel A e o conjunto unitário $\{0_A\}$ formado pelo elemento neutro da adição. Tais ideais são chamados de* ideais triviais.

Seja I um ideal em um anel comutativo A no qual consideramos a seguinte relação $\sim$:

$$x \sim y \Leftrightarrow x - y \in I, \quad \forall x, y \in A.$$

É fácil verificar que essa é uma relação de equivalência em A. As classes de equivalência, neste caso, são os conjuntos $\bar{x} = \{x+i \mid i \in I\} = x+I$ e o conjunto-quociente de A por $\sim$ é o conjunto $A/\sim \ = \ \{\bar{x} \mid x \in A\}$ que é formado por todas as classes de equivalência da relação $\sim$. Neste caso, denotaremos $A/\sim$ também por A/I.

Definição B.20 *Seja I um ideal em um anel comutativo A. O* anel quociente *de A por I é o conjunto*

$$A/I = \{x + I \mid x \in A\}$$

com as operações de adição e multiplicação definidas a seguir:

Adição: $(x + I) + (y + I) = (x + y) + I$, $\forall x, y \in A$

Multiplicação: $(x + I) \cdot (y + I) = (x \cdot y) + I$, $\forall x, y \in A$

É possível provar que $(A/I, +, \cdot)$ tem todas as propriedades de anel dadas na Definição B.11, mas esse não é o objetivo do nosso estudo.

B.2.4 Polinômios

Definição B.21 *Seja A um anel comutativo qualquer. Definimos o anel comutativo $A[x]$ como sendo o conjunto de todas as expressões da*

$$f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n,$$

com $a_j \in A$. Tais expressões são chamadas de polinômios *com coeficientes em A.*

Definição B.22 *Sejam $f(x) = \sum_j a_jx^j$ e $g(x) = \sum_j b_jx^j$ dois polinômios quaisquer definidos sobre um anel comutativo A. A soma e o produto no anel de polinômios $A[x]$ são dados por*

$$f(x) + g(x) \ = \ \sum_j (a_j + b_j)x^j;$$

$$f(x) \cdot g(x) \ = \ \sum_h c_hx^h, \ \textit{onde } c_h = \sum_{j+k=h} a_jb_k.$$

É possível verificar que $A[x]$ com as operações $+$ e $\cdot$ definidas acima tem a estrutura de anel. Nessas condições, dizemos que $A[x]$ é um anel de polinômios.

Definição B.23 *Seja A um anel e $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \in A[x]$ um polinômio não nulo. O* grau de f *é o maior índice dos termos não nulos de f, ou seja, é o maior j tal que $a_j \neq 0$. Neste caso, o termo a_j é denominado* coeficiente dominante de f. *Não definimos grau para o polinômio nulo. Representamos o grau de um polinômio f por ∂f ou por* $\deg(f)$.

Definição B.24 *Sendo A um anel comutativo com unidade, dados dois polinômios f e g em $A[x]$, dizemos que f* divide *g quando existir $h \in A[x]$ tal que $g = f \cdot h$.*

Exemplo B.19 *Sejam $f = 1+x$ e $g = -2-x+x^2 = (1+x)\cdot(-2+x)$. Considerando $h = -2 + x$, temos que $g = f \cdot h$ e daí concluímos que $f \mid g$.*

Enunciaremos, a seguir, uma teorema que trata do algorítimo da divisão para polinômios. Sua demonstração pode ser consultada na referência bibliográfica [5].

Teorema B.2 *Seja A um anel comutativo com unidade. Consideremos dois polinômios $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ e $g(x) = b_0+b_1x+b_2x^2+\cdots+b_mx^m$ de $A[x]$ tais que g não é o polinômio nulo e seu coeficiente dominante é invertível. Então, existem únicos polinômios $q, r \in A[x]$ tais que $f = g \cdot q + r$ e $r = 0$ ou $\partial r < \partial g$.*

No Teorema B.2, os polinômios $q(x)$ e $r(x)$ são denominados quociente e resto da divisão de $f(x)$ por $g(x)$, respectivamente.

