Universidade Federal de Pernambuco
Centro de Ciências Exatas e da Natureza
Programa de Pós Graduação em Matemática

André Luís de Sousa Vieira

Análise de Fourier em Grupos Finitos: Um Estudo Introdutório com Aplicações

Recife

2017

André Luís de Sousa Vieira

Análise de Fourier em Grupos Finitos: Um Estudo Introdutório com Aplicações

Dissertação apresentada ao Programa de Pós-graduação em Matemática da Universidade Federal de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Eduardo Shirlippe Góes Leandro

Recife

2017

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

V658a Vieira, André Luís de Sousa
Análise de Fourier em grupos finitos: um estudo introdutório com aplicações / André Luís de Sousa Vieira. – 2017.
80 f.

Orientador: Eduardo Shirlippe Góes Leandro.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CCEN, Matemática, Recife, 2017.
Inclui referências.

1. Matemática. 2. Representações de grupos. I. Leandro, Eduardo Shirlippe Góes (orientador). II. Título.

510 CDD (23. ed.) UFPE- MEI 2018-023

ANDRÉ LUÍS DE SOUSA VIEIRA

ANÁLISE FOURIER EM GRUPOS FINITOS: UM ESTUDO INTRODUTÓRIO COM APLICAÇÕES

Dissertação apresentada ao Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestrado em Matemática.

Aprovado em: 21/02/2017.

BANCA EXAMINADORA

_____

Prof. Dr. Eduardo Shirlippe Góes Leandro (Orientador)
Universidade Federal de Pernambuco

_____

Prof. Dr. Marco Barone (Examinador Externo)
Universidade Federal de Pernambuco

_____

Prof. Dr. Juliano Bandeira Lima (Examinador Externo)
Universidade Federal de Pernambuco

RESUMO

Nesta dissertação, é feita uma apresentação da teoria básica das representações de grupos finitos com o objetivo de introduzir a transformada de Fourier em tais grupos. A teoria de representação, que é a parte introdutória deste trabalho, é feita por meio de uma abordagem elementar, através do estudo dos homomorfismos de um grupo G em um grupo do tipo $GL(V)$, onde $GL(V)$ denota o grupo dos operadores invertíveis definidos em um espaço vetorial V. Apesar do caráter elementar, são apresentados resultados importantes, como o teorema de Maschke, o lema de Schur, as relações de ortogonalidade de Schur e um pouco da teoria dos caráteres. Em seguida, definimos a transformada como um isomorfismo da álgebra do grupo numa álgebra dada pelo produto direto de álgebras de matrizes, bem como estudamos suas propriedades básicas. Ao longo e ao final da dissertação são feitas algumas aplicações: teoria de grafos, anéis inteiros de grupos, centro da álgebra do grupo e caminhadas aleatórias em grupos finitos.

Palavras-chave: Análise harmônica. Representações de grupos. Caráteres.

ABSTRACT

In this dissertation a presentation of the basic theory of representations of finite groups with the objective of introducing the Fourier transform in such groups is provided. The theory of representation, which is an introductory part of this work, is done by means of an elementary approach, by studying the homomorphisms of a group G in a group of type $GL(V)$, where $GL(V)$ denotes the group of the invertible operators down in a vector space V. Despite the elementary character, important results are presented, such as Maschke's theorem, Schur's lemma, Schur's orthogonality relations, and a bit of character theory. Next, we define the transform as an isomorphism of the group algebra in an algebra given by the direct product of matrix algebras, and we study its basic properties. Throughout and at the end of the dissertation some applications are made: graph theory, groups interger rings, centers of group algebras and random walks in finite groups.

Keywords: Harmonic analysis. Group representations. Characters.

SUMÁRIO

1 INTRODUÇÃO

Organizamos a dissertação em três capítulos. No primeiro, apresentamos, de maneira bastante sucinta, a teoria básica das representações lineares de grupos, a qual é fundamental para os capítulos posteriores. Este capítulo é fortemente baseado em (STEINBERG, 2011), no entanto procuramos retirar tudo que não era essencial para a construção lógica do texto, bem como acrescentamos o que julgamos necessário para obtermos uma exposição mais clara. Introduzimos, por exemplo, a noção de representação matricial, a qual não é distinguida da noção de representação em (STEINBERG, 2011). Tanto esta definição quanto as proposições, com as respectivas demonstrações, que a envolvem são contribuições nossas. Um outro exemplo de acréscimo nosso é a proposição 2.1.28, cujo enunciado aparece em (STEINBERG, 2011) como um mero comentário, mas, devido a sua importância na estrutura da teoria, a demonstramos com todo o detalhe. Para uma abordagem também elementar da teoria de representação, mas de uma perspectiva diferente da nossa, indicamos (JAMES; LIEBECK, 2001). Já para um estudo mais avançado recomendamos, por exemplo, (SERRE, 2012) e (FULTON; HARRIS, 2013).

No segundo capítulo, tratamos da transformada de Fourier sobre grupos finitos, que é o assunto principal deste trabalho. Apesar deste capítulo também ter como referência principal (STEINBERG, 2011), o tratamos de forma muito mais detalhada que o anterior, isto é, retiramos menos e acrescentamos mais. Procuramos motivar algumas definições, acrescentar alguns resultados e fornecer demonstrações alternativas para as proposições mais importantes. Começamos recordando alguns conceitos que envolvem transformada de Fourier para funções no contexto contínuo, com o objetivo de fazer algumas analogias. Em seguida introduzimos transformada de Fourier sobre grupos abelianos finitos, a qual é suficiente para várias aplicações. Inclusive é feita uma aplicação dela aos chamados grafos de Cayley. Introduzimos as noções básicas sobre grafos, a fim de tornar o texto o mais auto-suficiente possível. Também incluímos algumas proposições sobre grafos, que são úteis para que tenhamos pelo menos uma noção básica da importância da aplicação que fizemos para esta teoria. Finalizamos o capítulo com um estudo detalhado da transformada de Fourier para grupos finitos arbitrários. Uma outra referência para a maior parte do assunto tratado neste capítulo, a qual é rica em aplicações, é (TERRAS, 1999).

O capítulo final é totalmente dedicado a aplicações. Começamos apresentando uma generalização da aplicação que fizemos no capítulo anterior, mas agora para um grafo de Cayley de um grupo não necessariamente abeliano. Nossa segunda aplicação diz respeito, principalmente, a teoria das unidades do anel $\mathbb{Z}G$. Por fim, faremos aplicações à teoria das probabilidades, ou, mais especificamente, às caminhadas aleatórias sobre

grupos finitos. Esta é a aplicação mais trabalhosa de todas, pois, diferentemente das duas últimas, o assunto aqui não é, a princípio, próximo do que desenvolvemos até então. Por isso, ele necessita que muitos conceitos e resultados sejam introduzidos. Porém o trabalho é recompensado pelos ganhos obtidos. Veremos, por exemplo, os chamados problemas de embaralhamento, que dizem respeito a maneiras de embaralhar cartas de modo que, ao final do processo, todas as cartas tenham a mesma chance de serem escolhidas ao acaso. Ou seja, como e quantas vezes devemos misturar as cartas de um baralho para torná-lo aleatório? Seremos capazes de, relativamente, responder a esta questão.

2 INTRODUÇÃO ÀS REPRESENTAÇÕES LINEARES DE GRUPOS

2.1 Definições básicas

Definição 2.1.1 (Representações e graus)**.** *Sejam G um grupo qualquer e V um $\mathbb{C}$-espaço vetorial de dimensão finita. Uma representação linear de G sobre V é um homomorfismo de grupos $\varphi : G \longrightarrow GL(V)$, onde $GL(V)$ é o grupo (cuja operação é a composição de funções) das bijeções lineares de V em V. A dimensão de V é o grau da representação φ, o qual será indicado por $\deg \varphi$.*

Observação 2.1.1. *A fim de simplificar os nomes e a notação, vamos, às vezes, nos referir a $\varphi : G \longrightarrow GL(V)$ simplesmente como uma representação de G e denotaremos o operador $\varphi(g)$ por φ_g, assim como $\varphi_g(v)$ será indicado por $\varphi_g v$.*

Definição 2.1.2 (Representação matricial)**.** *Seja $GL_n(\mathbb{C})$ o grupo das matrizes invertíveis de ordem n e com entradas em $\mathbb{C}$ e seja G um grupo. Uma representação matricial de G é um homomorfismo $\varphi : G \longrightarrow GL_n(\mathbb{C})$.*

Observação 2.1.2. *Dada uma representação matricial $\varphi : G \longrightarrow GL_n(\mathbb{C})$, vamos considerá-la uma representação linear de G sobre $\mathbb{C}^n$ compondo-a com o seguinte isomorfismo de grupos:*

$$\begin{array}{ccc} GL_n(\mathbb{C}) & \longrightarrow & GL(\mathbb{C}^n) \\ \mathcal{A} & \longmapsto & T \end{array}$$

onde $[T]_\xi = \mathcal{A}$ e ξ é a base canônica de $\mathbb{C}^n$. Ou seja, interpretaremos cada $\varphi(g)$ como um operador de $\mathbb{C}^n$ de maneira usual.

Definição 2.1.3 (Equivalência de representações)**.** *Sejam $\varphi : G \longrightarrow GL(V)$ e $\rho : G \longrightarrow GL(W)$ duas representações de um grupo G. Dizemos que φ é equivalente a ρ e escrevemos $\varphi \sim \rho$ se existe um isomorfismo $T : V \longrightarrow W$ tal que $\varphi_g = T^{-1}\rho_g T$ (ou equivalentemente $T\varphi_g = \rho_g T$) para todo $g \in G$.*

Em concordância com o seu nome, a relação definida acima é reflexiva, simétrica e transitiva, assim quando $\varphi \sim \rho$ (ou $\rho \sim \varphi$) diremos simplesmente que φ e ρ são equivalentes.

Observação 2.1.3. *Se na observação 2.1.2 tivéssemos considerado uma base diferente da canônica, obteríamos uma representação linear de G sobre $\mathbb{C}^n$ equivalente a que escolhemos.*

Proposição 2.1.1. *Sejam $\varphi : G \longrightarrow GL(V)$ uma representação de grau n e $B = \{v_1, ..., v_n\}$ uma base de V. Então $\varphi' : G \longrightarrow GL_n(\mathbb{C})$ definida por $\varphi'(g) = [\varphi_g]_B$ é uma representação matricial de G, a qual é equivalente a φ.*

Demonstração: É fácil ver que φ' é uma aplicação bem definida e que é homomorfismo, por isso mostraremos apenas que ela é equivalente a φ.

Precisamos exibir um isomorfismo $T : V \longrightarrow \mathbb{C}^n$ tal que $T\varphi_g = \varphi'_g T$ para todo $g \in G$. Nossa proposta é

$$\begin{array}{rcl} T : V & \longrightarrow & \mathbb{C}^n \\ v_j & \longmapsto & e_j \end{array}$$

onde $\xi = \{e_1, ..., e_n\}$ é a base canônica de $\mathbb{C}^n$. De fato, para $g \in G$ qualquer, temos:

$$[\varphi'_g(Tv_j)]_\xi = [\varphi'_g(e_j)]_\xi = [\varphi'_g]^\xi_\xi [e_j]_\xi = [\varphi_g]_B [e_j]_\xi,$$

que é a j-ésima coluna da matriz $[\varphi_g]_B$. Por outro lado

$$[T(\varphi_g(v_j))]_\xi = [T]^B_\xi [\varphi_g v_j]_B = I[\varphi_g v_j]_B = [\varphi_g]_B [v_j]_B,$$

que também é a j-ésima coluna da matriz $[\varphi_g]_B$. Portanto $T\varphi_g = \varphi'_g T$, ou seja, $\varphi'_g = T\varphi_g T^{-1}$. □

Corolário 2.1.1. *Sejam $\varphi : G \longrightarrow GL(V)$ e $\rho : G \longrightarrow GL(W)$ representações de G. Se $\varphi \sim \rho$, então, quaisquer que sejam as bases B_V de V e B_W de W, as representações matriciais*

$$\begin{array}{rcl} \varphi' : G & \longrightarrow & GL_n(\mathbb{C}) \\ g & \longmapsto & [\varphi_g]_{B_V} \end{array} \quad e \quad \begin{array}{rcl} \rho' : G & \longrightarrow & GL_m(\mathbb{C}) \\ g & \longmapsto & [\rho_g]_{B_W} \end{array}$$

são equivalentes. Reciprocamente, se existem B_V e B_W bases de V e W tais que φ' e ρ', definidas como acima, são equivalentes, então φ e ρ são equivalentes.

Demonstração: Basta aplicar a proposição anterior e usar a transitividade. □

Observação 2.1.4. *Duas representações matriciais $\varphi : G \longrightarrow GL_n(\mathbb{C})$ e $\rho : G \longrightarrow GL_m(\mathbb{C})$ são equivalentes se, e somente se, $m = n$ e existe uma matriz invertível $T \in GL_n(\mathbb{C})$ tal que $\varphi(g) = T^{-1}\rho(g)T$ para todo $g \in G$.*

Observação 2.1.5. *Identificaremos o grupo $GL_1(\mathbb{C})$ com $\mathbb{C}^* = \mathbb{C} - \{0\}$, munido do produto de números complexos.*

Corolário 2.1.2. *Duas representações matriciais de grau 1 são equivalentes se, e somente se, são iguais*

Demonstração: Como matrizes quadradas de ordem 1 comutam, o resultado segue. □

Exemplo 2.1.1 (Representação trivial)**.** *A representação trivial de um grupo G é a representação matricial dada por*

$$\begin{array}{rcl} \varphi : G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & 1 \end{array}$$

Exemplo 2.1.2. *Consideremos o grupo aditivo $\mathbb{Z}_n = \{[0], ..., [n-1]\}$ e seja $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{C}^*$ uma representação matricial de grau 1. Então $\varphi([1])^n = \varphi(n[1]) = \varphi([n]) = \varphi([0]) = 1$, logo os possíveis valores para $\varphi([1])$ são 1, $e^{\frac{2\pi i}{n}}$, ..., $(e^{\frac{2\pi i}{n}})^{n-1}$, os quais são as n raízes n-ésimas da unidade. Temos então n possíveis representações matriciais de grau 1 do grupo aditivo $\mathbb{Z}_n : \chi_0, ..., \chi_{n-1}$, onde $\chi_k([m]) = \chi_k(m[1]) = \chi_k([1])^m = e^{\frac{2\pi ikm}{n}}$. É fácil provar que estas funções são bem definidas e que $\chi_k([m] + [m']) = \chi_k([m]) \cdot \chi_k([m'])$. Pelo corolário 2.1.2, quaisquer duas destas representações são não-equivalentes, e pela proposição 2.1.1, uma representação de grau 1 de $\mathbb{Z}_n$ arbitrária é equivalente a alguma representação matricial de grau 1, logo é equivalente a uma destas. Portanto existem n classes de equivalência distinas de representações de grau 1 de $\mathbb{Z}_n$, das quais χ_0, ..., χ_{n-1} é um sistema completo de representantes.*

Exemplo 2.1.3 (Representação padrão de S_n)**.** *Consideremos o grupo S_n. A aplicação*

$$\begin{array}{rcl} \varphi : S_n & \longrightarrow & GL(\mathbb{C}^n) \\ \sigma & \longmapsto & \varphi_\sigma \end{array} \quad \textit{onde} \quad \begin{array}{rcl} \varphi_\sigma : \mathbb{C}^n & \longrightarrow & \mathbb{C}^n \\ e_i & \longmapsto & e_{\sigma(i)} \end{array}$$

é uma representação de S_n sobre o espaço $\mathbb{C}^n$, chamada representação padrão de S_n. Bem entendido, φ_σ é o único isomorfismo de $\mathbb{C}^n$ em $\mathbb{C}^n$ que leva a base canônica $\{e_1, ..., e_n\}$ nela mesma, de maneira indicada acima e, dados σ_1 e $\sigma_2 \in S_n$, temos $\varphi_{\sigma_1\sigma_2}(e_i) = e_{\sigma_1\sigma_2(i)} = e_{\sigma_1(\sigma_2(i))} = \varphi_{\sigma_1}(e_{\sigma_2(i)}) = \varphi_{\sigma_1}(\varphi_{\sigma_2}(e_i)) = \varphi_{\sigma_1}\varphi_{\sigma_2}(e_i)$. Portanto $\varphi_{\sigma_1\sigma_2} = \varphi_{\sigma_1}\varphi_{\sigma_2}$.

Definição 2.1.4 (Subespaço G-invariante)**.** *Seja $\varphi : G \longrightarrow GL(V)$ uma representação. Um subespaço W de V é dito G-invariante se ele é invariante por cada φ_g, ou seja, se, para todo $g \in G$ e $w \in W$, tem-se $\varphi_g w \in W$.*

Definição 2.1.5 (Subrepresentação)**.** *Sejam $\varphi : G \longrightarrow GL(V)$ uma representação de G sobre V e W um subespaço de V G-invariante. A aplicação $\varphi|W : G \longrightarrow GL(W)$ dada por $(\varphi|W)_g = \varphi_g|W$ é uma representação de G sobre W, chamada subrepresentação de φ.*

Definição 2.1.6 (Soma direta de representações)**.** *Sejam $\varphi^{(1)} : G \longrightarrow GL(V_1)$ e $\varphi^{(2)} : G \longrightarrow GL(V_2)$ representações de G. Então a soma direta (externa) de $\varphi^{(1)}$ e $\varphi^{(2)}$ é a representação de G sobre $V_1 \oplus V_2$ dada por:*

$$\begin{array}{rcl} \varphi^{(1)} \oplus \varphi^{(2)} : G & \longrightarrow & GL(V_1 \oplus V_2) \\ g & \longmapsto & (\varphi^{(1)} \oplus \varphi^{(2)})_g \end{array}$$

onde

$$\begin{array}{rcl} (\varphi^{(1)} \oplus \varphi^{(2)})_g : V_1 \oplus V_2 & \longrightarrow & V_1 \oplus V_2 \\ (v_1, v_2) & \longmapsto & (\varphi^{(1)}_g v_1, \varphi^{(2)}_g v_2). \end{array}$$

É fácil verificar que a soma direta externa é, de fato, uma representação de G.