Definição B.25 *Sejam A um anel comutativo com unidade. Consideremos o polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ e $a \in A$. O valor de f em r, denotado por $f(r)$, é o elemento de A dado por $f(r) = a_0 + a_1 \cdot r + a_2 \cdot r^2 + \cdots + a_n \cdot r^n$. Quando $f(r) = 0$, diremos que r é uma* raiz *do polinômio $f(x)$.*

Exemplo B.20 *Sejam $f(x) = -2 + x^2 + x^4 \in \mathbb{Z}[x]$, $r = -1$ e $s = 2$. Temos: $f(r) = f(-1) = -2+(-1)^2+(-1)^4 = 0$ e $f(s) = f(2) = -2+2^2+2^4 = 18$. Assim, r é uma raiz do polinômio $f(x)$, porém s não é raiz.*

Proposição B.6 *Se A for um anel de integridade e f for um polinômio não nulo de $A[x]$ com m raízes, então $m \leq \partial f$.*

Demonstração: Se $\partial f = 0$, então f é um polinômio constante e não tem raiz. Neste caso, $m = 0$ e $m \leq \partial f$. Suponhamos $\partial f = n > 0$ e que (por hipótese de indução) a proposição seja verdadeira para todo polinômio de grau $n - 1$. Se f não possui raiz, $m = 0$, então, neste caso, a proposição é verdadeira (porque $m < n$). Caso contrário, seja r uma raiz de f. Como f é divisível por $(x - r)$, temos que existe $q \in A[x]$ tal que $f = (x-r)\cdot q$. Daí, qualquer outra raiz de f (se existir), será também raiz de q. Como $\partial q = n - 1$, temos por hipótese que o número de raízes de q não ultrapassa $n - 1$. Juntando-se as raízes de q com r, obtemos as raízes de f. Logo, o número de raízes de f não ultrapassa $(n - 1) + 1 = n$ e daí, por indução, a proposição fica demonstrada. ∎

Apêndice C

Álgebra Linear

Nesse apêndice, apresentaremos algumas definições e resultados, da Álgebra Linear, essenciais para nosso estudo. Algumas demonstrações não serão feitas aqui e poderão ser consultadas na referência bibliográfica [6].

C.1 Espaços Vetoriais

Definição C.1 *Um* espaço vetorial V *consiste no seguinte:*

1. Um corpo K de escalares.
2. Um conjunto não vazio V de objetos chamados vetores.
3. Uma operação de adição de vetores que associa a cada par de vetores $u, v \in V$ um vetor $u + v \in V$, chamado soma de u e v, de tal forma que
(a) a adição é comutativa, ou seja, $u + v = v + u$, para quaisquer $u, v \in V$;
(b) a adição é associativa, ou seja, $u + (v + w) = (u + v) + w$, para quaisquer $u, v, w \in V$;
(c) existe um único vetor 0, chamado vetor nulo, tal que $v + 0 = v$, para todo $v \in V$;
(d) para cada vetor $v \in V$ existe um único vetor $-v \in V$ tal que $v + (-v) = 0$.

4. Uma operação de multiplicação por escalar que associa cada par com escalar $\lambda \in K$ e vetor $v \in V$ a um vetor $\lambda v \in V$, chamado produto de λ e v, de tal forma que
(a) $1v = v$, para todo $v \in V$;
(b) $(\lambda_1 \lambda_2)v = \lambda_1(\lambda_2 v)$, para quaisquer $\lambda_1, \lambda_2 \in K$ e $v \in V$;
(c) $\lambda(u + v) = \lambda u + \lambda v$, para quaisquer $\lambda \in K$ e $u, v \in V$;
(d) $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$, para quaisquer $\lambda_1, \lambda_2 \in K$ e $v \in V$.

Nas condições acima, dizemos que V é um espaço vetorial sobre o corpo K

ou, simplesmente, V é um espaço vetorial. Em seguida, veremos dois exemplos de espaços vetoriais.

Exemplo C.1 *Sejam K um corpo e K^n o conjunto formado por todas as n-uplas $v = (x_1, x_2, \cdots, x_n)$, com $x_i \in K$. Se $u = (y_1, y_2, \cdots, y_n) \in K^n$ podemos definir soma de vetores e produto por escalar em K^n da seguinte forma:*

$$v + u = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$$

$$\lambda v = (\lambda x_1, \lambda x_2, \cdots, \lambda x_n).$$

As operações de soma de vetores e multiplicação por escalar aqui definidas tem as propriedades dos itens 3 e 4 da Definição C.1, logo, K^n é um espaço vetorial. Em particular, como $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos, podemos concluir que $\mathbb{Q}^n$, $\mathbb{R}^n$ e $\mathbb{C}^n$ são espaços vetoriais com as operações dadas acima.

Exemplo C.2 *Sejam K um corpo e $m, n \in \mathbb{N}$. Consideremos o conjunto $K^{m\times n}$ formado por todas as matrizes $m \times n$ sobre o corpo K. Podemos definir soma de vetores e produto por escalar em $K^{m\times n}$ da seguinte forma:*

$$(A + B)_{ij} = A_{ij} + B_{ij}$$

$$(\lambda A)_{ij} = \lambda A_{ij}.$$

*O conjunto $K^{m\times n}$ junto com as operações definidas neste exemplo têm as propriedades dos itens 3 e 4 da Definição C.1, logo, $K^{m\times n}$ é um espaço vetorial e recebe o nome de **espaço das matrizes** $m \times n$.*

Definição C.2 *Seja V um espaço vetorial sobre um corpo K. Um* subespaço *de V é é um subconjunto W de V que também é um espaço vetorial sobre o corpo K com as operações de adição e multiplicação por escalar de V.*

Proposição C.1 *Um subconjunto não vazio W de V é um subespaço de V se, e somente se, para cada para de vetores u, v em W e escalar $\lambda \in K$, o vetor $\lambda u + v$ está em W.*

Exemplo C.3 *Consideremos o espaço vetorial K^n das n-uplas sobre um corpo K. Seja W um subconjunto de K^n formado por todas as n-uplas $(x_1,\ x_2,\ \cdots,\ x_n)$ com $x_n = 0$. Sendo $u = (x_1,\ x_2,\ \cdots,\ 0)$ e $v = (y_1,\ y_2,\ \cdots,\ 0)$ vetores quaisquer em W, temos que*

$$\begin{aligned} \lambda u + v &= \lambda(x_1,\ x_2,\ \cdots,\ 0) + (y_1,\ y_2,\ \cdots,\ 0) \\ &= (\lambda x_1,\ \lambda x_2,\ \cdots,\ 0) + (y_1,\ y_2,\ \cdots,\ 0) \\ &= (\lambda x_1 + y_1,\ \lambda x_2 + y_2,\ \cdots,\ 0) \in W. \end{aligned}$$

Pela Proposição C.1 podemos concluir que W é subespaço de K^n.

Definição C.3 *Seja V um espaço vetorial sobre o corpo K e consideremos os vetores u, v_1, v_2, $\cdots$, v_n em V. Dizemos que u é* combinação linear *de v_1, v_2, $\cdots$, v_n se existirem escalares λ_1, λ_2, $\cdots$, λ_n em K tais que*

$$\begin{aligned} u &= \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \\ &= \sum_{i=1}^{n} \lambda_i v_i. \end{aligned}$$

Definição C.4 *Seja S um subconjunto de vetores num espaço vetorial V. O* subespaço gerado por S *é definido como sendo a intersecção W de todos os subespaços de V que contêm S. Quando S é um conjunto finito $S = \{v_1,\ v_2,\ \cdots,\ v_n\}$, denominaremos W simplesmente o subespaço gerado pelos vetores v_1, v_2, $\cdots$, v_n.*

Proposição C.2 *O subespaço gerado por um subconjunto não vazio S de um espaço vetorial V é o conjunto de todas as combinações lineares de vetores de S.*

Exemplo C.4 *Seja V os espaço das funções polinomiais sobre um corpo K. Seja S o subconjunto de V formado pelas funções f_1, f_2, $\cdots$, f_n definidas por*

$$f_n(x) = x^n,\ n \in \{0, 1, 2, \cdots\}.$$

Pela Proposição C.2, V é o subespaço gerado pelo conjunto S.