Aplicando a definição acima para as representações matriciais $\varphi : G \longrightarrow GL_n(\mathbb{C})$ e $\rho : G \longrightarrow GL_m(\mathbb{C})$, temos $\varphi \oplus \rho : G \longrightarrow GL(\mathbb{C}^n \oplus \mathbb{C}^m)$ onde $(\varphi \oplus \rho)_g(v, u) = (\varphi_g v, \rho_g u)$ para todos $v \in \mathbb{C}^n$, $u \in \mathbb{C}^m$ e $g \in G$. Para uma base β de $\mathbb{C}^n \oplus \mathbb{C}^m$ adequada, a matriz $[(\varphi \oplus \rho)_g]_\beta$, correspondente a representação matricial

$$\begin{array}{rcl} \psi : G & \longrightarrow & GL_{n+m}(\mathbb{C}) \\ g & \longmapsto & [(\varphi \oplus \rho)_g]_\beta \end{array}$$

é uma matriz diagonal em blocos dada por $\begin{bmatrix} \varphi_g & 0 \\ 0 & \rho_g \end{bmatrix}$. Como ψ é equivalente a $\varphi \oplus \rho$, é razoável definir:

Definição 2.1.7 (Soma direta de representações matriciais)**.** *Sejam $\varphi^{(1)} : G \longrightarrow GL_n(\mathbb{C})$ e $\varphi^{(2)} : G \longrightarrow GL_m(\mathbb{C})$ representações matriciais de G. A soma direta (em termos matriciais) $\varphi^{(1)}$ e $\varphi^{(2)}$ é a representação matricial $\varphi^{(1)} \oplus \varphi^{(2)} : G \longrightarrow GL_{n+m}(\mathbb{C})$ definida por $(\varphi^{(1)} \oplus \varphi^{(2)})_g = \begin{bmatrix} \varphi_g^{(1)} & 0 \\ 0 & \varphi_g^{(2)} \end{bmatrix}$.*

Observação 2.1.6. *Naturalmente estendemos as definições 2.1.6 e 2.1.7 a uma quantidade finita de representações.*

Proposição 2.1.2. *Para $i \in \{1, ..., k\}$, sejam $\varphi^{(i)} : G \longrightarrow GL(V_i)$ e $\rho^{(i)} : G \longrightarrow GL(W_i)$ representações de G. Se $\varphi^{(i)} \sim \rho^{(i)}$ para todo i, então $\varphi^{(1)} \oplus \cdots \oplus \varphi^{(k)} \sim \rho^{(1)} \oplus \cdots \oplus \rho^{(k)}$.*

Demonstração: Para cada $i \in \{1, ..., k\}$, seja $T^{(i)} : V_i \longrightarrow W_i$ um isomorfismo tal que $T^{(i)}\varphi_g^{(i)} = \rho_g^{(i)} T^{(i)}$ para todo $g \in G$. Afirmo que $T = (T^{(1)}, ..., T^{(k)}) : V_1 \oplus \cdots \oplus V_k \longrightarrow W_1 \oplus \cdots \oplus W_k$ definido por $T(v_1, ..., v_k) = (T^{(1)}v_1, ..., T^{(k)}v_k)$ é o isomorfismo desejado. De fato, dado $g \in G$, temos

$$\begin{array}{rcl} T(\varphi^{(1)} \oplus \cdots \oplus \varphi^{(k)})_g(v_1, ..., v_k) & = & T(\varphi_g^{(1)}v_1, ..., \varphi_g^{(k)}v_k) \\ & = & (T^{(1)}\varphi_g^{(1)}v_1, ..., T^{(k)}\varphi_g^{(k)}v_k) \\ & = & (\rho_g^{(1)}T^{(1)}v_1, ..., \rho_g^{(k)}T^{(k)}v_k) \\ & = & (\rho^{(1)} \oplus \cdots \oplus \rho^{(k)})_g(T^{(1)}v_1, ..., T^{(k)}v_k) \\ & = & (\rho^{(1)} \oplus \cdots \oplus \rho^{(k)})_g T(v_1, ..., v_k). \end{array}$$

□

Proposição 2.1.3. *Seja $\varphi : G \longrightarrow GL(V)$ uma representação de grau n de G. Se $V = V_1 \oplus \cdots \oplus V_k$ onde cada V_i é um subespaço G-invariante de V, então $\varphi \sim \varphi|V_1 \oplus \cdots \oplus \varphi|V_k$.*

Demonstração: Para cada $i \in \{1, ..., k\}$, sejam $\varphi^{(i)} = \varphi|V_i$, $\mathrm{d}_i = \dim V_i$, β_i uma base de V_i e $\rho^{(i)} : G \longrightarrow GL_{\mathrm{d}_i}(\mathbb{C})$ a representação matricial definida por $\rho^{(i)}(g) = [\varphi_g^{(i)}]_{\beta_i}$. Como $\rho^{(i)} \sim \varphi^{(i)}$, a proposição anterior assegura que $\rho^{(1)} \oplus \cdots \oplus \rho^{(k)} \sim \varphi^{(1)} \oplus \cdots \oplus \varphi^{(k)}$.

Seja $\beta = \bigcup_i \beta_i$ e $\rho : G \longrightarrow GL_n(\mathbb{C})$ a representação matricial definida por $\rho(g) = [\varphi_g]_\beta$. Temos que $\rho \sim \varphi$ e

$$\rho(g) = \begin{bmatrix} [\varphi_g^{(1)}]_{\beta_1} & & 0 \\ & \ddots & \\ 0 & & [\varphi_g^{(k)}]_{\beta_k} \end{bmatrix} = (\rho^{(1)} \oplus \cdots \oplus \rho^{(k)})_g$$

Usando agora o corolário 2.1.1, concluímos o resultado. □

Definição 2.1.8 (Representação irredutível)**.** *Seja $\varphi : G \longrightarrow GL(V)$ uma representação de um grupo G. Dizemos que φ é irredutível se $\deg \varphi \neq 0$ e os únicos subespaços G-invariantes de V são $\{0\}$ e V.*

Exemplo 2.1.4. *Qualquer representação $\varphi : G \longrightarrow GL(V)$ de grau 1 é irredutível, visto que os únicos subespaços de V são $\{0\}$ e V.*

Definição 2.1.9 (Reducibilidade completa)**.** *Uma representação $\varphi : G \longrightarrow GL(V)$ é completamente redutível se $V = V_1 \oplus \cdots \oplus V_k$ onde cada V_i é um subespaço G-invariante de V e cada subrepresentação $\varphi|V_i$ é irredutível.*

Observação 2.1.7. *Dizer que $\varphi|V_i$ é irredutível equivale a afirmar que $V_i \neq \{0\}$ e os únicos subespaços de V_i G-invariantes (com respeito a φ) são $\{0\}$ e V_i.*

Observação 2.1.8. *A definição acima inclui o caso $k = 1$, que ocorre exatamente quando φ é irredutível. Portanto, mesmo soando horrivelmente, toda representação irredutível é completamente redutível.*

Proposição 2.1.4. *Seja $\varphi : G \longrightarrow GL(V)$ uma representação de um grupo G. Então φ é completamente redutível se, e somente se, $\varphi \sim \varphi^{(1)} \oplus \cdots \oplus \varphi^{(k)}$ onde $k \geq 1$ e $\varphi^{(1)}$, ..., $\varphi^{(k)}$ são representações irredutíveis de G.*

Demonstração: Suponhamos φ completamente redutível. Então $V = V_1 \oplus \cdots \oplus V_k$ com $k \geq 1$ e com toda a subrepresentação $\varphi|V_i$ irredutível. Pondo $\varphi^{(i)} = \varphi|V_i$ para cada i e usando a proposição 2.1.3 concluímos que $\varphi \sim \varphi^{(1)} \oplus \cdots \oplus \varphi^{(k)}$.

A demonstração da recíproca ficará mais clara quando tivermos a definição e as propriedades básicas dos morfismos entre representações, por isso a faremos depois. □

Definição 2.1.10 (Representação decomponível)**.** *Uma representação $\varphi : G \longrightarrow GL(V)$ é dita decomponível se $V = V_1 \oplus V_2$ com V_1 e V_2 subespaços G-invariantes e ambos não nulos.*

Observação 2.1.9. *As definições de representação irredutível, completamente redutível e decomponível são, como espera-se, invariantes com respeito à relação de equivalência de representações, ou seja, se φ e ρ são representações equivalentes, então φ é de algum dos três tipos se, e somente se, ρ também é. As respectivas demonstrações não são difíceis, por isso vamos omiti-las.*

2.2 Teorema de Maschke e Reducibilidade Completa

Definição 2.2.1 (Representação unitária)**.** *Seja $V \neq \{0\}$ um $\mathbb{C}$-espaço vetorial munido com produto hermitiano $\langle , \rangle$. Uma representação $\varphi : G \longrightarrow GL(V)$ é dita unitária se todos os operadores φ_g são unitários, isto é,*

$$\langle \varphi_g u, \varphi_g v \rangle = \langle u, v \rangle \text{ para todos } u, v \in V \text{ e } g \in G.$$

Observação 2.2.1. *Denotamos por $U_n(\mathbb{C})$ o subgrupo de $M_n(\mathbb{C})$ formado pelas matrizes unitárias. Se $\varphi : G \longrightarrow GL(V)$ é uma representação unitária e B é uma base ortonormal de V, então as matrizes $[\varphi_g]_B$ da representação matricial $\varphi' : G \longrightarrow GL_n(\mathbb{C})$ definida por $\varphi'(g) = [\varphi_g]_B$ são unitárias, ou seja, φ' é um homomorfismo de G em $U_n(\mathbb{C})$.*

Observação 2.2.2. *Quando escrevemos uma representação matricial na forma $\varphi : G \longrightarrow U_n(\mathbb{C})$, estamos assumindo tacitamente que $\mathbb{C}^n$ está munido com o produto hermitiano usual. Consequentemente φ é unitária.*

Proposição 2.2.1. *Seja $\varphi : G \longrightarrow GL(V)$ uma representação unitária. Então φ é irredutível ou decomponível.*

Demonstração: Por definição, φ é diferente de zero. Suponhamos que φ não é irredutível. Então existe um subspaço G-invariante W com $W \neq \{0\}$ e $W \neq V$. Temos que $V = W \oplus W^{\perp}$, onde $W^{\perp}$ é o complemento ortogonal de W, e vamos provar que $W^{\perp}$, o qual é diferente de zero, é um subspaço G-invariante de V. De fato, dados $u \in W^{\perp}$, $w \in W$ e $g \in G$ arbitrários, temos

$$\langle \varphi_g u, w \rangle = \langle u, (\varphi_g)^* w \rangle = \langle u, (\varphi_g)^{-1} w \rangle = \langle u, \varphi_{g^{-1}} w \rangle.$$

Como $\varphi_{g^{-1}} w \in W$, temos $\langle \varphi_g u, w \rangle = 0$. Portanto $\varphi_g u \in W^{\perp}$. □

Proposição 2.2.2. *Toda representação não-nula de um grupo finito G é equivalente a uma representação unitária.*

Demonstração: Como $\varphi \neq 0$, φ é equivalente a uma representação $\rho : G \longrightarrow GL(\mathbb{C}^n)$ ($n \geq 1$). Vamos mostrar que ρ é unitária quando consideramos o produto hermitiano em $\mathbb{C}^n$ que

definiremos a seguir. Seja $\langle , \rangle$ o produto usual de $\mathbb{C}^n$ e definamos $(\cdot, \cdot) : \mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$ por $(u, v) = \sum_{g \in G} \langle \rho_g u, \rho_g v \rangle$. É fácil provar que $(\cdot, \cdot)$ é um produto hermitiano sobre $\mathbb{C}^n$.

Sejam $v, u \in \mathbb{C}^n$ e $h \in G$ arbitrários.

$$\begin{aligned}(\varphi_h v, \varphi_h v) &= \sum_{g \in G} \langle \varphi_g(\varphi_h u), \varphi_g(\varphi_h v) \rangle \\ &= \sum_{g \in G} \langle \varphi_{gh} u, \varphi_{gh} v \rangle.\end{aligned}$$

Como $G \longrightarrow G$, $g \longmapsto gh$ é uma bijeção, temos

$$(\varphi_h v, \varphi_h v) = \sum_{x \in G} \langle \varphi_x u, \varphi_x v \rangle = (u, v).$$

□

Corolário 2.2.1. *Sejam G um grupo finito e $\varphi : G \longrightarrow GL(V)$ uma representação de grau diferente de zero. Então φ é irredutível ou decomponível.*

Demonstração: Imediato das duas últimas proposições. □

Observação 2.2.3. *A representação $\varphi : \mathbb{Z} \longrightarrow GL_2(\mathbb{C})$, definida por $\varphi(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, não é irredutível nem decomponível (também não é completamente redutível).*

Teorema 2.2.1 (Maschke)**.** *Toda representação não-nula de um grupo finito é completamente redutível.*

Demonstração: Seja $\varphi : G \longrightarrow GL(V)$ uma representação não-nula de um grupo finito G. Faremos indução no grau de φ. Se $\deg \varphi = 1$, então φ é irredutível. Seja $\deg \varphi = n \geq 2$ e suponhamos que o resultado é válido para representações de grau menor que n. Caso φ não seja irredutivel, será decomponível, isto é, $V = V_1 \oplus V_2$ com V_1 e V_2 G-invariantes e não-nulos. Segue que as subrepresentações φ/V_1 e φ/V_2 são representações não-nulas de um grupo finito e possuem grau menor que n. Aplicando a hipótese de indução, obtemos que $V_1 = U_1 \oplus \cdots \oplus U_s$ onde, para cada $j \in \{1, ..., s\}$, U_j é um subspaço de V_1 G-invariante com respeito a φ/V_1 (e portanto é G-invariante com respeito a φ) e os únicos subspaços de U_j que são G-invariantes por φ/V_1 (logo por φ) são $\{0\}$ e U_j (veja a observação 2.1.7). O mesmo vale para $V_2 = W_1 \oplus \cdots \oplus W_r$. Assim $V = U_1 \oplus \cdots \oplus U_s \oplus W_1 \oplus \cdots \oplus W_r$ e φ é completamente redutível. □

2.3 Morfismos de Representações e Lema de Schur

Definição 2.3.1 (Morfismo)**.** *Sejam $\varphi : G \longrightarrow GL(V)$ e $\rho : G \longrightarrow GL(W)$ representações de um grupo G. Um morfismo de φ em ρ é uma aplicação linear $T : V \longrightarrow W$ tal que $T\varphi_g = \rho_g T$, para todo $g \in G$.*

Observação 2.3.1. *Denotaremos o conjunto dos morfismos de φ em ρ por $Hom_G(\varphi,\rho)$ (ou simplesmente por $Hom(\varphi,\rho)$). Valem as propriedades básicas esperadas, isto é; se I é o operador identidade de V, então $I \in Hom(\varphi,\varphi)$; Dados $T \in Hom(\varphi,\rho)$ e $S \in Hom(\rho,\psi)$, então $S \circ T \in Hom(\varphi,\psi)$; se $T \in Hom(\varphi,\rho)$ é invertível, então $T^{-1} \in Hom(\rho,\varphi)$.*

Proposição 2.3.1. *Sejam $\varphi : G \longrightarrow GL(V)$ e $\rho : G \longrightarrow GL(W)$ representações de G. Se V' e W' são subespaços G-invariantes de V e W respectivamente e se $T \in Hom(\varphi,\rho)$, então $T^{-1}(W')$ e $T(V')$ são subespaços G-invariantes de V e W respectivamente. Consequentemente $Ker(T)$ é subespaço G-invariante de V e $Im(T)$ é subespaço G-invariante de W.*

Demonstração: Temos que $T^{-1}(W')$ é subespaço de V. A fim de provar que ele é G-invariante sejam $v \in T^{-1}(W')$ e $g \in G$. Então

$$T(\varphi_g v) = T\varphi_g v = \rho_g T v = \rho_g(Tv).$$

Como $Tv \in W'$ e este é G-invariante, temos $\rho_g(Tv) \in W'$ e, com isso, $\varphi_g v \in T^{-1}(W')$. Similarmente prova-se que $T(V')$ é G-invariante. Fazendo $V' = V$ e $W' = \{0\}$, obtem-se as outras afirmações. □

Observação 2.3.2. *Sejam $\rho^{(i)} : G \longrightarrow GL(W_i)$ com $i = 1, ..., k$ representações de G e seja $\rho = \rho^{(1)} \oplus \cdots \oplus \rho^{(k)}$ sua soma direta externa. É fácil provar que as aplicações*

$$\begin{aligned} \alpha_i : W_i &\longrightarrow W_1 \oplus \cdots \oplus W_k \\ w_i &\longmapsto (0, ..., 0, w_i, 0, ..., 0) \end{aligned}$$

são morfismos (injetivos) de $\rho^{(i)}$ em ρ, isto é, $\alpha_i \in Hom\left(\rho^{(i)}, \rho\right)$, $i = 1, ..., k$. Com isto, podemos provar a recíproca da proposição 2.1.4 . De fato, suponhamos que $\varphi \sim \rho = \rho^{(1)} \oplus \cdots \oplus \rho^{(k)}$ com $\rho^{(i)}$ irredutível para cada i. Então existe um isomorfismo $T : V \longrightarrow W = W_1 \oplus \cdots \oplus W_k$ com $T \in Hom(\varphi,\rho)$. Não é difícil provar que $W = W_1 \oplus \cdots \oplus W_k = \alpha_1(W_1) \oplus \cdots \oplus \alpha_k(W_k)$ (esta segunda soma direta é interna) e que isto acarreta que $V = V_1 \oplus \cdots \oplus V_k$ onde $V_i = T^{-1}(\alpha_i(W_i)) \neq \{0\}$, para todo i. Precisamos provar que os V_i são G-invariantes e que eles não contém subespaços G-invariantes além de $\{0\}$ e eles mesmos. A proposição anterior garante a veracidade das implicações: $\alpha_i \in Hom\left(\rho^{(i)}, \rho\right) \Rightarrow \alpha_i(W_i)$ é subespaço G-invariante de W, e $T \in Hom(\varphi,\rho) \Rightarrow T^{-1}(\alpha_i(W_i))$ é subespaço G-invariante de V. Portanto $V_1, ..., V_k$ são G-invariantes. Fixado $i \in \{1, ..., k\}$, seja V_i' um subespaço G-invariante de V_i. Temos que $T(V_i')$ é subespaço G-invariante de W contido em $\alpha_i(W_i)$. Portanto $\alpha_i^{-1}(T(V_i'))$ é subespaço G-invariante de W_i. Como $\rho^{(i)}$ é irredutível, $\alpha_i^{-1}(T(V_i')) = \{0\}$ ou $\alpha_i^{-1}(T(V_i')) = W_i$, e usando apenas propriedades básicas de funções, vemos que isto força $V_i' = \{0\}$ ou $V_i' = V_i$, como queríamos demonstrar.

Proposição 2.3.2. *Sejam $\varphi : G \longrightarrow GL(V)$ e $\rho : G \longrightarrow GL(W)$ representações de G. Então $Hom(\varphi,\rho)$ é um subespaço de $Hom(V,W)$ (o espaço das aplicações lineares de V em W).*

Demonstração: Sejam $T_1, T_2 \in \mathrm{Hom}_G(\varphi, \rho)$ e $c_1, c_2 \in \mathbb{C}$. Então:

$$(c_1T_1 + c_2T_2)\varphi_g = c_1T_1\varphi_g + c_2T_2\varphi_g = c_1\rho_gT_1 + c_2\rho_gT_2 = \rho_g(c_1T_1 + c_2T_2).$$

Portanto $c_1T_1 + c_2T_2 \in \mathrm{Hom}\,(\varphi, \rho)$. □

Lema 2.3.1 (Lema de Schur)**.** *Sejam $\varphi : G \longrightarrow GL\,(V)$ e $\rho : G \longrightarrow GL\,(W)$ representações irredutíveis de G e seja $T \in Hom_G(\varphi, \rho)$. Então $T = 0$ ou T é invertível. Consequentemente:*

1. *Se φ e ρ não são equivalentes, então $Hom_G(\varphi, \rho) = \{0\}$.*
2. *Se $\varphi = \rho$ então $T = \lambda I$ para algum $\lambda \in \mathbb{C}$.*

Demonstração: Usando a proposição 2.3.1 e a irredutibilidade de φ e ρ, temos: $T \neq 0 \Rightarrow (\mathrm{Ker}\,(T) \neq V$ e $\mathrm{Im}\,(T) \neq \{0\}) \Rightarrow (\mathrm{Ker}\,(T) = \{0\}$ e $\mathrm{Im}\,(T) = W) \Rightarrow T$ é invertível $\Rightarrow \varphi \sim \rho$. As implicações acima provam que $T = 0$ ou T é invertível e provam o item 1.