C.2 Bases e Dimensão

Definição C.5 *Seja V um espaço vetorial sobre o corpo K. Um subconjunto S de V é dito* linearmente dependente (ou simplesmente LD) *se existem vetores distintos v_1, v_2, $\cdots$, v_n em S e escalares λ_1, λ_2, $\cdots$, λ_n em K, não todos nulos, tais que*

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0.$$

Um conjunto que não é LD é dito linearmente independente (ou simplesmente LI).

Observação C.1 *O que nos interessa de fato são os conjuntos de vetores LI. A Definição C.5 nos diz que S é LI se, e somente se, para quaisquer vetores distintos v_1, v_2, $\cdots$, v_n em S, $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$ implica que cada $\lambda_i = 0$.*

Definição C.6 *Uma* base *de um espaço vetorial V é um conjunto linearmente independente de geradores de V.*

Definição C.7 *Um espaço vetorial V é de* dimensão finita *se ele possui uma base finita. Nesse caso, o número de elementos da base é a dimensão de V, que denotamos por* $\dim V$.

Exemplo C.5 *Consideremos um espaço vetorial $\mathbb{C}^n$, on de $\mathbb{C}$ é o corpo dos números complexos. Seja S o subconjunto formado pelos vetores*

$$\begin{array}{rcl} e_1 & = & (1,0,0,\cdots,0) \\ e_2 & = & (0,1,0,\cdots,0) \\ \vdots & \vdots & \vdots \\ e_n & = & (0,0,0,\cdots,1). \end{array}$$

Se x_1, x_2, $\cdots$, x_n são escalares em K, podemos escrever

$$v = x_1e_1 + x_2e_2 + \cdots + x_ne_n,$$

ou seja, $v = (x_1, x_2, \cdots, x_n)$. Isso mostra que e_1, e_2, $\cdots$, e_n são geradores K^n.

Por outro lado,

$$\begin{array}{rcl} x_1e_1 + x_2e_2 + \cdots + x_ne_n = 0 & \Leftrightarrow & (x_1, x_2, \cdots, x_n) = (0,0,0,\cdots,0) \\ & \Leftrightarrow & x_1 = x_2 = \cdots = x_n = 0. \end{array}$$

Assim, os vetores e_1, e_2, $\cdots$, e_n são LI e, portanto, $S = \{e_1,\ e_2,\ \cdots,\ e_n\}$ é uma base de $\mathbb{C}^n$, denominada base canônica. *Como a base S do espaço $\mathbb{C}^n$ tem n elementos, podemos concluir que* $\dim \mathbb{C}^n = n$, *ou seja, $\mathbb{C}^n$ é um* espaço n-dimensional.

C.3 Transformações Lineares

Definição C.8 *Sejam V e W espaços vetoriais sobre um corpo K. Uma* transformação linear *T de V em W é uma função de V em W tal que*

$$T(\lambda u + v) = \lambda(Tu) + Tv,$$

para quaisquer vetores u, v em V e escalar $\lambda \in K$.

Exemplo C.6 *Seja K um corpo e V o espaço vetorial de todas as funções polinomiais $f : K \longrightarrow K$ dadas por*

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0.$$

Seja

$$(Df)(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2x + a_1.$$

Nesse caso, D é uma transformação linear de V em V chamada transformação derivação.

Definição C.9 *Sejam V e W espaços vetoriais sobre um corpo K. Uma transformação linear bijetora T de V em W é denominado um* isomorfismo *de V em W. Nesse caso, dizemos que V é* isomorfo *a W.*

Teorema C.1 *Todo espaço vetorial n-dimensional sobre um corpo K é isomorfo ao espaço K^n.*

Demonstração: Sejam V um espaço vetorial de dimensão n sobre um corpo K e $\mathscr{B} = \{\beta_1, \beta_2, \cdots, \beta_n\}$ uma base de V. Consideremos uma aplicação $T : V \longrightarrow K^n$ que associa cada vetor v de V a n-uplas de suas coordenadas com relação a base $\mathscr{B}$. Em outras palavras, sendo x_1, x_2, $\cdots$, x_n as coordenadas de um vetor qualquer de V com relação a base $\mathscr{B}$ temos que $Tv = (x_1, x_2, \cdots, x_n)$. É fácil perceber que T é uma transformação linear. Além disso, para qualquer vetor v de V existe uma única n-upla $(x_1, x_2, \cdots, x_n) \in K^n$ associada a v pois se existisse outra n-upla $(y_1, y_2, \cdots, y_n) \in K^n$ associada ao mesmo vetor teríamos

$$v = \sum_{i=1}^{n} x_i\beta_i \quad \text{e} \quad v = \sum_{i=1}^{n} y_i\beta_i,$$

logo

$$\sum_{i=1}^{n} x_i\beta_i = \sum_{i=1}^{n} y_i\beta_i \Rightarrow \sum_{i=1}^{n}(x_i - y_i)\beta_i = 0$$

e a independência linear dos vetores β_i nos levaria concluir que $x_i - y_i = 0$, ou seja, $x_i = y_i$, para cada i. Assim mostramos que T é injetiva. Além disso, se considerarmos uma n-upla qualquer $(x_1, x_2, \cdots, x_n) \in K^n$, ela representará as coordenadas do vetor $v = \sum_{i=1}^{n} x_i\beta_i$, logo T também é sobrejetora e, portanto, V e K^n são espaços vetoriais isomorfos. ∎

Geralmente, ao invés de utilizarmos n-uplas, é mais conveniente representar um vetor v por meio de uma matriz coluna das coordenadas de V em relação a uma base $\mathscr{B}$ do espaço vetorial ao qual ele pertence. Em outros termos, ao invés de escrevermos $v = (x_1, x_2, \cdots, x_n)$, podemos representar v por

$$[v]_{\mathscr{B}} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

onde x_1, x_2, $\cdots$, x_n são as coordenadas de v com relação a uma base de V.

Para finalizar esta secção, enunciaremos um teorema que nos mostra como determinar a matriz de uma transformação linear.

Teorema C.2 *Sejam V e W espaços vetoriais sobre um corpo K tais que $\dim V = n$ e $\dim W = m$. Sejam $\mathscr{B}$ e $\mathscr{B}'$ bases ordenadas de V e W, respectivamente. Para cada transformação linear $T : V \longrightarrow W$ existe uma matriz $m \times n$ A sobre o corpo K, denominada a matriz de T em relação a $\mathscr{B}$ e $\mathscr{B}'$, tal que*

$$[Tv]_{\mathscr{B}'} = A[v]_{\mathscr{B}},$$

para todo vetor v em V. Além disso, $T \mapsto A$ é uma correspondência bijetora entre o conjuntos das transformações lineares de V em W e o conjunto das matrizes $m \times n$ sobre o corpo K.

C.4 Espaços Vetoriais com Produto Interno

Definição C.10 *Sejam $\mathbb{C}$ o corpo dos números complexos e V um espaço vetorial sobre $\mathbb{C}$. Um* produto interno *em V é uma função que associa a cada par de vetores $u, v \in V$ um escalar $\langle u, v\rangle \in \mathbb{C}$ de modo que, para todo $u, v, w \in V$ e $\lambda \in \mathbb{C}$, temos:*

(a) $\langle v, v\rangle \geq 0$ e $\langle v, v\rangle = 0$ se, e somente se, $v = 0$;

(b) $\langle u, v\rangle = \overline{\langle v, u\rangle}$, onde a barra representa conjugação complexa;

(c) $\langle u + v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$;

(d) $\langle \lambda u, v\rangle = \lambda\langle u, v\rangle$;

Nas condições acima, dizemos que V é um espaço vetorial com produto interno.