A fim de provar o item 2, seja λ um autovalor do operador T (estamos no caso $\varphi = \rho$). Pela proposição anterior, $T - \lambda I \in \mathrm{Hom}_G(\varphi, \varphi)$ e tal operador não é invertivel, portanto $T - \lambda I = 0$, ou seja, $T = \lambda I$. □

Corolário 2.3.1. *Sejam $\varphi : G \longrightarrow GL\,(V)$ e $\rho : G \longrightarrow GL\,(W)$ representações irredutíveis de G. Se $\varphi \sim \rho$ e $T \in Hom_G(\varphi, \rho)$ é invertível, então $Hom_G(\varphi, \rho) = \{\lambda T \ : \ \lambda \in \mathbb{C}\}$.*

Demonstração: $S \in \mathrm{Hom}_G(\varphi, \rho)$ e $T^{-1} \in \mathrm{Hom}_G\,(\rho, \varphi)$ implicam que $T^{-1}S \in \mathrm{Hom}_G\,(\varphi, \varphi)$. Usando o lema de Schur, temos $T^{-1}S = \lambda I \Rightarrow S = T(\lambda I) = \lambda TI = \lambda T$. □

Corolário 2.3.2. *Seja G um grupo abeliano. Então qualquer representação irredutível de G tem grau 1.*

Demonstração: Seja $\varphi : G \longrightarrow \mathrm{GL}\,(V)$ irredutível. Como G é abeliano, $\varphi_g \in \mathrm{Hom}_G\,(\varphi, \varphi) = \{\lambda I \ : \ \lambda \in \mathbb{C}\}$, para todo $g \in G$. Assim, dado $v \in V$, o subspaço $\{\lambda v \ : \ \lambda \in \mathbb{C}\}$ é G-invariante, ou seja, todo subspaço de dimensão 1 é G-invariante, donde segue o resultado. □

Corolário 2.3.3. *Seja G um grupo finito abeliano e $\varphi : G \longrightarrow GL_n\,(\mathbb{C})$ uma representação matricial de G. Então existe uma matriz invertível T tal que $T^{-1}\varphi(g)T$ é diagonal para todo $g \in G$.*

Demonstração: Pelo teorema de Maschke e pelo corolário anterior, existem $\varphi^{(1)}$, ..., $\varphi^{(n)}$ representações matriciais irredutíveis, logo de grau 1, tais que $\varphi \sim \varphi^{(1)} \oplus \cdots \oplus \varphi^{(n)}$. Usando

agora a Observação 2.1.4, temos

$$T^{-1}\varphi(g)T = (\varphi^{(1)} \oplus \cdots \oplus \varphi^{(n)})(g) = \begin{bmatrix} \varphi^{(1)}(g) & & 0 \\ & \ddots & \\ 0 & & \varphi^{(n)}(g) \end{bmatrix}$$

Para alguma matriz T invertível. □

Observação 2.3.3. *Sejam $\varphi : G \longrightarrow GL_n(\mathbb{C})$ e $\rho : G \longrightarrow GL_m(\mathbb{C})$ representações matriciais de G. Usando a aplicação $Hom(\mathbb{C}^n, \mathbb{C}^m) \longrightarrow M_{n\times m}(\mathbb{C})$ que leva cada transformação linear de $\mathbb{C}^n$ em $\mathbb{C}^m$ na sua respectiva matriz com respeito as bases canônicas, podemos interpretar o subspaço $Hom_G(\varphi, \rho)$ como o subspaço de $M_{n\times m}(\mathbb{C})$ formado pelas matrizes $\mathcal{A}$ tais que $\mathcal{A}\varphi(g) = \rho(g)\mathcal{A}\ \forall\ g \in G$. Assim, as versões matriciais para o lema de Schur e para os demais resultados desta seção são óbivias.*

2.4 Álgebra do Grupo e a Representação Regular

A partir desta seção, vamos sempre supor que o grupo com o qual estivermos trabalhando seja finito. Seja G um grupo. Vamos definir um $\mathbb{C}$-espaço vetorial que tem G como base (ortonormal) da seguinte forma:

$$\mathbb{C}G = \{\sum_{g\in G} \lambda_g g \ :\ \lambda_g \in \mathbb{C}\}.$$

Ou seja, o conjunto denotado por $\mathbb{C}G$ é formado por todas as combinações lineares formais dos elementos de G, com coeficientes em $\mathbb{C}$. Por definição

$$\sum_{g\in G} \lambda_g g = \sum_{g\in G} \mu_g g \Leftrightarrow \lambda_g = \mu_g\ \forall g \in G.$$

Definimos a soma e a multiplicação por

$$\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g$$

e

$$\lambda \left(\sum_{g\in G} \lambda_g g \right) = \sum_{g\in G} \lambda\lambda_g g.$$

Temos também o produto hermitiano

$$\left\langle \sum_{g\in G} \lambda_g g, \sum_{g\in G} \mu_g g \right\rangle = \sum_{g\in G} \lambda_g \overline{\mu_g}.$$

É facil provar que a soma, a multiplicação por escalar e o produto hermitiano satisfazem as propriedades requeridas para que $\mathbb{C}G$ seja um $\mathbb{C}$-espaço vetorial com produto hermitiano.

Observação 2.4.1. *As aplicações*

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C}G \\ \lambda & \longmapsto & \lambda 1_G + \sum\limits_{h \neq 1_G} 0h \end{array} \quad e \quad \begin{array}{ccc} G & \longrightarrow & \mathbb{C}G \\ g & \longmapsto & 1g + \sum\limits_{h \neq g} 0h \end{array}$$

são injetivas, portanto podemos identificar suas imagens com $\mathbb{C}$ *e* G *respectivamente. Dessa forma,* $\mathbb{C}$ *e* G *são subconjuntos de* $\mathbb{C}G$*.*

Observação 2.4.2. *Não é difícil provar que* G *é base ortonormal de* $\mathbb{C}G$*.*

Definição 2.4.1 (Representação regular)**.** *Seja* G *um grupo finito. A representação regular de* G *é o homorfimismo*

$$\begin{array}{ccc} L : G & \longrightarrow & GL(\mathbb{C}G) \\ g & \longmapsto & L_g \end{array} \quad onde \quad \begin{array}{ccc} L_g : \mathbb{C}G & \longrightarrow & \mathbb{C}G \\ h & \longmapsto & gh. \end{array}$$

Bem entendido, L_g *é o operador de* $\mathbb{C}G$ *que leva a base* G *nela própria, da seguinte maneira: dado* $h \in G$*,* $L_g(h) = gh$*. Com isto,* L *é uma aplicação bem definida. Para ver que* L *é um homomorfismo, sejam* $g, h, x \in G$*.*

$$L_{gh}(x) = (gh)x = g(hx) = L_g(L_h(x)) = L_g L_h(x).$$

Portanto $L_{gh} = L_g L_h$*.*

Proposição 2.4.1. *A representação regular de* G *é unitária.*

Demonstração: Ora, cada operador L_g é unitário, pois leva base ortonormal em base ortonormal. □

É bastante natural definir o seguinte produto em $\mathbb{C}G$:

$$\left(\sum_{g \in G} \lambda_g g\right) \cdot \left(\sum_{h \in G} \mu_h h\right) = \sum_{g \in G} \sum_{h \in G} \lambda_g \mu_h (gh).$$

Provaremos que, com este produto, $\mathbb{C}G$ é uma algebra sobre $\mathbb{C}$.

Observação 2.4.3. *Para cada* $g \in G$ *fixado, façamos* $gh = x$ *(e portanto* $h = g^{-1}x$*). Como a aplicação* $G \longrightarrow G$ *que leva* h *em* gh *é uma bijeção, temos*

$$\sum_{g \in G} \sum_{h \in G} \lambda_g \mu_h (gh) = \sum_{g \in G} \sum_{x \in G} \lambda_g \mu_{g^{-1}x} x = \sum_{x \in G} \left(\sum_{g \in G} \lambda_g \mu_{g^{-1}x}\right) x.$$

Definição 2.4.2. *Seja* V *um* $\mathbb{C}$*-espaço vetorial. Dizemos que* V *é uma álgebra sobre* $\mathbb{C}$ *se, além das operações de espaço vetorial, está definido um produto que satisfaz as seguintes condições:*

1. $v_1 \cdot (v_2 \cdot v_3) = (v_1 \cdot v_2) \cdot v_3$*,* $\forall v_1, v_2, v_3 \in V$*.*

2. $v_1 \cdot (v_2 + v_3) = v_1 \cdot v_2 + v_1 \cdot v_3$ *e* $(v_1 + v_2) \cdot v_3 = v_1 \cdot v_3 + v_2 \cdot v_3$, $\forall v_1, v_2, v_3 \in V$.

3. Existe $1 \in V$ *tal que* $1 \cdot v = v \cdot 1 = v$, $\forall v \in V$.

4. $\lambda(v_1 \cdot v_2) = (\lambda v_1) \cdot v_2 = v_1 \cdot (\lambda v_2)$, $\forall v_1, v_2 \in V$ *e* $\lambda \in \mathbb{C}$.

Ou seja, o espaço vetorial V *é uma álgebra sobre* $\mathbb{C}$ *se, com o produto* $\cdot$ *,* V *é um anel e a multiplicação por escalar e o produto* $\cdot$ *são compatíveis, isto é, vale 4.*

Antes de provarmos que o espaço $\mathbb{C}G$ é uma álgebra, veremos duas observações importantes.

Observação 2.4.4. *Como comentamos na observação 2.4.2,* G*, além de subconjunto, é base (ortonormal) de* $\mathbb{C}G$*. Portanto um elemento* $\sum_{g \in G} \lambda_g g$ *de* $\mathbb{C}G$ *será interpretado não mais como uma expressão formal, mas como uma combinação linear de fato. Por exemplo, dados* $g, h \in G \subset \mathbb{C}G$ *e* $\lambda, \mu \in \mathbb{C}$*, temos* $(\lambda + \mu)g = \lambda g + \mu g$ *e* $\lambda(g + h) = \lambda g + \lambda h$*, ou seja, podemos usar as propriedades de espaço vetorial sem peso na consciência.*

Observação 2.4.5. *Não é difícil provar que a aplicação de inclusão de* $\mathbb{C}$ *em* $\mathbb{C}G$ *da observação 2.4.1 respeita soma e produto, assim podemos dizer que o corpo* $\mathbb{C}$ *esta contido em* $\mathbb{C}G$*. Do mesmo modo, o grupo* G *está contido em* $\mathbb{C}G$*. Por exemplo, se* $g, h \in G$ *e* $\lambda, \mu \in \mathbb{C}$*, o produto de* g *por* h *como elementos de* G *é* gh*, que é produto de* $g \in \mathbb{C}G$ *por* $h \in \mathbb{C}G$*. O mesmo vale para* $\lambda\mu$*.*

Proposição 2.4.2. *O espaço vetorial* $\mathbb{C}G$ *munido com o produto definido anteriormente é uma álgebra.*

Demonstração: Precisamos verificar as condições da definição 2.4.2. Comecemos pelo item 4. Sejam $\lambda \in \mathbb{C}$, $r = \sum_{g \in G} \lambda_g g$ e $s = \sum_{h \in G} \mu_h h$ elementos de $\mathbb{C}G$. Então

$$\lambda(r \cdot s) = \lambda \sum_{g \in G} \sum_{h \in G} \lambda_g \mu_h (gh) = \sum_{g,h \in G} \lambda \lambda_g \mu_h (gh) = \left(\sum_{g \in G} \lambda \lambda_g g \right) \left(\sum_{h \in G} \mu_h h \right) = (\lambda r) \cdot s.$$

Do mesmo modo, prova-se que $\lambda(r \cdot s) = r \cdot (\lambda s)$. Vejamos agora a condição 2. Sejam r e s denotados como antes e seja $t = \sum_{g \in G} \alpha_g g$.

$$\begin{aligned}
(r + t) \cdot s &= \left(\sum_{g \in G} (\lambda_g + \alpha_g) g \right) \cdot \left(\sum_{h \in G} \mu_h h \right) \\
&= \sum_{g,h \in G} (\lambda_g \mu_h + \alpha_g \mu_h)\, gh \\
&= \sum_{g,h \in G} \lambda_g \mu_h (gh) + \sum_{g,h \in G} \alpha_g \mu_h (gh) \\
&= r \cdot s + t \cdot s.
\end{aligned}$$

De forma análoga prova-se a outra distributividade.

Para provar o item 1, usaremos os dois itens provados acima. Sejam r e s como antes e seja $t = \sum_{x \in G} \alpha_x x$.

$$\begin{aligned}(rs)t &= \left(\sum_{g,h\in G} \lambda_g \mu_h (gh)\right) \cdot \left(\sum_{x\in G} \alpha_x x\right) \\ &= \sum_{g,h,x\in G} \lambda_g \mu_h \alpha_x (gh)x.\end{aligned}$$

$$\begin{aligned}r(st) &= \left(\sum_{g,h\in G} \lambda_g g\right) \cdot \left(\sum_{h,x\in G} \mu_h \alpha_x (hx)\right) \\ &= \sum_{g,h,x\in G} \lambda_g \mu_h \alpha_x g(hx).\end{aligned}$$

Finalmente, dado $r \in \mathbb{C}G$,

$$r1_G = \left(\sum_{g\in G} \lambda_g g\right) 1_G = \sum_{g\in G} \lambda_g (g1_G) = r.$$

Analogamente, $1_G r = r$. □

2.5 Relações de Ortogonalidade de Schur

Sejam G um grupo finito e $\varphi : G \longrightarrow GL_n(\mathbb{C})$ uma representação matricial de G. Denotando por $\varphi_{ij}(g)$ a entrada ij da matriz φ_g, obtemos n^2 funções de G em $\mathbb{C}$:

$$\begin{array}{rccc}\varphi_{ij} : G & \longrightarrow & \mathbb{C} & \\ g & \longmapsto & \varphi_{ij}(g) & \end{array}, \quad 1 \leq i, j \leq n.$$

O ambiente adequado para estudar tais funções é o espaço vetorial das funções de G em $\mathbb{C}$, o qual denotaremos por $L^2(G)$. Veremos que este espaço é uma reformulação de $\mathbb{C}G$, com uma pequena diferença no produto hermitiano, por isso também o chamaremos de álgebra do grupo G.

Definição 2.5.1 (Álgebra do grupo)**.** *Dado um grupo finito G, definimos o $\mathbb{C}$-espaço vetorial $L^2(G) = \{f \ : \ f : G \longrightarrow \mathbb{C}\}$ com a soma e a multiplicação por escalar definidas como se faz usualmente num espaço de funções, e o produto hermitiano dado por*

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g\in G} f_1(g)\overline{f_2(g)} \ , \text{ para todos } f_1, f_2 \in L^2(G).$$

Observação 2.5.1. *Seja* $\{\delta_g \ : \ g \in G\}$*, onde* $\delta_g(h) = 0$ *se* $h \neq g$*, e* $\delta_g(g) = 1$*, a base canônica de* $L^2(G)$*. Temos um isomorfismo natural entre os espaços* $L^2(G)$ *e* $\mathbb{C}G$*, que é a aplicação*

$$\begin{array}{rcl} T : L^2(G) & \longrightarrow & \mathbb{C}G \\ \delta_g & \longmapsto & g \end{array},$$

isto é, T *leva a base* $\{\delta_g \ : \ g \in G\}$ *na base* G *de maneira óbvia. Percebamos que a base* $\{\delta_g \ : \ g \in G\}$ *é apenas ortogonal:* $\langle \delta_g, \delta_g \rangle = \dfrac{1}{|G|}$*. Isto ocorre porque o produto hermitiano que fixamos em* $L^2(G)$ *é, por causa do fator* $\dfrac{1}{|G|}$*, um pouco diferente do produto que seria a versão do produto hermitiano de* $\mathbb{C}G$ *para* $L^2(G)$*.*

Observação 2.5.2. *No próximo capítulo definiremos um produto em* $L^2(G)$*, que corresponde ao produto definido em* $\mathbb{C}G$*, com o qual* $L^2(G)$ *tornar-se-á, de fato, uma álgebra.*

Proposição 2.5.1. *Sejam* $\varphi : G \longrightarrow GL(V)$ *e* $\rho : G \longrightarrow GL(W)$ *representações do grupo finito* G *e seja* $T : V \longrightarrow W$ *uma aplicação linear. Então:*

1. $T^{\#} = \dfrac{1}{|G|} \sum\limits_{g \in G} \rho_{g^{-1}} T \varphi_g \in Hom_G(\varphi, \rho)$.
2. *Se* $T \in Hom_G(\varphi, \rho)$*, então* $T^{\#} = T$.
3. *A aplicação* $P : Hom(V, W) \longrightarrow Hom_G(\varphi, \rho)$ *definida por* $P(T) = T^{\#}$ *é linear e sobrejetiva.*

Demonstração: Devido a sua importância, provaremos apenas o item 1. As demonstrações dos outros itens podem ser encontradas em (STEINBERG, 2011). Claramente $T^{\#}$ é uma aplicação linear de V em W. Seja $h \in G$. Temos que

$$T^{\#}\varphi_h = (\frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g)\varphi_h = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_{gh}$$

Fazendo $gh = x$ (e portanto $g^{-1} = hx^{-1}$), obtemos:

$$\begin{array}{rcl} T^{\#}\varphi_h & = & \dfrac{1}{|G|} \sum\limits_{x \in G} \rho_{hx^{-1}} T \varphi_x \\ & = & \rho_h (\dfrac{1}{|G|} \sum\limits_{x \in G} \rho_{x^{-1}} T \varphi_x) \\ & = & \rho_h T^{\#} \end{array}$$

□

Proposição 2.5.2. *Sejam* $\varphi : G \longrightarrow GL(V)$*,* $\rho : G \longrightarrow GL(W)$ *representações irredutíveis de* G *e seja* $T : V \longrightarrow W$ *uma aplicação linear. Então:*

1. *Se φ e ρ não são equivalentes, então $T^{\#} = 0$.*

2. *Se $\varphi = \rho$, então $T^{\#} = \dfrac{Traço\,(T)}{deg\ \varphi} I$.*

Demonstração: O item 1 segue imediatamente do lema de Schur e da proposição anterior. No caso $\varphi = \rho$, $T^{\#}$ é o operador de V definido por $T^{\#} = \dfrac{1}{|G|}\sum_{g\in G}\varphi_{g^{-1}} T \varphi_g$, portanto

$$\begin{aligned} \text{Traço } (T^{\#}) &= \frac{1}{|G|}\sum_{g\in G}\text{Traço}(\varphi_{g^{-1}} T \varphi_g) \\ &= \frac{1}{|G|}|G|\text{Traço}(T) \\ &= \text{Traço}(T). \end{aligned}$$

Por outro lado, o lema de Schur garante que $T^{\#} = \lambda I$ para algum $\lambda \in \mathbb{C}$. Consequentemete, $\text{Traço}(T) = \text{Traço}(T^{\#}) = \text{Traço}(\lambda I) = \lambda \deg\ \varphi$, ou seja, $\lambda = \dfrac{\text{Traço}(T)}{\deg\ \varphi}$. □

Observação 2.5.3. *Tendo em vista a observação 2.3.3, se $\varphi : G \longrightarrow GL_n(\mathbb{C})$ e $\rho : G \longrightarrow GL_m(\mathbb{C})$ são representações matriciais e A é uma matriz $m \times n$, então $A^{\#} = \dfrac{1}{|G|}\sum_{g\in G}\rho(g^{-1})A\varphi(g) \in Hom_G(\varphi, \rho)$ (interpretado matricialmente). Se φ e ρ são irredutíveis e não-equivalentes, então $A^{\#} = 0$. E finalmente, se φ é irredutível e A é uma matriz $n \times n$, então $A^{\#} = \dfrac{1}{|G|}\sum_{g\in G}\varphi(g^{-1})A\varphi(g) = \dfrac{Traço(A)}{n} I$.*

Lema 2.5.1 (Veja (STEINBERG, 2011) na página 33)**.** *Sejam $\mathcal{A} \in M_{r\times m}(\mathbb{C})$, $\mathcal{B} \in M_{n\times s}(\mathbb{C})$ e $\mathcal{E}_{ki}$ a matriz da base canônica de $M_{m\times n}(\mathbb{C})$ cuja entrada ki é 1 e as demais são nulas. Então $(\mathcal{A}\mathcal{E}_{ki}\mathcal{B})_{lj} = a_{lk}b_{ij}$ onde $\mathcal{A} = (a_{ij})$ e $\mathcal{B} = (b_{ij})$.*

Lema 2.5.2. *Sejam $\varphi : G \longrightarrow U_n(\mathbb{C})$ e $\rho : G \longrightarrow U_m(\mathbb{C})$ representações matriciais unitárias. Então $\left((\mathcal{E}_{ki})^{\#}\right)_{lj} = \langle \varphi_{ij}, \rho_{kl} \rangle$.*