Exemplo C.7 *Consideremos o espaço vetorial $\mathbb{C}^n$ sobre o corpo $\mathbb{C}$. Sejam $u = (u_1,\ u_2,\ \cdots,\ u_n)$ e $v = (v_1,\ v_2,\ \cdots,\ v_n)$ vetores em $\mathbb{C}^n$, o* produto interno canônico *desse espaço é definido por*

$$\langle u, v\rangle = u_1\overline{v}_1 + u_2\overline{v}_2 + \cdots + u_n\overline{v}_n = \sum_{j=1}^{n} u_j\overline{v}_j.$$

Quando tratamos do espaço $\mathbb{R}$, esta definição torna-se

$$\langle u, v\rangle = u_1v_1 + u_2v_2 + \cdots + u_nv_n = \sum_{j=1}^{n} u_jv_j.$$

Esse produto interno é, usualmente, chamado de produto escalar.

Definição C.11 *Consideremos um espaço vetorial com produto interno V sobre $\mathbb{C}$. Seja v um vetor em V. A* norma *de v é dada por*

$$\|v\| = \langle v, v\rangle^{1/2}.$$

Definição C.12 *Sejam u e v vetores num espaço vetorial V com produto interno. Dizemos que u e v são* vetores ortogonais *quando $\langle u, v\rangle = 0$. Se S é um subconjunto de V, dizemos que S é um* conjunto ortogonal *se dois quaisquer vetores distintos de S são ortogonais. Um conjunto* ortonormal *é um conjunto ortogonal S, com a propriedade adicional de que $\|v\| = 1$, para todo v em S.*

Exemplo C.8 *As bases canônicas de $\mathbb{R}^n$ e $\mathbb{C}^n$ são ortonormais em relação ao produto interno canônico definido no Exemplo C.7.*

Proposição C.3 *Seja V um espaço vetorial com produto interno, então, para quaisquer vetores $u, v \in V$ temos:*

(a) $|\langle v, u\rangle| \leq \|v\|\ \|u\|$ (desigualdade de Cauchy-Schwarz);

(b) $\|v + u\| \leq \|v\| + \|u\|$ (desigualdade triangular).

Demonstração: (a) Se $u = 0$, a desigualdade é óbvia. Suponhamos que $u \neq 0$ e vamos tomar $w = v - \dfrac{\langle v, u\rangle}{\|u\|^2}u$. Os vetores u e w são ortogonais, pois

$$\langle w, u\rangle = \left\langle v - \frac{\langle v, u\rangle}{\|u\|^2}u, u\right\rangle = \langle v, u\rangle - \frac{\langle v, u\rangle}{\|u\|^2}\langle u, u\rangle = \langle v, u\rangle - \frac{\langle v, u\rangle}{\|u\|^2}\|u\|^2 = 0.$$

Como $\|w\|^2 = \langle w, w\rangle \geq 0$ temos que

$$\begin{aligned}
\|v\|^2 &= \left\langle w + \frac{\langle v, u\rangle}{\|u\|^2}u,\ w + \frac{\langle v, u\rangle}{\|u\|^2}u\right\rangle \\
&= \langle w, w\rangle + \left\langle w,\ \frac{\langle v, u\rangle}{\|u\|^2}u\right\rangle + \left\langle \frac{\langle v, u\rangle}{\|u\|^2}u,\ w\right\rangle + \left\langle \frac{\langle v, u\rangle}{\|u\|^2}u,\ \frac{\langle v, u\rangle}{\|u\|^2}u\right\rangle \\
&= \|w\|^2 + \frac{\overline{\langle v, u\rangle}}{\|u\|^2}\langle w, u\rangle + \frac{\langle v, u\rangle}{\|u\|^2}\,\langle u, w\rangle + \frac{\langle v, u\rangle}{\|u\|^2}\cdot\frac{\overline{\langle v, u\rangle}}{\|u\|^2}\cdot\|u\|^2 \\
&= \|w\|^2 + \frac{|\langle v, u\rangle|^2}{\|u\|^2} \quad \geq \quad \frac{|\langle v, u\rangle|^2}{\|u\|^2}.
\end{aligned}$$

Logo, $|\langle v, u\rangle|^2 \leq \|v\|^2\|u\|^2$ e, portanto, $|\langle v, u\rangle| \leq \|v\|\ \|u\|$.