Demonstração: Como ρ é unitária, $\rho_{g^{-1}} = \rho_g^{-1} = \rho_g^*$. Portanto $\rho_{lk}(g^{-1}) = \overline{\rho_{kl}(g)}$.

$$\begin{aligned} \left((\mathcal{E}_{ki})^{\#}\right)_{lj} &= \left(\frac{1}{|G|}\sum_{g\in G}\rho_{g^{-1}}\mathcal{E}_{ki}\varphi_g\right)_{lj} \\ &= \frac{1}{|G|}\sum_{g\in G}\left(\rho_{g^{-1}}\mathcal{E}_{ki}\varphi_g\right)_{lj} \\ &= \frac{1}{|G|}\sum_{g\in G}\rho_{lk}(g^{-1})\varphi_{ij}(g) \\ &= \frac{1}{|G|}\sum_{g\in G}\varphi_{ij}(g)\overline{\rho_{kl}(g)} \\ &= \langle \varphi_{ij}, \rho_{kl} \rangle. \end{aligned}$$

□

Teorema 2.5.1 (Relações de Ortogonalidade de Schur)**.** *Sejam $\varphi : G \longrightarrow U_n(\mathbb{C})$ e $\rho : G \longrightarrow U_m(\mathbb{C})$ representações matriciais irredutíveis, não equivalentes e unitárias. Então:*

1. $\langle \varphi_{ij}, \rho_{kl} \rangle = 0$.
2. $\langle \varphi_{ij}, \varphi_{kl} \rangle = \begin{cases} \frac{1}{n} \text{ , se } i = k \text{ e } j = l, \\ 0 \text{ , caso contrário.} \end{cases}$

Demonstração: O item 1 segue imediatamente da observação 2.5.3 combinada com o lema anterior. Estes dois resultados também garantem que

$$\langle \varphi_{ij}, \varphi_{kl} \rangle = \left(\frac{\text{Traço}(E_{ki})}{n} I \right)_{lj}.$$

E desta igualdade obtemos o item 2. □

Corolário 2.5.1. *Seja $\varphi : G \longrightarrow U_d(\mathbb{C})$ uma representação matricial, unitária e irredutível. Então as d^2 funções $\{\sqrt{d}\varphi_{ij} \ : \ 1 \leq i, j \leq d\}$ formam um conjunto ortonormal em $L^2(G)$.*

Demonstração: Imediata do item 2 do teorema 2.5.1. □

Corolário 2.5.2. *O número de classes de equivalência de representações irredutíveis de um grupo finito G é finito e limitado por $|G|$.*

Demonstração: De cada uma destas classes de equivalência, podemos escolher como representante uma representação matricial e unitária, da qual podemos extrair pelo menos uma função do tipo φ_{ij}, isto é, uma "função entrada". O conjunto formado por tais funções (que são não-nulas) é, pelas relações de ortogonalidade de Schur, ortogonal, portanto sua cardinalidade é limitada pela dimensão de $L^2(G)$, que é $|G|$. □

Observação 2.5.4. *Combinando o exemplo 2.1.4 com o corolário 2.3.2, concluímos que as representações irredutíveis de um grupo abeliano G são precisamente as representações de grau 1. Revisitando agora o exemplo 2.1.2, vemos que existem $n = |\mathbb{Z}_n|$ classes de representações irredutíveis de $\mathbb{Z}_n$, das quais χ_0, ..., χ_{n-1} formam um sistema completo de representantes (matriciais e unitários). Veremos que este exemplo não é um caso isolado. Pelo contrário, o número de classes de representações irredutíveis de um grupo finito G é $|G|$ se, e somente se, G é abeliano.*

Corolário 2.5.3. *Seja G um grupo finito e sejam $\varphi^{(1)}$, ..., $\varphi^{(s)}$ um sistema completo de representantes matriciais e unitários das classes de representações irredutíveis de G. Então, pondo $d_k = deg\ \varphi^{(k)}$, com $k = 1, ..., n$, as funções*

$$\{\sqrt{d_k}\varphi^{(k)}_{ij} \ : \ 1 \leq k \leq s, \ 1 \leq i, j \leq d_k\}$$

formam um conjunto ortonormal em $L^2(G)$. Consequentemente $s \leq d_1^2 + \cdots + d_s^2 \leq |G|$.

2.6 Caráteres e Funções de Classe

Definição 2.6.1 (Caráter)**.** *Seja $\varphi : G \longrightarrow GL(V)$ uma representação. O caráter da representação φ é a função $\chi_\varphi : G \longrightarrow \mathbb{C}$ definida por $\chi_\varphi(g) = Traço(\varphi_g)$, para todo $g \in G$. Um caráter de um grupo G é o caráter de alguma representação de G, e se tal representação for irredutível, diremos que este é um caráter irredutível de G.*

Observação 2.6.1. *Se $\varphi : G \longrightarrow GL_n(\mathbb{C})$ é uma representação matricial de G, então*

$$\chi_\varphi(g) = Traço(\varphi_g) = \sum_{i=1}^{n} \varphi_{ii}(g).$$

Observação 2.6.2. *Sejam $\varphi : G \longrightarrow GL(V)$ uma representação e B uma base de V. Então $\chi_\varphi = \chi_{\varphi'}$ onde φ' é a representação matricial de G determinada por φ e B.*

Observação 2.6.3. *Se $\varphi : G \longrightarrow \mathbb{C}^*$ é uma representação matricial de grau 1, então $\chi_\varphi = \varphi$.*

Proposição 2.6.1. *Seja φ uma representação de G. Então $\chi_\varphi(1_G) = deg\ \varphi$. Consequentemente o caráter de uma representação não-nula é não-nulo.*

Demonstração: Imediata. □

Proposição 2.6.2. *Se φ e ρ são representações equivalentes de um grupo G, então $\chi_\varphi = \chi_\rho$.*

Demonstração: Sejam φ' e ρ' representações matriciais obitidas a partir de φ e ρ, como no corolário 2.1.1. Usando o corolário 2.1.1, a observação 2.1.4, a observação 2.6.2 e o fato que o traço é invariante pela relação de semelhança de matrizes, obtemos: $\chi_\varphi(g) = \chi_{\varphi'}(g) = \text{Traço}\left(\varphi'_g\right) = \text{Traço}\left(T^{-1}\rho'_g T\right) = \text{Traço}\left(\rho'_g\right) = \chi_{\rho'}(g) = \chi_\rho(g)$, para todo $g \in G$. □

Proposição 2.6.3. *Seja φ uma representação de G. Então, para todos $g, h \in G$, tem-se*

$$\chi_\varphi(g) = \chi_\varphi(hgh^{-1}).$$

Demonstração: Análoga à anterior. □

Definição 2.6.2 (Função de classe)**.** *Uma função $f : G \longrightarrow \mathbb{C}$ é dita uma função de classe se $f(g) = f(hgh^{-1})$ para todos $g, h \in G$, ou seja, se f é constante nas classes de conjugação de G. Indicaremos o subconjunto de $L^2(G)$ formado pelas funções de classe por $Class(L^2(G))$.*

Observação 2.6.4. *$f \in Class(L^2(G)) \Leftrightarrow f(gh) = f(hg)$ para todos $g, h \in G$.*

Observação 2.6.5. *Devido a proposição 2.6.3, concluímos que os caráteres de um grupo G são elementos de $Class(L^2(G))$.*

Observação 2.6.6. *É fácil observar que Class*$(L^2(G))$ *é, na verdade, um subespaço de* $L^2(G)$.

Proposição 2.6.4. *Denotemos por* $Cl(G)$ *o conjunto cujos elementos são as classes de conjugação de* G. *Então o conjunto* $B = \{\delta_C \ : \ C \in Cl(G)\}$, *onde*

$$\delta_C(g) = \begin{cases} 1 \ \textit{se} \ g \in C \\ 0 \ \textit{caso contrário,} \end{cases}$$

é uma base de Class$(L^2(G))$. *Consequentemente dimClass*$(L^2(G)) = |Cl(G)|$.

Demonstração: Dados $f \in \text{Class}\,(L^2(G))$ e $C \in \text{Cl}(G)$, indiquemos por $f(C)$ o valor de f em qualquer elemento de C. É fácil ver que

$$f = \sum_{C \in \text{Cl}(G)} f(C)\delta_C$$

e, portanto, B gera $\text{Class}\,(L^2(G))$.

Também é muito simples concluir que B é LI: basta avaliar a combinação linear trivial $\sum_{C \in \text{Cl}(G)} \lambda_C \delta_C = 0$ em um elemento $g \in C_0$ para concluir que o escalar λ_{C_0} é nulo. □

Teorema 2.6.1 (Primeiras relações de ortogonalidade para caráteres)**.** *Sejam* φ *e* ρ *representações irredutíveis de* G. *Então*

$$\langle \chi_\varphi, \chi_\rho \rangle = \begin{cases} 1 \ \textit{se} \ \varphi \sim \rho, \\ 0 \ \textit{caso contrário.} \end{cases}$$

Consequentemente os caráteres irredutíveis de G *formam um conjunto ortonormal em Class*$(L^2(G))$.

Demonstração: Pela proposição 2.6.2, podemos supor que $\varphi : G \longrightarrow U_n(\mathbb{C})$ e $\rho : / \longrightarrow GU_m(G)$ são representações matriciais e unitárias.

$$\begin{aligned} \langle \chi_\varphi, \chi_\rho \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g) \overline{\chi_\rho(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^{n} \varphi_{ii}(g) \right) \left(\sum_{j=1}^{m} \overline{\rho_{jj}(g)} \right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{1}{|G|} \sum_{g \in G} \varphi_{ii}(g) \overline{\rho_{jj}(g)} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle \varphi_{ii}, \rho_{jj} \rangle. \end{aligned}$$

Se φ e ρ não são equivalentes, as relações de ortogonalidade de Schur (teorema 2.5.1) garantem que $\langle \varphi_{ii}, \rho_{jj} \rangle = 0$, quaisquer que sejam i e j. Portanto $\langle \chi_\varphi, \chi_\rho \rangle = 0$ neste caso.

Assumindo agora que $\varphi \sim \rho$, podemos, pela proposição 2.6.2, supor que $\varphi = \rho$ e neste caso as relações de ortogonalidade de Schur dizem que

$$\langle \varphi_{ii}, \varphi_{jj} \rangle = \begin{cases} \frac{1}{n} \text{ se } i = j \\ 0 \text{ se } i \neq j \end{cases}$$

Portanto

$$\begin{aligned} \langle \chi_\varphi, \chi_\rho \rangle &= \sum_{i=1}^{n} \sum_{j=1}^{n} \langle \varphi_{ii}, \varphi_{jj} \rangle \\ &= \sum_{i=1}^{n} \langle \varphi_{ii}, \varphi_{ii} \rangle \\ &= \sum_{i=1}^{n} \frac{1}{n} = 1. \end{aligned}$$

□

Observação 2.6.7. *Tendo em vista o teorema acima, concluímos que duas representações irredutíveis φ e ρ são equivalentes se, e somente se, seus respectivos caráteres coincidem. Posteriormente, vamos estender este resultado para representações arbitrárias.*

Corolário 2.6.1. *Existem no máximo $|Cl(G)|$ classes de representações irredutíveis de G.*

Demonstração: O conjunto dos caráteres irredutíveis de G, cuja cardinalidade é precisamente o número de classes de representações irredutíveis de G, é ortonormal, portanto sua cardinalidade é no máximo $\dim \text{Class}\,(L^2(G)) = |\text{Cl}(G)|$. □

Observação 2.6.8. *Dada uma representação $\varphi : G \longrightarrow GL\,(V)$, vamos denotar a representação $\varphi \oplus \cdots \oplus \varphi$ ($m \geq 1$ parcelas) por $m\varphi$. Sejam $\varphi^{(1)}$, ..., $\varphi^{(s)}$ um sistema completo de representantes das classes de representações irredutíveis de G. Combinando a proposição 2.1.2 com o teorema de Maschke, obtemos, para cada representação ρ de G, a decomposição*

$$\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}.$$

Aqui estamos convencionando que $m_i = 0$ quando não houver uma representação equivalente a $\varphi^{(i)}$ na decomposição de ρ. No caso $m_i > 1$, dizemos que $\varphi^{(i)}$ é uma componente irredutível de ρ. Provaremos logo mais que tal decomposição é única, isto é, para cada representação ρ, os coeficientes m_1, ..., m_s são unicamente determinados.

Observação 2.6.9. *Se $\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$ então deg $\rho = m_1 d_1 + \cdots + m_s d_s$ onde $d_i =$ deg $\varphi^{(i)}$, $i = 1, ..., s$.*

Lema 2.6.1. *Seja $\varphi = \rho \oplus \psi$. Então $\chi_\varphi = \chi_\rho + \chi_\psi$.*

Demonstração: Podemos assumir que $\rho : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$ e $\psi : G \longrightarrow \mathrm{GL}_m(\mathbb{C})$ são representações matriciais, logo $\varphi : G \longrightarrow \mathrm{GL}_{n+m}(\mathbb{C})$ é dada por:

$$\varphi_g = \begin{bmatrix} \rho_g & 0 \\ 0 & \psi_g \end{bmatrix} \text{ (matriz diagonal em blocos).}$$

Donde segue o resultado. □

Teorema 2.6.2. *Seja $\varphi^{(1)}, \ldots, \varphi^{(s)}$ um sistema completo de representantes das classes de representações irredutíveis de G e seja $\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$. Então $m_i = \langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle$. Consequentemente a decomposição de ρ em componentes irredutíveis é única.*

Demonstração: Pelo lema acima

$$\chi_\rho = m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}.$$

Usando agora o teorema 2.6.1 obtemos que $m_i = \langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle$, $i = 1, ..., s$. □

Corolário 2.6.2. *As representações φ e ρ de um grupo G são equivalentes se, e somente se, $\chi_\varphi = \chi_\rho$.*

Corolário 2.6.3. *Uma representação ρ é irredutível se, e somente se, $\langle \chi_\rho, \chi_\rho \rangle = 1$.*

Demonstração: Sendo $\rho \sim m_1\varphi^{(1)} \oplus \cdots \oplus m_s\varphi^{(s)}$, $\langle \chi_\rho, \chi_\rho \rangle = m_1^2 + \cdots + m_s^2$. O resultado segue desta igualdade. □

Proposição 2.6.5. *Seja $L : G \longrightarrow GL(\mathbb{C}G)$ a representação regular de G da definição 2.4.1 e seja χ_L seu respectivo caráter. Então*

$$\chi_L(g) = \begin{cases} |G| \text{ se } g = 1_G, \\ 0 \text{ se } g \neq 1_G. \end{cases}$$

Demonstração: Sejam $G = \{g_1, ..., g_n\}$ e $[L_g]$ a matriz de L_g com respeito a esta ordenação de G. Então:

$$\begin{aligned} [L_g]_{ij} &= \begin{cases} 1 \text{ se } g_i = gg_j, \\ 0 \text{ caso contrário.} \end{cases} \\ &= \begin{cases} 1 \text{ se } g = g_ig_j^{-1}, \\ 0 \text{ caso contrário.} \end{cases} \end{aligned}$$

em particular,

$$[L_g]_{ii} = \begin{cases} 1 \text{ se } g = 1_G, \\ 0 \text{ caso contrário.} \end{cases}$$

Portanto $\chi_L(g) = \mathrm{Traço}(L_g) = \begin{cases} |G| \text{ se } g = 1_G, \\ 0 \text{ se } g \neq 1_G. \end{cases}$ □

Observação 2.6.10. *Para os próximos resultados vamos assumir que $\varphi^{(1)}$, ..., $\varphi^{(s)}$ é um sistema completo de representantes das classes de representações irredutíveis de G, com $d_i = deg\ \varphi^{(i)}$ e $\chi_i = \chi_{\varphi^{(i)}}$, $i = 1, ..., s$.*

Teorema 2.6.3. *Seja L a representação regular de G. Então*

$$L \sim d_1\varphi^{(1)} \oplus \cdots \oplus d_s\varphi^{(s)}.$$

Demonstração:

$$\begin{aligned} \langle \chi_L, \chi_i \rangle &= \frac{1}{|G|}\sum_{g\in G}\chi_L(g)\overline{\chi_i(g)} \\ &= \frac{1}{|G|}|G|\overline{\chi_i(1_G)} \\ &= \deg\ \varphi^{(i)} \\ &= d_i. \end{aligned}$$

□

Corolário 2.6.4. *Vale a igualdade $|G| = d_1^2 + \cdots + d_s^2$.*

Demonstração: Como $L \sim d_1\varphi^{(1)} \oplus \cdots \oplus d_s\varphi^{(s)}$, temos:

$$\begin{aligned} |G| &= \deg\ L \\ &= \deg\ \left(d_1\varphi^{(1)} \oplus \cdots \oplus d_s\varphi^{(s)}\right) \\ &= d_1\deg\ \varphi^{(1)} + \cdots + d_s\deg\ \varphi^{(s)} \\ &= d_1^2 + \cdots + d_s^2. \end{aligned}$$

□

Teorema 2.6.4. *Suponhamos adicionalmente que $\varphi^{(1)}$, ... ,$\varphi^{(s)}$ são matriciais e unitárias. Então o conjunto $B = \{\sqrt{d_k}\varphi_{ij}^{(k)} \ : \ 1 \leq k \leq s,\ 1 \leq i, j \leq d_k\}$ é base ortonormal de $L^2(G)$.*

Demonstração: Pelo corolário 2.5.3, sabemos que tal conjunto é ortonormal e, como sua cardinalidade é $d_1^2 + \cdots + d_s^2$, o corolário anterior garante o resultado. □

Teorema 2.6.5. *O conjunto $\{\chi_1, ..., \chi_s\}$ (formado pelos caráteres irredutíveis de G) é uma base ortonormal para Class$\,(L^2(G))$.*

Demonstração: Já sabemos que tal conjunto é ortonormal, portanto basta provar que ele é gerador. Dada $f \in$ Class$\,(L^2(G))$ podemos, pelo teorema anterior, escrever

$$f = \sum_{k,i,j} C_{ij}^{(k)}\varphi_{ij}^{(k)},$$

onde $C_{ij}^{(k)} \in \mathbb{C}$, $1 \leq k \leq s$ e $1 \leq i, j \leq d_k$. Notemos os índices i e j dependem de k, portanto este deve sempre vir primeiro no somatório.

Explorando o fato de f ser uma função de classe, usando a escrita de f acima e lembrando da Observação 2.5.3, obtemos a seguinte sequência de igualdades:

$$\begin{aligned}
f(x) &= \frac{1}{|G|}\sum_{g\in G} f(g^{-1}xg) \\
&= \frac{1}{|G|}\sum_{g\in G}\sum_{k,i,j} C_{ij}^{(k)}\varphi_{ij}^{(k)}(g^{-1}xg) \\
&= \sum_{k,i,j} C_{ij}^{(k)}\frac{1}{|G|}\sum_{g\in G}\varphi_{ij}^{(k)}(g^{-1}xg) \\
&= \sum_{k,i,j} C_{ij}^{(k)}\left[\frac{1}{|G|}\sum_{g\in G}\varphi_{g^{-1}}^{(k)}\varphi_{x}^{(k)}\varphi_{g}^{(k)}\right]_{ij} \\
&= \sum_{k,i,j} C_{ij}^{(k)}\left[(\varphi_x^{(k)})^{\#}\right]_{ij} \\
&= \sum_{k,i,j} C_{ij}^{(k)}\left[\frac{\text{Traço}\left(\varphi_x^{(k)}\right)}{\deg\,\varphi^{(k)}} I\right]_{ij} \\
&= \sum_{k,i} C_{ii}^{(k)}\frac{1}{d_k}\chi_k(x) \\
&= \left(\sum_k\left(\sum_i \frac{C_{ii}^{(k)}}{d_k}\right)\chi_k\right)(x).
\end{aligned}$$

Portanto $f = \sum_{k=1}^{s}\left(\sum_{i=1}^{d_k}\frac{C_{ii}^{(k)}}{d_k}\right)\chi_k$. □

Corolário 2.6.5. *O número de classes de representações irredutíveis de G é o número de classes de conjugação de G.*

Demonstração: Imediata. □

Corolário 2.6.6. *Um grupo finito G é abeliano se, e somente se, ele possui $|G|$ classes de representações irredutíveis.*

Demonstração: G é abeliano $\Leftrightarrow |G| = |\mathrm{Cl}(G)| \Leftrightarrow |G| = s$. □

Definição 2.6.3 (Tabela de caráteres)**.** *Seja G um grupo finito cujos caráteres irredutíveis são χ_1, ..., χ_s e as classes de conjugação são C_1, ..., C_s. A tabela de caráteres de G é a matriz $X_{s\times s}$ definida por $X_{ij} = \chi_i(C_j)$ (lembrando que $\chi_i(C_j)$ é o valor da função de classe χ_i avaliada em qualquer elemento de C_j).*

Exemplo 2.6.1. *A tabela de caráteres de* $\mathbb{Z}_4$ *é dada por:*

	[0]	[1]	[2]	[3]
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

Teorema 2.6.6 (Segundas relações de ortogonalidade para caráteres)**.** *Sejam* C *e* C' *classes de conjugação de* G *e sejam* $g \in C$ *e* $h \in C'$*. Então*

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} \frac{|G|}{|C|} \text{ se } C = C', \\ 0 \text{ caso contrário.} \end{cases}$$

Consequentemente, as colunas da tabela de caráteres são duas a duas ortogonais, portanto a tabela de caráteres é invertível.

Demonstração: Temos que $\delta_{C'} = \sum_{i=1}^{s} \langle \delta_{C'}, \chi_i \rangle \chi_i$. Assim

$$\begin{aligned} \delta_{C'}(g) &= \sum_{i=1}^{s} \langle \delta_{C'}, \chi_i \rangle \chi_i(g) \\ &= \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x \in G} \delta_{C'}(x)\overline{\chi_i(x)}\chi_i(g) \\ &= \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x \in C'} \overline{\chi_i(x)}\chi_i(g) \\ &= \frac{|C'|}{|G|} \sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(h)} \end{aligned}$$

Como $\delta_{C'}(g) = 0$ se $C \neq C'$, e $\delta_{C'}(g) = 1$ se $C = C'$, o resultado segue. □

3 ANÁLISE DE FOURIER EM GRUPOS FINITOS

Nosso objeto de estudo neste capítulo, como seu título sugere, está relacionado com a análise de Fourier clássica, a qual é feita sobre funções no contexto contínuo (funções definidas em $\mathbb{R}$). Não temos a pretensão de estudar tais relações, mas estamos interessados em, pelo menos, fazer algumas analogias. Por isso relembraremos alguns conceitos.

3.1 Análise de Fourier Clássica

Sejam $f, g : \mathbb{R} \longrightarrow \mathbb{C}$ funções absolutamente integráveis. Então a convolução de f por g é definida por

$$f * g(x) = \int_{-\infty}^{\infty} f(x-y)g(y)dy$$

A transformada de Fourier de f é a função

$$\widehat{f}(x) = \int_{-\infty}^{\infty} f(t)e^{-2\pi ixt}dt.$$

A fórmula de inversão diz que

$$f(x) = \int_{-\infty}^{\infty} \widehat{f}(t)e^{2\pi ixt}dt.$$

E, por fim, vale a seguinte relação

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g}.$$

Poderíamos tentar estudar as versões discretas das fórmulas acima, isto é, para funções $f, g : \mathbb{Z} \longrightarrow \mathbb{C}$. Se supusermos adicionalmente que $f, g : \mathbb{Z} \longrightarrow \mathbb{C}$ são n-periódicas, poderemos identificar f e g como funções de $L^2(\mathbb{Z}_n)$ (é fácil exibir uma bijeção entre o conjunto das funções n-periódicas de $\mathbb{Z}$ em $\mathbb{C}$ e o conjunto $L^2(\mathbb{Z}_n)$). Isto é ótimo para nós, já que estamos interessados em fazer análise de Fourier em funções definidas em grupos. Sem mais rodeios, daremos as definições correspondentes para funções $f, g : \mathbb{Z} \longrightarrow \mathbb{C}$ n-periódicas que, repetimos, podem ser pensadas como funções de $L^2(\mathbb{Z}_n)$. A convolução de f por g é definida por

$$f * g(m) = \sum_{k=0}^{n-1} f(m-k)g(k).$$

Dada uma função $f \in L^2(\mathbb{Z}_n)$, lembremos que os caráteres irredutíveis de $\mathbb{Z}_n$, $\{\chi_0, ..., \chi_{n-1}\}$ onde $\chi_k([m]) = e^{\frac{2\pi ikm}{n}}$, formam uma base ortonormal para $L^2(\mathbb{Z}_n)$, logo $f = \sum_{k=0}^{n-1} \langle f, \chi_k \rangle \chi_k$.

Definimos a transformada de Fourier de f nesse contexto, como a função $\widehat{f} \in L^2(\mathbb{Z}_n)$ dada por

$$\widehat{f}([m]) = n\langle f, \chi_m \rangle = \sum_{k=0}^{n-1} f([k]) e^{\frac{-2\pi i m k}{n}}.$$

Temos agora que

$$f = \sum_{k=0}^{n-1} \langle f, \chi_k \rangle \chi_k \Rightarrow f = \frac{1}{n} \sum_{k=0}^{n-1} n\langle f, \chi_k \rangle \chi_k \Rightarrow f = \frac{1}{n} \sum_{k=0}^{n-1} \widehat{f}([k]) \chi_k.$$

Portanto a fórmula da inversão é dada por

$$f([m]) = \frac{1}{n} \sum_{k=0}^{n-1} \widehat{f}([k]) e^{\frac{2\pi i k m}{n}}.$$

Mostraremos posteriormente que vale a igualdade $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$.

A tradução da convolução para funções de $L^2(\mathbb{Z}_n)$ é perfeita: a integral dá lugar à soma e esta é tomada somente nos valores que importam. Já as traduções da transformada de Fourier e da fórmula da inversão não são tão perfeitas assim, mas são similares o suficiente para justificar os mesmos nomes. Aliás, um dos objetivos principais desta seção introdutória é justificar, mesmo que superficialmente, a nossa terminologia.

3.2 A Convolução

Nesta seção, vamos generalizar a convolução de funções de $L^2(\mathbb{Z}_n)$ para funções de $L^2(G)$ onde G é um grupo finito arbitrário. Veremos que esta operação torna $L^2(G)$ uma álgebra e estudaremos algumas de suas propriedades.

Definição 3.2.1 (Convolução)**.** *Seja G um grupo finito e sejam a e b funções de $L^2(G)$. A convolução de a por b é a função de $L^2(G)$ indicada por $a * b$ e definida por*

$$a * b(x) = \sum_{y \in G} a(xy^{-1}) b(y).$$

Perceba que a definição acima é a generalização imediata da convolução para funções de $L^2(\mathbb{Z}_n)$, que, por sua vez, foi definida em analogia com o caso contínuo.

A fórmula da convolução pode ser expressa de outras maneiras. Fazendo a mudança de variável $xy^{-1} = z$ (e portanto $y = z^{-1}x$), obtemos

$$a * b(x) = \sum_{z \in G} a(z) b(z^{-1}x).$$

Uma outra forma é

$$a * b(x) = \sum_{\substack{g, h \in G \\ gh = x}} a(g) b(h).$$

Definir por analogia, apesar de interessante, não é completamente satisfatório. Ainda mais quando o objeto sobre o qual se faz a analogia não faz parte do trabalho em questão. Por isso mostraremos como a convolução aparece de maneira muito simples do ponto de vista algébrico, por meio de coisas básicas, das quais já tratamos. Recorde que existe um isomorfismo muito simples entre os espaços vetoriais $L^2(G)$ e $\mathbb{C}G$, o qual leva a base canônica de $L^2(G)$ na base canônica de $\mathbb{C}G$, isto é, $\{\delta_g \ : \ g \in G\}$ é levada em G de maneira óbvia. Um outro lembrete é que $\mathbb{C}G$ é uma álgebra (a álgebra do grupo G) cujas propriedades tratamos no capítulo anterior. A convolução surge quando forçamos que este isomorfismo de espaços vetoriais seja um isomorfismo de álgebras. A próxima proposição descreve esta ideia de forma precisa.

Proposição 3.2.1. *Sejam V um $\mathbb{C}$-espaço vetorial, W um álgebra sobre $\mathbb{C}$ e $T : V \longrightarrow W$ um isomorfismo entre V e W como espaços vetoriais. Então, dados $v_1, v_2 \in V$, $v_1 * v_2 := T^{-1}(Tv_1 \cdot Tv_2)$ define uma operação sobre V, a qual é respeitada por T. Consequentemente, $(V, *)$ é uma álgebra e T é um isomorfismo de álgebras.*

Demonstração: Claramente, a operação $*$ é bem definida e $T(v_1 * v_2) = Tv_1 \cdot Tv_2$ para todos v_1, $v_2 \in V$. Falta provar que $(V, *)$ é uma álgebra, o que também é simples. Comecemos com a associatividade.

$$\begin{aligned} v_1 * (v_2 * v_3) &= T^{-1}(Tv_1 \cdot T(v_2 * v_3)) \\ &= T^{-1}(Tv_1 \cdot (Tv_2 \cdot Tv_3)) \\ &= T^{-1}((Tv_1 \cdot Tv_2) \cdot Tv_3) \\ &= T^{-1}(T(v_1 * v_2) \cdot Tv_3) \\ &= (v_1 * v_2) * v_3. \end{aligned}$$

Vejamos agora a distributividade à esquerda (a distributividade à direita é completamente análoga)

$$\begin{aligned} v_1 * (v_2 + v_3) &= T^{-1}(Tv_1 \cdot T(v_2 + v_3)) \\ &= T^{-1}(Tv_1 \cdot Tv_2 + Tv_1 \cdot Tv_3) \\ &= T^{-1}(Tv_1 \cdot Tv_2) + T^{-1}(Tv_1 \cdot Tv_3) \\ &= v_1 * v_2 + v_1 * v_3. \end{aligned}$$

E finalmente vejamos a compatibilidade da operação $*$ com a multiplicação por escalar.

$$\begin{aligned} \lambda(v_1 * v_2) &= \lambda T^{-1}(Tv_1 \cdot Tv_2) \\ &= T^{-1}(\lambda(Tv_1 \cdot Tv_2)) \\ &= T^{-1}((\lambda Tv_1) \cdot Tv_2) \\ &= T^{-1}(T\lambda v_1 \cdot Tv_2) \\ &= (\lambda v_1) * v_2). \end{aligned}$$

Similarmente, prova-se que $\lambda(v_1 * v_2) = v_1 * (\lambda v_2)$. □

Corolário 3.2.1. *A convolução é a operação induzida em $L^2(G)$ quando forçamos, no sentido preciso da proposição anterior, que o isomorfismo de espaços vetoriais*

$$\begin{aligned} T : L^2(G) &\longrightarrow \mathbb{C}G \\ \delta_g &\longmapsto g \end{aligned}$$

seja um isormorfismo de álgebras.

Demonstração: Seja $*$ a operação induzida em $L^2(G)$ segundo a proposição anterior.

$$\begin{aligned} a * b &= T^{-1}(Ta \cdot Tb) \\ &= T^{-1}\left(\left(\sum_{g\in G} a(g)g\right) \cdot \left(\sum_{h\in G} b(h)h\right)\right) \\ &= T^{-1}\left(\sum_{g\in G}\sum_{h\in G} a(g)b(h)gh\right) \\ &= T^{-1}\left(\sum_{g\in G} a(g)\sum_{h\in G} b(h)gh\right) \end{aligned}$$

Fazendo a mudança de variável $gh = x$ ($\therefore h = g^{-1}x$), obtemos $\sum\limits_{h\in G} b(h)gh = \sum\limits_{x\in G} b(g^{-1}x)x$ e portanto

$$\begin{aligned} a * b &= T^{-1}\left(\sum_{g\in G} a(g)\sum_{x\in G} b(g^{-1}x)x\right) \\ &= T^{-1}\left(\sum_{g\in G}\sum_{x\in G} a(g)b(g^{-1}x)x\right) \\ &= T^{-1}\left(\sum_{x\in G}\left(\sum_{g\in G} a(g)b(g^{-1}x)\right)x\right) \\ &= \sum_{x\in G}\left(\sum_{g\in G} a(g)b(g^{-1}x)\right)\delta_x \end{aligned}$$

ou seja, $a * b(x) = \sum\limits_{g\in G} a(g)b(g^{-1}x)$, que é precisamente a convolução da definição 3.2.1. □

Corolário 3.2.2. *O espaço $L^2(G)$ munido com o produto convolução é uma álgebra cuja identidade é a função δ_{1_G}.*

Demonstração: Segue imediatamente da proposição 3.2.1 que $L^2(G)$ é uma álgebra. Para ver que δ_{1_G} é a identidade, seja $a \in L^2(G)$.

$$\begin{aligned} \delta_{1_G} * a &= T^{-1}(T(\delta_{1_G}) \cdot Ta) \\ &= T^{-1}(1_G \cdot Ta) \\ &= T^{-1}(Ta) \\ &= a. \end{aligned}$$

Similarmente, prova-se que $a * \delta_{1_G} = a$. □

Corolário 3.2.3. *Dados $g, h \in G$, tem-se $\delta_g * \delta_h = \delta_{gh}$.*

Demonstração: $\delta_g * \delta_h = T^{-1}(T\delta_g \cdot T\delta_h) = T^{-1}(gh) = \delta_{gh}$. □

Corolário 3.2.4. *A álgebra $L^2(G)$ é comutativa se, e somente se, o grupo G é abeliano.*

Demonstração: Como $L^2(G)$ e $\mathbb{C}G$ são álgebras isomorfas, uma será comutativa se, e somente se, o mesmo ocorrer com a outra. Como $\mathbb{C}G$ é comutativa se, e somente se, G é abeliano (veja o capítulo anterior) o resultado segue. □

Proposição 3.2.2. *Sejam $f \in L^2(G)$, $x \in G$ e $g \in G$. Então*

1. $(f * \delta_g)(x) = f(xg^{-1})$.
2. $(\delta_g * f)(x) = f(g^{-1}x)$.

Demonstração: 1. $(f * \delta_g)(x) = \sum_{y \in G} f(xy^{-1})\delta_g(y) = f(xg^{-1})$.

2. $(\delta_g * f)(x) = \sum_{z \in G} \delta_g(z) f(z^{-1}x) = f(g^{-1}x)$.

□

Recordemos que o centro de um anel R é o conjunto $Z(R) = \{a \in R \ : \ ar = ra, \text{ para todo } r \in R\}$. É fácil verificar que $Z(R)$ é um subanel de R. Já o centro de uma álgebra é uma subálgebra. O centro da álgebra das matrizes quadradas de ordem n e com entradas em $\mathbb{C}$ é a subálgebra $\{\lambda I \ : \ \lambda \in \mathbb{C}\}$ onde I é a matriz identidade. Este resultado será importante quando estudarmos a transformada de Fourier sobre um grupo não necessariamente abeliano, por isso vamos demonstrá-lo e, em seguida, provaremos que o centro da álgebra $L^2(G)$ é o subespaço (agora subálgebra) das funções de classe.

Proposição 3.2.3. $Z(M_n(\mathbb{C})) = \{\lambda I \ : \ \lambda \in \mathbb{C}\}$.

Demonstração: Seja $\varphi : G \longrightarrow GL_n(\mathbb{C})$ uma representação matricial de grau n de um grupo G. O espaço dos morfismos de φ em φ, $\mathrm{Hom}_G(\varphi, \varphi)$, pode ser interpretado como o conjunto das matrizes $n \times n$ que comutam com $\varphi(g)$, para todo $g \in G$, isto é, $A \in \mathrm{Hom}_G(\varphi, \varphi) \Leftrightarrow A\varphi(g) = \varphi(g)A$, para todo $g \in G$. Consequentemente $Z(M_n(\mathbb{C})) \subset \mathrm{Hom}_G(\varphi, \varphi)$. Se adicionalmente supusermos que φ é irredutível, o lema de Schur garantirá que $\mathrm{Hom}_G(\varphi, \varphi) = \{\lambda I \ : \ \lambda \in \mathbb{C}\}$. Portanto $Z(M_n(\mathbb{C})) \subset \mathrm{Hom}_G(\varphi, \varphi) = \{\lambda I \ : \ \lambda \in \mathbb{C}\} \subset Z(M_n(\mathbb{C}))$. Assim, a demonstração estará completa se pudermos exibir uma representação $\varphi : G \longrightarrow GL_n(\mathbb{C})$ irredutível. Basta tomar $G = GL_n(\mathbb{C})$ e φ o homomorfismo identidade. A fim de provar que esta representação é irredutível, seja W um subespaço G-invariante de $\mathbb{C}^n$. Então W é invariante por todos os operadores da forma φ_A com $A \in G$, ou seja,

W é invariante por todos os operadores invertíveis de $\mathbb{C}^n$. Se $W \neq \{0\}$ e $W \neq \mathbb{C}^n$, é fácil exibir um operador invertível tal que W não seja invariante por ele. Logo $W = \{0\}$ ou $W = \mathbb{C}^n$. □

Proposição 3.2.4. *$Z(L^2(G)) = Class(L^2(G))$.*

Demonstração: Recorde que uma função de classe de $L^2(G)$ é aquela que é constante nas classes de conjugação de G, ou equivalentemente, $f \in \text{Class}(L^2(G))$ se $f(gh) = f(hg)$ para todos $g, h \in G$.

Sejam $f \in \text{Class}(L^2(G))$ e $a \in L^2(G)$.

$$\begin{aligned} f * a(x) &= \sum_{y \in G} f(xy^{-1})a(y) \\ &= \sum_{y \in G} a(y)f(xy^{-1}) \\ &= \sum_{y \in G} a(y)f(y^{-1}x) \\ &= a * f(x). \end{aligned}$$

Assim $f * a = a * f$ e consequentemente $\text{Class}(L^2(G)) \subset Z(L^2(G))$. Reciprocamente, sejam $f \in Z(L^2(G))$, $g \in G$ e $h \in G$. Então $f * \delta_{g^{-1}}(h) = \delta_{g^{-1}} * f(h)$, ou seja, $f(hg) = f(gh)$. Dessa forma obtemos a outra inclusão. □

Corolário 3.2.5. *A convolução de funções de classe ainda é uma função de classe.*

Demonstração: Evidente. □

3.3 Análise de Fourier em Grupos Abelianos Finitos

Nesta seção, vamos considerar o caso em que o grupo finito G é abeliano. Esta é uma situação bem mais simples que o caso geral, que trataremos posteriormente, porém é suficiente para várias aplicações. Podemos citar, por exemplo, aplicações em processamento de sinais e em teoria dos números (o leitor pode consultar, por exemplo, (TERRAS, 1999)). Na próxima seção faremos uma aplicação em teoria dos grafos, ou mais precisamente, na teoria espectral dos grafos e uma pequena aplicação às matrizes circulantes.

Como vimos no Corolário 3.2.4, $L^2(G)$ é uma álgebra comutativa (uma outra forma de ver isto é usando que $Z(L^2(G)) = \text{Class}(L^2(G))$; fica fácil provar que $\text{Class}(L^2(G)) = L^2(G) \Leftrightarrow G$ é abeliano). Estamos interessados em estudar a estrutura de $L^2(G)$ identificando-a com uma álgebra mais familiar. Com este propósito definiremos a transformada de Fourier sobre G.