(b) Denotaremos por $\mathrm{Re}\langle u, v\rangle$ a parte real do produto interno $\langle u, v\rangle$. Desse modo

$$\begin{aligned}
\|v+u\|^2 &= \langle v+u, v+u\rangle = \langle v, v\rangle + \langle v, u\rangle + \langle u, v\rangle + \langle u, u\rangle \\
&= \|v\|^2 + \langle v, u\rangle + \overline{\langle v, u\rangle} + \|u\|^2 \\
&= \|v\|^2 + 2\cdot \mathrm{Re}\langle v, u\rangle + \|u\|^2 \\
&\leq \|v\|^2 + 2\cdot |\langle v, u\rangle| + \|u\|^2 \\
&\leq \|v\|^2 + 2\cdot \|v\|\cdot\|u\| + \|u\|^2 \qquad \text{(desigualdade de Cauchy-Schwarz)}
\end{aligned}$$

Portanto, $\|v+u\|^2 \leq (\|v\| + \|u\|)^2$ e, portanto, $\|v+u\| \leq \|v\| + \|u\|$. ■

Teorema C.3 *Um conjunto ortogonal de vetores não nulos é linearmente independente.*

Demonstração: Seja S um conjunto de vetores ortogonais em um espaço vetorial com produto interno V. Suponhamos que $v_1,\ v_2,\ \cdots,\ v_n$ sejam vetores distintos em S e que $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$. Desse modo

$$\langle v, v_i\rangle = \sum_j \langle \lambda_j v_j, v_i\rangle = \sum_j \lambda_j \langle v_j, v_i\rangle = \lambda_j \langle v_j, v_j\rangle.$$

Como $\langle v_j, v_j\rangle \neq 0$ temos que

$$\lambda_j = \frac{\langle v, v_j\rangle}{\langle v_j, v_j\rangle} = \frac{\langle v, v_j\rangle}{\|v_j\|^2}. \tag{C.1}$$

■

Corolário C.1 *Se um vetor v é combinação linear de um conjunto ortogonal de vetores não nulos $v_1,\ v_2,\ \cdots,\ v_n$ então v é exatamente a combinação linear*

$$v = \sum_{j=1}^{n} \frac{\langle v, v_j\rangle}{\|v_j\|^2} v_j.$$

Demonstração: Sendo $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n$, basta aplicar o resultado obtido em (C.1) para obter

$$\begin{aligned}
v &= \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n \\
&= \sum_{j=1}^{n} \lambda_j v_j = \sum_{j=1}^{n} \frac{\langle v, v_j\rangle}{\|v_j\|^2} v_j.
\end{aligned}$$

■

Referências Bibliográficas

[1] A. Terras, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, (1999).

[2] A. Hefez, *Aritmética*, Coleção PROFMAT, SBM, (2014).

[3] C. G. T. Moreira, F. E. B. Martinez, N. C. Saldanha, *Tópicos de Teoria dos Números*, Coleção PROFMAT, SBM, (2012).

[4] D. M. Burton, *Elementary number theory*, McGraw-Hill Companies, (2007).

[5] A. Gonçalves, *Introdução à Álgebra*, Projeto Euclides, SBM, (1979).

[6] K. Hoffman, R. Kunze *Linear Algebra*, Prentice-Hall, (1971).

[7] M. P. do Carmo, A. C. Morgado, E. Wagner, *Trigonometria, Números Complexos*, Coleção Professor de Matemática, SBM,(1992).