No início do capítulo definimos a transformada de Fourier de uma função $f \in L^2(\mathbb{Z}_n)$ como a função $\widehat{f} \in L^2(\mathbb{Z}_n)$ definida por $\widehat{f}([m]) = n\langle f, \chi_m \rangle$. Esta definição induz o operador

$$\begin{array}{rcl} T : L^2(\mathbb{Z}_n) & \longrightarrow & L^2(\mathbb{Z}_n) \\ f & \longmapsto & \widehat{f} \end{array}$$

o qual chamaremos de transformada de Fourier sobre o grupo abeliano $\mathbb{Z}_n$, que leva a base $\{\chi_0, ..., \chi_{n-1}\}$ de caráteres irredutíveis de $\mathbb{Z}_n$ na base $\{n\delta_{[0]}, ..., n\delta_{[n-1]}\}$ de maneira óbvia: $\chi_j \longmapsto n\delta_{[j]}$. Se tentarmos proceder de maneira idêntica para um grupo abeliano G, isto é, definir a transformada de Fourier sobre G como o operador que leva a base de caráteres irredutíveis de G, $\{\chi : G \longrightarrow \mathbb{C}^* \ : \ \chi \text{ é homomorfismo}\}$, na base $\{|G|\delta_g \ : \ g \in G\}$, encontraremos uma dificuldade: no caso $\mathbb{Z}_n$ tínhamos a correspodência natural $[m] \longmapsto \chi_m$, enquanto que para G não temos nenhuma correspondência a priori. Dito de outra forma, existem muitas maneiras de levar a base (não ordenada) $\{\chi : G \longrightarrow \mathbb{C}^* \ : \ \chi \text{ é homomorfismo}\}$ na base (não ordenada) $\{|G|\delta_g \ : \ g \in G\}$. Como escolher uma? Começaremos a contornar este problema com a seguinte definição:

Definição 3.3.1 (Grupo dual)**.** *Seja G um grupo abeliano finito. Indicamos por $\widehat{G}$ o conjunto dos caráteres irredutíveis de G e dizemos que $\widehat{G}$ é o grupo dual de G.*

Como o nome sugere, vamos provar que $\widehat{G}$ é um grupo. Lembre-se que $\widehat{G}$ é base ortonormal para $\text{Class}\,(L^2(G))$ e, portanto, para $L^2(G)$ já que G é abeliano.

Proposição 3.3.1. *Seja G um grupo abeliano finito. Então $\widehat{G}$ munido da operação produto ponto-a-ponto de funções, ou seja, $(\chi \cdot \theta)(g) = \chi(g)\theta(g)$ para $\chi,\ \theta \in \widehat{G}$, é um grupo de ordem $|G|$.*

Demonstração: Dados χ e θ, é fácil provar que $\chi \cdot \theta$ e $\overline{\chi}$, que é o inverso de χ, são homomorfismos. Isto é suficiente para para que mostrar que $\widehat{G}$ é um grupo, mas, para os detalhes, o leitor pode consultar (STEINBERG, 2011) na página 55.

□

Exemplo 3.3.1. *Seja $G = \mathbb{Z}_n$. Então $\widehat{G} = \{\chi_0, ..., \chi_{n-1}\}$ onde $\chi_k([m]) = e^{\frac{2\pi ikm}{n}}$. É fácil verificar que a correspondência $[k] \longmapsto \chi_k$ é um isomorfismo entre os grupos G e $\widehat{G}$.*

A correspondência acima é bem natural porque ela é o isomorfismo entre os grupos cíclicos $\mathbb{Z}_n$ e $\widehat{\mathbb{Z}}_n$ (é facil ver que $\widehat{\mathbb{Z}}_n$ é cíclico e gerado por χ_1) que leva [1] em χ_1, os quais são os geradores mais simples de $\mathbb{Z}_n$ e $\widehat{\mathbb{Z}}_n$ respectivamente. Apesar de não termos uma correspondência imediata entre G e $\widehat{G}$ quando G é um grupo abeliano finito qualquer, uma pergunta interessante é se G e $\widehat{G}$ são isomorfos. A resposta é afirmitiva e a demonstração é relativamente simples: prova-se primeiro para grupos cíclicos e depois é só usar o fato que todo grupo abeliano é produto direto de grupos cíclicos, entretanto não faremos os

detalhes aqui. Vamos agora definir a transformada de Fourier sobre G. Veja que agora podemos considerar o espaço vetorial $L^2(\widehat{G})$ no contra-domínio da transformada em vez de $L^2(G)$ e usar a correspondência natural entre as bases $\widehat{G}$ e $\{\delta_\chi \ : \ \chi \in \widehat{G}\}$. Observamos ainda que, apesar da notação, não consideraremos o produto convolução em $L^2(\widehat{G})$.

Definição 3.3.2 (Transformada de Fourier)**.** *Seja $f : G \longrightarrow \mathbb{C}$ uma função complexa definida sobre um grupo finito e abeliano G. Então a transformada de Fourier de f é a função $\widehat{f} : \widehat{G} \longrightarrow \mathbb{C}$ definida por $\widehat{f}(\chi) = |G|\langle f, \chi\rangle = \sum_{g\in G} f(g)\overline{\chi(g)}$. Os números complexos $|G|\langle f, \chi\rangle$ são chamados de coeficientes de Fourier de f.*

A definição acima induz uma aplicação $T : L^2(G) \longrightarrow L^2(\widehat{G})$, que leva $f \in L^2(G)$ em $\widehat{f} \in L^2(\widehat{G})$, chamada transformada de Fourier sobre o grupo abeliano G. Veremos que esta aplicação é um isomorfismo entre $L^2(G)$ e $L^2(\widehat{G})$ como espaços vetoriais e, posteriormente, que é um isomorfismo de álgebras. Para isto, como já dissemos, não consideraremos $L^2(\widehat{G})$ uma álgebra com o produto convolução. Se lembrarmos do caso contínuo, onde $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$, suspeitaremos que o produto que devemos considerar em $L^2(\widehat{G})$ é a multiplicação ponto-a-ponto de funções (a demonstração de que, com este produto, $L^2(\widehat{G})$ é uma álgebra é simples, por isso será omitida). Mostraremos que este é o caso de fato.

Uma última observação é que, como definimos no início do capítulo a transformada de Fourier sobre $\mathbb{Z}_n$ como um operador de $L^2(\mathbb{Z}_n)$, temos uma ambiguidade: dada $f \in L^2(\mathbb{Z}_n)$, na definição anterior tínhamos $\widehat{f} \in L^2(\mathbb{Z}_n)$ e na definição atual temos $\widehat{f} \in L^2(\widehat{\mathbb{Z}_n})$. Isto não é um problema, pois denotando por $\widetilde{f}$ a transformada de Fourier de f na definição antiga e sendo $\alpha : \mathbb{Z}_n \longrightarrow \widehat{\mathbb{Z}_n}$ o isomorfismo dado por $\alpha([k]) = \chi_k$, vemos que $\widetilde{f} = \widehat{f} \circ \alpha$ e, como isso, todas as propriedades que provarmos que $\widehat{f}$ possui, passam para $\widetilde{f}$ e vice-versa. Mostraremos, por exemplo, que $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$. A partir disto obtemos facilmente que $\widetilde{f * g} = \widetilde{f} \cdot \widetilde{g}$:

$$\begin{aligned}
\widetilde{f * g} &= \widehat{f * g} \circ \alpha \\
&= \left(\widehat{f} \cdot \widehat{g}\right) \circ \alpha \\
&= \left(\widehat{f} \circ \alpha\right) \cdot (\widehat{g} \circ \alpha) \\
&= \widetilde{f} \cdot \widetilde{g}.
\end{aligned}$$

Para os próximos resultados desta seção, estaremos sempre supondo que G é um grupo abeliano de ordem n.

Proposição 3.3.2 (Fórmula de inversão)**.** *Se $f \in L^2(G)$, então $f = \dfrac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi$.*

Demonstração: $f = \sum_{\chi\in\widehat{G}} \langle f, \chi\rangle\chi = \sum_{\chi\in\widehat{G}} \dfrac{\widehat{f}(\chi)}{|G|}\chi = \dfrac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi.$ □

Proposição 3.3.3. *A transformada de Fourier sobre o grupo abeliano G,*

$$\begin{array}{rcl} T : L^2(G) & \longrightarrow & L^2(\widehat{G}) \\ f & \longmapsto & \widehat{f} \end{array},$$

leva a base $\widehat{G} = \{\chi_1, ..., \chi_n\}$ de $L^2(G)$ na base $\{n\delta_{\chi_1}, ..., n\delta_{\chi_n}\}$, isto é, $\widehat{\chi}_j = n\delta_{\chi_j}$.

Demonstração: Dados $\chi, \theta \in \widehat{G}$, $\widehat{\chi}(\theta) = n\langle \chi, \theta \rangle$. Portanto $\widehat{\chi} = n\delta_\chi$. □

Corolário 3.3.1.

$$\begin{array}{rcl} T : L^2(G) & \longrightarrow & L^2(\widehat{G}) \\ f & \longmapsto & \widehat{f} \end{array}$$

é um isomorfismo entre $L^2(G)$ e $L^2(\widehat{G})$ como espaços vetoriais.

Demonstração: Seja $S : L^2(G) \longrightarrow L^2(\widehat{G})$ o isomorfismo que leva a base $\{\chi_1, ..., \chi_n\}$ na base $\{n\delta_{\chi_1}, ..., n\delta_{\chi_n}\}$. Dado $f \in L^2(G)$, temos $Sf = S\left(\sum_{j=1} \langle f, \chi_j \rangle \chi_j\right) = \sum_{j=1}^{n} \langle f, \chi_j \rangle n\delta_{\chi_j}$, ou seja, $(Sf)(\chi_j) = n\langle f, \chi_j \rangle = \widehat{f}(\chi_j) = (Tf)(\chi_j)$ para todo $j \in \{1, ...n\}$. Portanto $T = S$. □

A notação $\widehat{G}$ e o termo grupo dual introduzidos na Definição 3.3.1 fazem referência a um produto, que é a multiplicação ponto-a-ponto de funções. Entretanto quando pensamos em $\widehat{G}$ como base de $L^2(G)$, em particular como subconjunto de $L^2(G)$, é claro que o produto que devemos considerar entre seus elementos é a convolução. Isto pode causar alguma confusão, por isso e por outro motivo que veremos adiante, sempre que estivermos considerando $\widehat{G}$ como base de $L^2(G)$, o chamaremos de base de Fourier sobre o grupo abeliano G.

Tendo em vista a discussão acima e os dois últimos resultados, podemos dizer que a transformada de Fourier é o isomorfismo de espaços vetoriais que leva a base de Fourier, $\widehat{G} = \{\chi_1, ..., \chi_n\}$, a qual é estreitamente relacionada com a estrutura do grupo G e que possui toda uma teoria subjacente (ver capítulo anterior) na base $\{n\delta_{\chi_1}, ..., n\delta_{\chi_n}\}$ que, por sua vez, é, a menos de multiplicação pelo escalar n, a base mais simples possível de $L^2(\widehat{G})$. Esta é uma das propriedades que distingue a transformada de Fourier de um isomorfismo qualquer e, ao mesmo tempo, é uma motivação algébrica para defini-la: Ora, qual isomorfismo entre $L^2(G)$ e $L^2(\widehat{G})$ seria mais natural para estudar a estrutura de $L^2(G)$ que o que leva a base de Fourier na base canônica $\{\delta_{\chi_1}, ..., \delta_{\chi_n}\}$? É verdade que a imagem da base de Fourier pela transformada é $\{n\delta_{\chi_1}, ..., n\delta_{\chi_n}\}$ e não $\{\delta_{\chi_1}, ..., \delta_{\chi_n}\}$, mas o escalar n é apenas um ajuste para que a transformada tenha sua propriedade mais importante que é ser um isomorfismo de álgebras. Provaremos isto logo mais.

Proposição 3.3.4. *A transformada de Fourier sobre o grupo abeliano G leva a base $\{\delta_g \ : \ g \in G\}$ de $L^2(G)$ na base $\{\widehat{\delta}_g \ : \ g \in G\}$, onde $\widehat{\delta}_g(\chi) = \overline{\chi(g)}$, ou seja, $\widehat{\delta}_g = \sum_{\chi \in \widehat{G}} \overline{\chi(g)}\delta_\chi$.*

Demonstração: É óbvio que $\{\widehat{\delta}_g \ : \ g \in G\}$ é um base. Agora, $\widehat{\delta}_g(\chi) = n\langle \delta_g, \chi\rangle = \sum\limits_{x\in G} \delta_g(x)\overline{\chi(x)} = \overline{\chi(g)}$. □

Finalmente vamos demonstrar que a transformada de Fourier é um isomorfismo entre as álgebras $L^2(G)$ e $L^2(\widehat{G})$ (esta com o produto ponto-a-ponto de funções). Daremos duas demonstrações. A primeira consta na nossa referência principal, (STEINBERG, 2011), já a segunda é uma simplificação nossa, mas que precisará do seguinte fato: Sejam V e W álgebras sobre $\mathbb{C}$, $T : V \longrightarrow W$ uma aplicação linear e $\{e_1, ..., e_n\}$ uma base de V. Se $T(e_i \cdot e_j) = Te_i \cdot Te_j$ para todos i e j, então $T(u \cdot v) = Tu \cdot Tv$ para todos $u, v \in V$. De fato, dados $u, v \in V$, $u = \sum\limits_{i=1}^{n} \alpha_i e_i$ e $v = \sum\limits_{j=1}^{n} \beta_j e_j$,

$$\begin{aligned}
T(u \cdot v) &= T\left(\left(\sum_{i=1}^{n}\alpha_i e_i\right) \cdot \left(\sum_{j=1}^{n}\beta_j e_j\right)\right) \\
&= T\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\beta_j e_i \cdot e_j\right) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\beta_j T\left(e_i \cdot e_j\right) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\beta_j T(e_i) \cdot T(e_j) \\
&= \left(\sum_{i=1}^{n}\alpha_i T(e_i)\right) \cdot \left(\sum_{j=1}^{n}\beta_j T(e_j)\right) \\
&= T\left(\sum_{i=1}^{n}\alpha_i e_i\right) \cdot T\left(\sum_{j=1}^{n}\beta_j e_j\right) \\
&= T\left(u\right) \cdot T\left(v\right)
\end{aligned}$$

Teorema 3.3.1. *Dados $a, b \in L^2(G)$, tem-se $\widehat{a * b} = \widehat{a} \cdot \widehat{b}$.*

Demonstração 1: Dado $\chi \in \widehat{G}$, temos:

$$\begin{aligned}
\widehat{a * b}(\chi) &= n\langle a * b, \chi\rangle \\
&= \sum_{x\in G} a * b(x)\overline{\chi(x)} \\
&= \sum_{x\in G}\left(\sum_{y\in G} a(xy^{-1})b(y)\right)\overline{\chi(x)} \\
&= \sum_{x\in G}\sum_{y\in G} a(xy^{-1})b(y)\overline{\chi(x)} \\
&= \sum_{y\in G} b(y)\sum_{x\in G} a(xy^{-1})\overline{\chi(x)}
\end{aligned}$$

Fazendo $xy^{-1} = z$ (portanto $x = zy$) obtemos

$$\sum_{x\in G} a(xy^{-1})\overline{\chi(x)} = \sum_{z\in G} a(z)\overline{\chi(zy)} = \sum_{z\in G} a(z)\overline{\chi(z)\chi(y)}.$$

Portanto:

$$\begin{aligned}
\widehat{a*b}(\chi) &= \sum_{y\in G} b(y)\sum_{z\in G} a(z)\overline{\chi(z)\chi(y)} \\
&= \sum_{y\in G}\sum_{z\in G} a(z)\overline{\chi(z)}b(y)\overline{\chi(y)} \\
&= \left(\sum_{z\in G} a(z)\overline{\chi(z)}\right)\left(\sum_{y\in G} b(y)\overline{\chi(y)}\right) \\
&= \widehat{a}(\chi)\widehat{b}(\chi)
\end{aligned}$$

Logo $\widehat{a*b} = \widehat{a}\cdot\widehat{b}$. □

Demonstração 2: Dados $g, h \in G$ e $\chi \in \widehat{G}$, temos $\widehat{\delta_g * \delta_h}(\chi) = \widehat{\delta_{gh}}(\chi) = \overline{\chi(gh)} = \overline{\chi(g)\chi(h)} = \widehat{\delta}_g(\chi)\widehat{\delta}_h(\chi) = \left(\widehat{\delta}_g \cdot \widehat{\delta}_h\right)(\chi)$. Portanto $\widehat{\delta_g * \delta_h} = \widehat{\delta}_g \cdot \widehat{\delta}_h$. Pela observação feita antes deste teorema, $\widehat{a*b} = \widehat{a} * \widehat{b}$ para todos $a, b \in L^2(G)$. □

Na próxima proposição veremos se a transformada de Fourier respeita o produto hermitiano, que é a estrutura de $L^2(G)$ que resta para analisarmos.

Proposição 3.3.5 (Fórmula de Plancherel)**.** *Dados $a, b \in L^2(G)$, tem-se $\langle a, b\rangle = \frac{1}{n}\langle \widehat{a}, \widehat{b}\rangle$, ou seja, se trocarmos o produto hermitiano de $L^2(\widehat{G})$ por $\langle\cdot,\cdot\rangle' = \frac{1}{n}\langle\cdot,\cdot\rangle$, então a transformada de Fourier é uma isometria* (*ou transformação linear unitária*)*.*

Demonstração 1: Vamos simplesmente desenvolver o lado direito da igualdade:

$$\begin{aligned}
\frac{1}{n}\langle \widehat{a}, \widehat{b}\rangle &= \frac{1}{n^2}\sum_{\chi\in\widehat{G}} \widehat{a}(\chi)\overline{\widehat{b}(\chi)} \\
&= \frac{1}{n^2}\sum_{\chi\in\widehat{G}} \left(\sum_{g\in G} a(g)\overline{\chi(g)}\right)\overline{\left(\sum_{h\in G} b(h)\overline{\chi(h)}\right)} \\
&= \frac{1}{n^2}\sum_{\chi\in\widehat{G}}\sum_{g\in G}\sum_{h\in G} a(g)\overline{b(h)}\chi(h)\overline{\chi(g)} \\
&= \frac{1}{n^2}\sum_{g\in G}\sum_{h\in G} a(g)\overline{b(h)}\sum_{\chi\in\widehat{G}}\chi(h)\overline{\chi(g)}.
\end{aligned}$$

Como G é abeliano, as segundas relações de ortogonalidade para caráteres (teorema 2.6.6) dizem que $\sum_{\chi\in\widehat{G}}\chi(h)\overline{\chi(g)}=0$ se $h\neq g$, e $\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(g)}=n$. Assim:

$$\begin{aligned}\frac{1}{n}\langle\widehat{a},\widehat{b}\rangle &= \frac{1}{n^2}\sum_{g\in G}a(g)\overline{b(g)}n\\ &= \frac{1}{n}\sum_{g\in G}a(g)\overline{b(g)}\\ &= \langle a,b\rangle.\end{aligned}$$

□

Demonstração 2: Verificaremos a fórmula apenas para os elementos da base de Fourier. Sejam $\chi,\theta\in\widehat{G}$.

$$\frac{1}{n}\langle\widehat{\chi},\widehat{\theta}\rangle=\frac{1}{n}\langle n\delta_\chi,n\delta_\theta\rangle=n\langle\delta_\chi,\delta_\theta\rangle=\sum_{\chi'\in\widehat{G}}\delta_\chi(\chi')\overline{\delta_\theta(\chi')}=\begin{cases}0 \text{ se } \chi\neq\theta,\\ 1 \text{ se } \chi=\theta.\end{cases}$$

Portanto $\frac{1}{n}\langle\widehat{\chi},\widehat{\theta}\rangle=\langle\chi,\theta\rangle$. Podemos concluir que a fórmula vale para $a,b\in L^2(G)$, escrevendo-os na base de Fourier e usando as propriedades do produto hermitiano. Ou podemos considerar o produto hermitiano $\langle\cdot,\cdot\rangle'$ e concluir que a transformada de Fourier é unitária porque ela leva uma base ortonormal (a base de Fourier) em um conjunto ortonormal. □

Assim como fizemos nos dois últimos resultados, apresentaremos mais de uma demonstração para as próximas proposições. Nosso objetivo é ilustrar a utilidade da transformada de Fourier. Começaremos investigando o comportamento da base de Fourier com respeito a convolução.

Proposição 3.3.6. *Sejam $\chi,\theta\in\widehat{G}$. Então $\chi*\theta=0$ se $\chi\neq\theta$, e $\chi*\chi=n\chi$.*

Demonstração 1: Fazendo uma computação direta, obtemos:

$$\begin{aligned}\chi*\theta(x) &= \sum_{y\in G}\chi(xy^{-1})\theta(y)\\ &= \sum_{z\in G}\chi(z)\theta(z^{-1}x)\\ &= \sum_{z\in G}\chi(z)\theta(z^{-1})\theta(x)\\ &= \left(\sum_{z\in G}\chi(z)\overline{\theta(z)}\right)\theta(x)\\ &= n\langle\chi,\theta\rangle\theta(x).\end{aligned}$$

Se $\chi\neq\theta$, obtemos $\chi*\theta(x)=0\ \forall\ x\in G$. Logo, $\chi*\theta=0$. Já $\chi*\chi(x)=n\chi(x)=(n\chi)(x)$. Portanto $\chi*\chi=n\chi$. □

Demonstração 2: $\chi * \theta = T^{-1}(T(\chi * \theta)) = T^{-1}(T\chi \cdot T\theta) = T^{-1}(n\delta_\chi \cdot n\delta_\theta) = nT^{-1}(n\delta_\chi \cdot \delta_\theta)$. É imediato que $\delta_\chi \cdot \delta_\theta = 0$ caso $\chi \neq \theta$, e que $\delta_\chi \cdot \delta_\chi = \delta_\chi$. Assim $\chi * \theta = T^{-1}(0) = 0$ se $\chi \neq \theta$, e $\chi * \chi = nT^{-1}(n\delta_\chi) = n\chi$. □

Se V é uma álgebra, então existem operadores lineares muito especiais definidos em V, que são os operadores obtidos via multiplicação por uma constante fixa. Em muitos contextos tais operadores são importantíssimos. No nosso caso não será diferente. Estes operadores serão úteis na aplicação que faremos na teoria dos grafos, mas para isso precisaremos da próxima proposição.

Proposição 3.3.7. *Seja $a \in L^2(G)$. Consideremos o operador convolução por a, isto é, a aplicação $A : L^2(G) \longrightarrow L^2(G)$ definida por $A(b) = a * b$. Então A é linear e χ é autovetor de A com autovalor $\widehat{a}(\chi)$ para todo $\chi \in \widehat{G}$. Consequentemente A é diagonalizável e a base de Fourier é base ortonormal de autovetores.*

Demonstração 1: A linearidade de A é uma consequência imediata das propriedades básicas da convolução. Dado $\chi \in \widehat{G}$, temos:

$$\begin{aligned}
A(\chi) &= a * \chi \\
&= \sum_{x \in G} (a * \chi)(x)\delta_x \\
&= \sum_{x \in G} \left(\sum_{y \in G} a(xy^{-1})\chi(y) \right) \delta_x \\
&= \sum_{x \in G} \left(\sum_{z \in G} a(z)\chi(z^{-1}x) \right) \delta_x \\
&= \sum_{x \in G} \sum_{z \in G} a(z)\chi(z^{-1})\chi(x)\delta_x \\
&= \sum_{z \in G} a(z)\overline{\chi(z)} \sum_{x \in G} \chi(x)\delta_x \\
&= n\langle a, \chi \rangle \chi \\
&= \widehat{a}(\chi)\chi
\end{aligned}$$

□

Demonstração 2: $A(\chi) = a * \chi = T^{-1}(T(a * \chi)) = T^{-1}(Ta \cdot T\chi) = T^{-1}(\widehat{a} \cdot n\delta_\chi)$. Nota-se imediatamente que $\widehat{a} \cdot n\delta_\chi = n\widehat{a}(\chi)\delta_\chi$, assim $A(\chi) = T^{-1}(n\widehat{a}(\chi)\delta_\chi) = \widehat{a}(\chi)T^{-1}(n\delta_\chi) = \widehat{a}(\chi)\chi$. □

Demonstração 3: Podemos usar proposição 3.3.6. Dado que $a = \sum_{\theta \in \widehat{G}} \langle a, \theta \rangle \theta$, temos que

$$A(\chi) = a * \chi = \left(\sum_{\theta \in \widehat{G}} \langle a, \theta \rangle \theta \right) * \chi = \sum_{\theta \in \widehat{G}} \langle a, \theta \rangle (\theta * \chi) = \langle a, \chi \rangle n\chi = \widehat{a}(\chi)\chi.$$

□

Observação 3.3.1. *O operador da proposição acima é hermitiano se, e somente se,* $a(g^{-1}) = \overline{a(g)}$ *para todo* $g \in G$*. Recorde que um operador é hermitiano se, e somente se, ele admite uma base ortonormal de autovetores e seus autovalores são reais. Supondo* A *hermitiano, temos* $\widehat{a}(\chi) \in \mathbb{R}$ *para todo* $\chi \in \widehat{G}$*. A fórmula de inversão diz que* $a = \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{a}(\chi)\chi$*. Então dado* $g \in G$

$$\begin{aligned} a(g^{-1}) &= \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{a}(\chi)\chi(g^{-1}) \\ &= \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{a}(\chi)\overline{\chi(g)} \\ &= \frac{1}{n}\sum_{\chi\in\widehat{G}} \overline{\widehat{a}(\chi)}\ \overline{\chi(g)} \\ &= \overline{\frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{a}(\chi)\chi(g)} \\ &= \overline{a(g)}. \end{aligned}$$

Suponhamos agora que $a(g^{-1}) = \overline{a(g)}$ *para todo* $g \in G$*. Uma vez que* A *possui base ortonormal de autovetores, resta-nos provar que seus autovalores são reais. Ora*

$$\begin{aligned} \widehat{a}(\chi) &= \sum_{g\in G} a(g)\overline{\chi(g)} \\ &= \sum_{g\in G} a(g)\chi(g^{-1}) \\ &= \sum_{g\in G} \overline{a(g^{-1})}\ \overline{\overline{\chi(g^{-1})}} \\ &= \overline{\sum_{g\in G} a(g^{-1})\overline{\chi(g^{-1})}} \\ &= \overline{\widehat{a}(\chi)}. \end{aligned}$$

Portanto $\widehat{a}(\chi) \in \mathbb{R}$ *para todo* $\chi \in \widehat{G}$*.*

3.4 Uma Aplicação à Teoria dos Grafos

Um grafo Γ é um par ordenado $\Gamma = (V, E)$ de conjuntos, onde V é finito e não-vazio e E é um conjunto formado por subconjuntos de dois elementos de V, ou seja, $E \subset \{\{x, y\} \ : \ x, y \in V \text{ e } x \neq y\}$. Os elementos de V são chamados vértices, enquanto que os elementos de E são ditos arestas. Um grafo cujo conjunto de vértices é unitário e o conjunto de arestas é vazio é chamado grafo trivial.

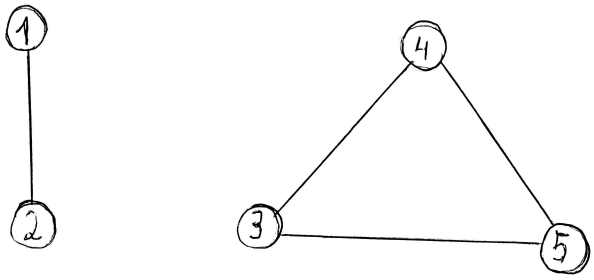

Figura 1: Grafo $\Gamma = (V, E)$ onde $V = \{1, 2, 3, 4, 5\}$ e $E = \{\{1, 2\}, \{3, 4\}, \{4.5\}, \{3, 5\}\}$.

Seja $\Gamma = (V, E)$ um grafo e sejam $x, y \in V$. Se $\{x, y\} \in E$ dizemos que x e y são adjacentes ou vizinhos. O grau de um vértice x é o número de vértices vizinhos a ele, o qual é indicado por $d(x)$.

Costuma-se representar um grafo desenhando pontos (ou círculos) que correspondem aos seus vértices, e segmentos entre os pontos que representam vértices adjacentes. Por exemplo, se $\Gamma = (V, E)$ onde $V = \{1, 2, 3, 4, 5\}$ e $E = \{\{1, 2\}, \{3, 4\}, \{4.5\}, \{3, 5\}\}$, então tal grafo pode ser representado como na figura 1 acima.

Uma sequência finita x_1, ..., x_k de vértices de um grafo $\Gamma = (V, E)$ é dita uma cadeia de x_1 a x_k quando $\{x_i, x_{i+1}\} \in E$ para todo $i \in \{1, ..., k-1\}$, isto é, quando os vértices consecutivos são adjacentes. Caso os vértices que compõem uma cadeia de x_1 a x_k sejam dois a dois distintos, tal cadeia será chamada de caminho de x_1 a x_k. E finalmente, o comprimento de uma cadeia $x_1, ..., x_k$ é o número (com repetição) de arestas que nela ocorre. Dito de forma mais precisa, o comprimento da cadeia $x_1, \ldots, x_k$ é $k - 1$.

Dizemos que um grafo Γ é conexo quando existe um caminho ligando qualquer par de seus vértices, ou seja, dados $x, y \in V$ existe um caminho de x e y. Caso contrário, dizemos que o grafo é desconexo. Note que o grafo da figura 1 é desconexo.

Definição 3.4.1 (Matriz de adjacência)**.** *Seja Γ um grafo no qual está fixada uma ordenação para o conjunto de vértices. Digamos $V = \{v_1, ..., v_n\}$. Então a matriz de adjacência $A = (a_{ij})$ é definida por*

$$a_{ij} = \begin{cases} 1 \text{ se } \{v_i, v_j\} \in E, \\ 0 \text{ caso contrário.} \end{cases}$$

Note que esta matriz depende da ordenação escolhida para o conjunto de vértices.

Sejam $\Gamma = (V, E)$ e A como na definição acima. Teceremos alguns comentários sobre as propriedades de A. Primeiramente, o grau de um vértice v_i é a soma da i-ésima linha ou da i-ésima coluna de A, isto é, $d(v_i) = \sum_{k=1}^{n} a_{ik} = \sum_{l=1}^{n} a_{li}$. Uma outra observação simples é que a matriz de adjacência é hermitiana, consequentemente é diagonalizável e seus autovalores são reais (aqui usamos o teorema espectral para matrizes). Definimos o

espectro do grafo Γ como o conjunto dos autovalores de A levando em conta suas respectivas multiplicidades algébricas. Esta definição não depende da ordenação escolhida para o conjunto de vértices. De fato, escolher outra ordenação para $V = \{v_1, ..., v_n\}$ corresponde a aplicar uma permutação nos índices, a qual se escreve como produto de transposições, ou seja, podemos inverter a posição de dois vértices de cada vez, uma quantidade finita de vezes para obter a nova ordenação. Não é difícil convencer-se que se invertermos as posições dos vértices v_i e v_j, a matriz de adjacência correspondente é obtida invertendo as posições das linhas $i - ésima$ e $j - ésima$ de A e, em seguida, as posições das colunas i-ésima e j-ésima. Em termos de produtos de matrizes, isto é o mesmo que multiplicar a direita e a esquerda da matriz A pela matriz T, isto é, TAT onde T é obtida invertendo as posições da $i - ésima$ e $j - ésima$ linhas da matriz identidade. Portanto, a matriz de adjacência relativa à nova ordenação é dada por $T_k.....T_1AT_1.....T_k$ e, como $T_jT_j = I$, ela é semelhante a A. Da álgebra linear, sabemos que os polinômios característicos são iguais, logo os autovalores e as respectivas multiplicidades também coincidem.

Pode-se obter muitas informações sobre um grafo a partir de seus autovalores, inclusive existe uma área de teoria dos grafos, a teoria espectral dos grafos, que dedica-se a este tipo de estudo. Para se ter uma ideia, recordemos que as potências de uma matriz diagonalizável são facilmente calculadas com auxílio de seus autovalores. Na próxima proposição veremos que as potências da matriz de adjacência fornecem uma informação interessante a cerca do grafo, portanto temos, pelo menos, uma aplicação indireta de seus autovalores.

Proposição 3.4.1. *Seja $\Gamma = (V, E)$ com $V = \{v_1, ..., v_n\}$ um grafo e seja A a respectiva matriz de adjacência. Então o número de cadeias de v_i a v_j com comprimento l é dado pela entrada ij da matriz A^l.*

Demonstração: Faremos indução em l. Suponhamos $l = 1$. O número de cadeias de v_i a v_j com comprimento 1 é 1 caso v_i e v_j sejam adjacentes, e 0 caso contrário. Isto é por definição a entrada de ij da matriz de adjacência.

Suponhamos agora que o resultado é válido para $l \geq 1$ e provemos que também vale para $l + 1$. Notemos que toda cadeia de comprimento $l + 1$ ligando v_i a v_j é da forma $v_i, ..., v_k, v_j$ onde $v_i, ..., v_k$ é uma cadeia de comprimento l ligando v_i a algum vértice v_k adjacente a v_j. Assim o número de tais cadeias é dado por

$$\sum_{k \in \{1,...,n\} \,:\, \{v_k, v_j\} \in E} (\mathcal{A}^l)_{ik} = \sum_{k=1}^{n} (\mathcal{A}^l)_{ik} \mathcal{A}_{kj} = (\mathcal{A}^{l+1})_{ij}$$

□

A aplicação da transformada de Fourier sobre grupos abelianos que faremos nesta seção, diz respeito ao cálculo dos autovalores de um tipo especial de grafo, o qual definiremos a seguir:

Definição 3.4.2 (Grafo de Cayley)**.** *Sejam G um grupo finito e X um subconjunto de G. X é dito simétrico se*

1. $1_G \notin X$;
2. $x \in X \Rightarrow x^{-1} \in X$.

Se X é um subconjunto simétrico de G, então o grafo de Cayley de G com respeito ao subconjunto simétrico X é o grafo cujo conjunto de vértices é G e o conjunto E de arestas é definido por: $\{g, h\} \in E$ se gh^{-1} (ou hg^{-1}) pertence a X.

Seja Γ o grafo de Cayley de um grupo finito G com respeito a um subconjunto simétrico X. Fazer o desenho de Γ é muito simples, pois fixado $g \in G$, $\{h, g\} \in E$ se, e somente se, $hg^{-1} \in X$ se, e somente se, existe $x \in X$ tal que $hg^{-1} = x$ se, e somente se, $h = xg$. Portanto, o conjunto de vértices de Γ adjacentes a g é $\{xg/x \in X\}$. Consequentemente os graus de todos os vértices do grafo de Cayley Γ são todos iguais ao número de elementos do subconjunto simétrico X, isto é, $d(g) =\mid X \mid$ para todo $g \in G$.

Proposição 3.4.2. *Um grafo de Cayley de um grupo finito G com respeito a um subconjunto simétrico X é conexo se, e somente se, o conjunto X gera G.*

Demonstração. Indiquemos por Γ tal grafo, suponhamos que X gera G e sejam $g, h \in G$. Como X, além de gerador, é simétrico, existem $x_1, \ldots x_k \in X$ tais que $gh^{-1} = x_k x_{k-1} ... x_1$, isto é, $g = x_k x_{k-1} ... x_1 h$. Pondo

$$\begin{aligned} z_1 &= x_1 h \\ z_2 &= x_2 z_1 = x_2 x_1 h \\ &\vdots \\ z_k &= x_k z_{k-1} = x_k x_{k-1} ... x_1 h = g \end{aligned}$$

$h, z_1, z_2, ..., z_{k-1}, g$ é claramente uma cadeia de h a g, da qual podemos extrair um caminho de h a g. Portanto Γ é conexo. Reciprocamente, suponhamos Γ conexo e seja $g \in G$. Pela conexidade de Γ, existe um caminho $g^{-1}, z_1, ..., z_k, 1_G$ ligando os vértices g^{-1} e 1_G. Consequentemente existem $x_1, ..., x_{k+1} \in X$ tais que

$$\begin{aligned} z_1 &= x_1 g^{-1} \\ z_2 &= x_2 z_1 = x_2 x_1 g^{-1} \\ &\vdots \\ z_k &= x_k z_{k-1} = x_k x_{k-1} ... x_2 x_1 g^{-1} \\ 1_G &= x_{k+1} z_k = z_{k+1} ... x_1 g^{-1} \end{aligned}$$

Portanto $g = x_{k+1}, ..., x_1$, o que mostra que X gera G. □

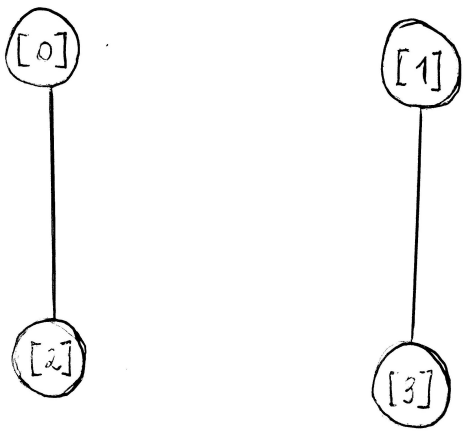

Figura 2: Grafo do exemplo 3.4.1.

Exemplo 3.4.1. *Sejam $G = \mathbb{Z}_4$ e $X = \{\pm[2]\} = \{[2]\}$ um subconjunto simétrico. Então a matriz de adjacência correspondente (segundo a ordenação $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$) é*

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

O desenho deste grafo pode ser visto acima, na figura 2. Perceba que, como esperado, já que $X = \{[2]\}$ não gera $\mathbb{Z}_4$, o grafo é desconexo.

Exemplo 3.4.2. *Sejam $G = \mathbb{Z}_6$ e $X = \{\pm[2], \pm[3]\} = \{[2], [3], [4]\}$ um subconjunto simétrico. Então o grafo de Cayley correspondente pode ser visto na Figura 3. A matriz de adjecência segundo a ordenação natural é*

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Por fim, daremos um exemplo em que o grupo finito G não é abeliano.

Exemplo 3.4.3. *Sejam $G = S_3 = \{1, a, a^2, b, ab, a^2b\}$ onde $a = (1\ 2\ 3)$ e $b = (1\ 2)$, e $X = \{a, a^2, b\}$ um subconjunto simétrico. Então o desenho do grafo de Cayley correspondente consta na figura 4. Já a matriz de adjecência segundo a ordenação proposta é*

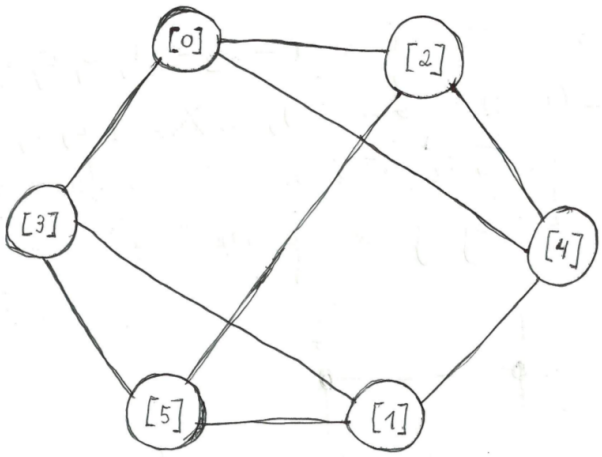

Figura 3: Grafo do exemplo 3.4.2.

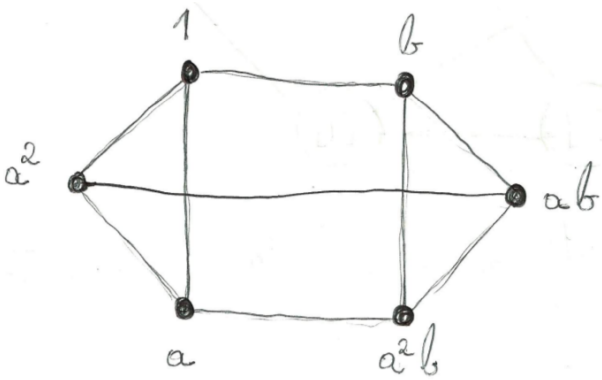

Figura 4: Grafo do exemplo 3.4.3.

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Definição 3.4.3 (Grafo circulante)**.** *Um grafo de Cayley de $\mathbb{Z}_n$ é dito grafo circuntante sobre n vértices.*

A razão do nome da acima é que a matriz de adjacência de um tal grafo é de um tipo especial, que definiremos a seguir.

Definição 3.4.4 (Matriz circulante)**.** *Uma matriz circulante de ordem n é uma matriz*

$n \times n$ da forma

$$\mathcal{A} = \begin{bmatrix} x_0 & x_1 & \cdots & x_{n-2} & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-3} & x_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2 & x_3 & \cdots & x_0 & x_1 \\ x_1 & x_2 & \cdots & x_{n-1} & x_0 \end{bmatrix}$$

Ou seja, as entradas de primeira linha são x_0, x_1, ..., x_{n-2}, x_{n-1}, fixados arbitrariamente, e as demais linhas são obtidas recursivamente por $\mathcal{A}_{i1} = \mathcal{A}_{(i-1)n}$ caso $i > 1$, e $\mathcal{A}_{ij} = \mathcal{A}_{(i-1)(j-1)}$ caso $i, j > 1$.

Proposição 3.4.3. *Uma matriz $\mathcal{A}$ é circulante de ordem n se, e somente se, existe uma única função $f \in L^2(\mathbb{Z}_n)$ tal que $\mathcal{A}_{ij} = f([j] - [i])$. Consequentemente, temos uma bijeção entre o conjunto das matrizes circulantes de ordem n e o conjunto $L^2(\mathbb{Z}_n)$.*

Demonstração: Seja $\mathcal{A}$ uma matriz circulante denotada como na definição anterior e seja $f \in L^2(\mathbb{Z}_n)$ definida por $f([k]) = x_k$ para todo $k \in \{0, ..., n-1\}$. Claramente $\mathcal{A}_{1j} = f([j] - [1])$ para todo $j \in \{1, ..., n\}$. Suponhamos que $\mathcal{A}_{ij} = f([j] - [i])$ para i fixo e para j variando de 1 a n, e provemos que o mesmo ocorre para $i + 1$.

De fato, $\mathcal{A}_{(i+1)1} = \mathcal{A}_{in} = f([n] - [i]) = f([1] - [i + 1])$. E para $j > 1$, $\mathcal{A}_{(i+1)j} = \mathcal{A}_{i(j-1)} = f([j - 1] - [i]) = f([j] - [i + 1])$.

Reciprocamente, seja $\mathcal{A}$ uma matriz definida por $\mathcal{A}_{ij} = f([j] - [i])$ onde $f \in L^2(\mathbb{Z}_n)$. A primeira linha de $\mathcal{A}$ é dada por $f([0])$, ..., $f([n-1])$. Seja $i > 1$. Então $\mathcal{A}_{i1} = f([1] - [i]) = f([n] - [i - 1]) = \mathcal{A}_{(i-1)n}$. E se $j > 1$, $\mathcal{A}_{ij} = f([j] - [i]) = f([j - 1] - [i - 1]) = \mathcal{A}_{(i-1)(j-1)}$. Portanto $\mathcal{A}$ é circulante de ordem n. □

Proposição 3.4.4. *A matriz de adjacência de um grafo de Cayley de $\mathbb{Z}_n$ segundo a ordenação natural, $\mathbb{Z}_n = \{[0], ..., [n-1]\}$, é a matriz circulante induzida pela função δ_X, onde X é o respectivo subconjunto simétrico.*

Demonstração: Sejam $\mathcal{A}$ a matriz de adjacência e $\mathcal{B}$ a matriz circulante correspondente a função δ_X. Temos que $\mathcal{A}_{ij} = 1 \Leftrightarrow \{[i-1], [j-1]\} \in E \Leftrightarrow [i-1] - [j-1] \in X \Leftrightarrow [j] - [i] \in X \Leftrightarrow \delta_X([j] - [i]) = 1 \Leftrightarrow \mathcal{B}_{ij} = 1$. Analogamente prova-se que $\mathcal{A}_{ij} = 0 \Leftrightarrow \mathcal{B}_{ij} = 0$. Como tanto $\mathcal{A}$ quanto $\mathcal{B}$ são matrizes cujas entradas são 0 ou 1, segue que $\mathcal{A} = \mathcal{B}$. □

Antes de calcularmos os autovalores do grafo de Cayley de um grupo abeliano, usaremos análise de Fourier sobre grupos abelianos para estudar algumas propriedades das matrizes circulantes. Começaremos provando que tais matrizes são diagonalizáveis e calculando seus autovalores.

Proposição 3.4.5. *Sejam $\mathcal{A}$ uma matriz circulante de ordem n e $g \in L^2(\mathbb{Z}_n)$ a função correspondente a $\mathcal{A}$, isto é, $\mathcal{A}_{ij} = g([j] - [i])$. Então A é diagonalizável e $\lambda_i = \widehat{f}(\chi_i)$ para*

$i = 0, ..., n-1$ são seus autovalores, onde $\{\chi_0, ..., \chi_{n-1}\}$ é a base de caráteres irredutíveis de $\mathbb{Z}_n$ e $f \in L^2(\mathbb{Z}_n)$ é dada por $f([k]) = g([-k])$ para todo k.

Demonstração: Seja

$$\begin{aligned} F : L^2(\mathbb{Z}_n) &\longrightarrow L^2(\mathbb{Z}_n) \\ a &\longmapsto f * a \end{aligned}$$

Da Proposição 3.3.7 sabemos que F é diagonalizável e que seus autovalores são $\widehat{f}(\chi_0)$, ..., $\widehat{f}(\chi_{n-1})$. Seja $\mathcal{B}$ a matriz de F com respeito a base $\{\delta_{[0]}, ..., \delta_{[n-1]}\}$. Afirmamos que $\mathcal{A} = \mathcal{B}$, o que completa a demonstração. De fato, $B_{ij} = F(\delta_{[j]})([i]) = f * \delta_{[j]}([i]) = f([i] - [j]) = g([j] - [i]) = \mathcal{A}_{ij}$. □

Proposição 3.4.6. *O conjunto das matrizes circulantes de ordem n é uma subálgebra de $M_n(\mathbb{C})$. Consequentemente, soma, produto e multiplicação por escalar de matrizes circulantes resultam em matrizes circulantes.*

Demonstração: Pela Proposição 3.4.3 a aplicação

$$\begin{aligned} F : L^2(\mathbb{Z}_n) &\longrightarrow M_n(\mathbb{C}) \\ f &\longmapsto F(f) \end{aligned}$$

onde $F(f)_{ij} = f([j] - [i])$, é injetiva e sua imagem é exatamente o conjunto das matrizes circulantes de ordem n. Assim, basta provarmos que F é um homomorfismo de álgebras, isto é, que respeita soma, produto e multiplicação por escalar. Sejam $a, b \in L^2(\mathbb{Z}_n)$ e $\lambda \in \mathbb{C}$. $F(a+b)_{ij} = (a+b)([j] - [i]) = a([j] - [i]) + b([j] - [i]) = F(a)_{ij} + F(b)_{ij}$. Portanto $F(a+b) = F(a) + F(b)$.

$F(\lambda a)_{ij} = (\lambda a)([j] - [i]) = \lambda a([j] - [i]) = \lambda F(a)_{ij}$. Logo $F(\lambda a) = \lambda F(a)$. E finalmente

$$\begin{aligned} F(a * b)_{ij} &= a * b([j] - [i]) \\ &= \sum_{k=0}^{n-1} a([j] - [i] - [k])b([k]) \\ &= \sum_{k=1}^{n} a([j] - [i] - [k])b([k]). \end{aligned}$$

Por outro lado,

$$\begin{aligned} (F(a) \cdot F(b))_{ij} &= \sum_{l=1}^{n} F(a)_{il} F(b)_{lj} \\ &= \sum_{l=1}^{n} a([l] - [i])b([j] - [l]). \end{aligned}$$

Fazendo $[j] - [l] = [k]$, obtemos $[l] = [j] - [k]$ e assim

$$(F(a)F(b))_{ij} = \sum_{k=1}^{n} a([j] - [k] - [i])b([k]).$$

Portanto, $F(a * b) = F(a)F(b)$. □

Proposição 3.4.7. *Sejam G um grupo finito e X um subconjunto simétrico. Então a matriz do operador convolução*

$$\begin{aligned} F : L^2(G) &\longrightarrow L^2(G) \\ a &\longmapsto \delta_X * a \end{aligned}$$

na base $\{\delta_{g_1}, ..., \delta_{g_n}\}$ coincide com a matriz de adjacência do grafo de Cayley de G segundo a ordenação $G = \{g_1, ..., g_n\}$.

Demonstração: A entrada ij da matriz de F na base indicada é dada por

$$\begin{aligned} F(\delta_{g_j})(g_i) &= \delta_X * \delta_{g_j}(g_i) \\ &= \delta_X(g_i g_j^{-1}) \\ &= \begin{cases} 1 \text{ se } g_i g_j^{-1} \in X \\ 0 \text{ caso contrário.} \end{cases} \end{aligned}$$

Donde segue o resultado. □

Teorema 3.4.1. *Sejam $G = \{g_1, ..., g_n\}$ um grupo abeliano e $X \subset G$ um subconjunto simétrico. Sejam χ_1, ..., χ_n os carácteres irredutíveis de G e seja $\mathcal{A}$ a matriz de adjacência do grafo de Cayley de G com respeito a X (usando esta ordenação para os elementos de G). Então:*

1. *Os autovalores de $\mathcal{A}$ são os números reais*

$$\lambda_i = \sum_{x \in X} \chi_i(x),$$

   onde $1 \leq i \leq n$.

2. *A base ortonormal de autovetores correspondente a $\mathcal{A}$ é $\{v_1, ..., v_n\}$ onde*

$$v_i = \frac{1}{\sqrt{n}}(\chi_i(g_1), ..., \chi_i(g_n)).$$

Demonstração: Pela proposição anterior os autovalores de $\mathcal{A}$ são os autovalores do operador $F : L^2(G) \longrightarrow L^2(G)$ definido por $F(a) = \delta_X * a$ para todo $a \in L^2(G)$. E usando a Proposição 3.3.7 temos que estes autovalores são $\widehat{\delta}_X(\chi_1)$, ..., $\widehat{\delta}_X(\chi_n)$, isto é,

$$\lambda_i = \widehat{\delta}_X(\chi_i) = n\langle \delta_X, \chi_i \rangle = \sum_{g \in G} \delta_X(g)\overline{\chi_i(g)} = \sum_{x \in X} \overline{\chi_i(x)}.$$

Se $x = x^{-1}$, então $\chi(x) = \chi(x^{-1}) = \overline{\chi(x)}$. Caso $x \neq x^{-1}$, temos $\overline{\chi(x)} + \overline{\chi(x^{-1})} = \overline{\chi(x^{-1})} + \overline{\chi(x)}$. Portanto $\lambda_i = \sum\limits_{x \in X} \chi_i(x)$.

Ainda usando a Proposição 3.3.7, temos que $\{\chi_1, ..., \chi_n\}$ é a base ortonormal de autovetores de F, assim, se $\mathcal{B} = \{\delta_{g_1}, ..., \delta_{g_n}\}$, então

$$[F\chi_i]_{\mathcal{B}} = [\lambda_i \chi_i]_B = \lambda_i [\chi_i]_B = \lambda_i \begin{bmatrix} \chi_i(g_1) \\ \vdots \\ \chi_i(g_n) \end{bmatrix}$$

Por outro lado,

$$[F\chi_i]_{\mathcal{B}} = [F]_B [\chi_i]_B = \mathcal{A} \begin{bmatrix} \chi_i(g_1) \\ \vdots \\ \chi_i(g_n) \end{bmatrix}$$

Portanto $\{(\chi_i(g_1), ..., \chi_i(g_n)) \ : \ i = 1, ..., n\}$ é base de autovetores de $\mathcal{A}$. É fácil ver que tal base é ortogonal e que cada vetor tem norma n segundo o produto interno usual de $\mathbb{C}^n$. Isto conclui a demostração. □

3.5 Análise de Fourier sobre Grupos não (necessariamente) Abelianos

Vamos definir e estudar a transformada de Fourier sobre um grupo finito arbitrário. Gostaríamos que ela fosse um isomorfismo entre a álgebra $L^2(G)$ e uma álgebra mais familiar e que generalizasse de algum modo a transformada para grupos abelianos. Se tentarmos proceder de forma idêntica ao caso abeliano, isto é, se indicarmos por $\widehat{G}$ o conjunto formado pelos caráteres irredutíveis de G e tentarmos definir $T : L^2(G) \longrightarrow L^2(\widehat{G})$ teremos vários problemas. Primeiro, não provamos que $\widehat{G}$ é um grupo quando G não é abeliano. Em segundo lugar, se G não for abeliano, teremos dim $L^2(\widehat{G}) = |\widehat{G}| =$ dim $Z(L^2(G)) <$ dim $L^2(G)$ e assim fica impossível obter um isomorfismo entre $L^2(G)$ e $L^2(\widehat{G})$. E por fim, a álgebra $L^2(G)$ não é necessariamente comutativa, portanto se queremos obter um isomorfismo de álgebras, precisamos de um álgebra não necessariamente comutativa no contra-domínio. Começaremos, então, reformulando o caso abeliano.

Sejam G um grupo abeliano finito de ordem n e $\widehat{G} = \{\chi_1, ..., \chi_n\}$ o conjunto dos caráteres irredutíveis de G. O isomorfismo $S : L^2(\widehat{G}) \longrightarrow \mathbb{C}^n$ que leva a base $\{\delta_{\chi_1}, ..., \delta_{\chi_n}\}$ na base canônica $\{e_1, ..., e_n\}$ de $\mathbb{C}^n$, ou seja, $S\widehat{f} = \{\widehat{f}(\chi_1), ..., \widehat{f}(\chi_n)\}$, é um isomorfismo de álgebras quando consideramos $\mathbb{C}^n$ uma álgebra de maneira óbvia: $(a_1, ..., a_n) \cdot (b_1, ..., b_n) = (a_1 b_1, ..., a_n b_n)$. Compondo este isomorfismo de álgebras com a transformada de Fourier sobre o grupo abeliano G, obtemos o isomorfismo de álgebras $T : L^2(G) \longrightarrow \mathbb{C}^n$ definido por $Tf = (n\langle f, \chi_1\rangle, ..., n\langle f, \chi_n\rangle)$. Esta será nossa segunda versão para a transformada no caso abeliano. Notemos que esta versão leva a base de Fourier $\widehat{G} = \{\chi_1, ..., \chi_n\}$ na base $\{ne_1, ..., ne_n\}$ de $\mathbb{C}^n$ e portanto leva uma função f no vetor $(n\langle f, \chi_1\rangle, ..., n\langle f, \chi_n\rangle)$ cujas entradas são os coeficientes de Fourier de f. Para deduzir o caso geral, precisamos de

uma base de $L^2(G)$ correspondente a base de Fourier no caso abeliano, isto é, que esteja relacionada com a estrutura do grupo G, e também será necessário uma versão para os coeficientes de Fourier de uma função f.

Seja G um grupo finito de ordem n. Como de costume no capítulo anterior, seja $\varphi^{(1)}, ..., \varphi^{(s)}$ um sistema completo de representantes matriciais e unitários das classes de equivalência das representações irredutíveis de G e seja $d_k = \deg \varphi^{(k)}$ com $k \in \{1, ..., s\}$ seus respectivos graus. Como sabemos, $\{\sqrt{d_k}\varphi_{ij}^{(k)} \ : \ 1 \leq k \leq s, \ 1 \leq i, j \leq d_k\}$ é base ortonormal para $L^2(G)$, assim, dado $f \in L^2(G)$, temos

$$f = \sum_{k=1}^{s} \sum_{i,j=1}^{d_k} \langle f, \sqrt{d_k}\varphi_{ij}^{(k)} \rangle \sqrt{d_k}\varphi_{ij}^{(k)} = \sum_{k=1}^{s} d_k \sum_{i,j=1}^{d_k} \langle f, \varphi_{ij}^{(k)} \rangle \varphi_{ij}^{(k)}.$$

É razoável considerarmos $\{\varphi_{ij}^{(k)} \ : \ 1 \leq k \leq s, \ 1 \leq i, j \leq d_k\}$ a base de Fourier quando G é arbitrário, e $n\langle f, \varphi_{ij}^{(k)} \rangle$ com $1 \leq k \leq s$ e $1 \leq i, j \leq d_k$, os coeficientes de Fourier de uma função f. Dada uma função $f \in L^2(G)$ e um $k \in \{1, ..., s\}$ fixado, podemos organizar os coeficientes de Fourier de f, $n\langle f, \varphi_{ij}^{(k)} \rangle$ com i e j variando entre 1 e d_k, como uma matriz $d_k \times d_k$. Veja que é natural pensar em matrizes, pois estamos a procura de uma álgebra não comutativa mais familiar possível. Portanto, vamos indicar por $\widehat{f}(\varphi^{(k)})$ a k-ésima matriz associada a função $f \in L^2(G)$, ou seja, $\widehat{f}(\varphi^{(k)})$ é a matriz $d_k \times d_k$ cuja entrada ij é o coeficiente de Fourier $n\langle f, \varphi_{ij}^{(k)} \rangle$. Temos então que

$$\begin{aligned} \widehat{f}(\varphi^{(k)})_{ij} &= n\langle f, \varphi_{ij}^{(k)} \rangle \\ &= \sum_{g \in G} f(g)\overline{\varphi_{ij}^{(k)}(g)} \\ &= \left[\sum_{g \in G} f(g)\overline{\varphi_{g}^{(k)}} \right]_{ij} \end{aligned}$$

Portanto $\widehat{f}(\varphi^{(k)}) = \sum_{g \in G} f(g)\overline{\varphi_g^{(k)}}$.

Nosso próximo passo é investigar a relação entre matrizes associadas e a convolução. Sejam $a, b \in L^2(G)$ e $k \in \{1, ..., s\}$. Vamos estudar a k-ésima matriz associada a $a * b$.

$$\begin{aligned} \widehat{a * b}(\varphi^{(k)}) &= \sum_{x \in G} a * b(x)\overline{\varphi_x^{(k)}} \\ &= \sum_{x \in G} \left(\sum_{y \in G} a(xy^{-1})b(y) \right) \overline{\varphi_x^{(k)}} \\ &= \sum_{y \in G} b(y) \left(\sum_{x \in G} a(xy^{-1})\overline{\varphi_x^{(k)}} \right). \end{aligned}$$

Fazendo a mudança de variável $xy^{-1} = z$ ($\therefore x = zy$), obtemos

$$\widehat{a * b}(\varphi^{(k)}) = \sum_{y \in G} b(y) \left(\sum_{z \in G} a(z)\overline{\varphi_{zy}^{(k)}} \right)$$

$$\begin{aligned} &= \sum_{y\in G}\sum_{z\in G} b(y)a(z)\overline{\varphi^{(k)}_{zy}} \\ &= \sum_{y\in G}\sum_{z\in G} a(z)\overline{\varphi^{(k)}_{z}}\, b(y)\overline{\varphi^{(k)}_{y}} \\ &= \left(\sum_{z\in G} a(z)\overline{\varphi^{(k)}_{z}}\right)\left(\sum_{y\in G} b(y)\overline{\varphi^{(k)}_{y}}\right) \\ &= \widehat{a}(\varphi^{(k)})\widehat{b}(\varphi^{(k)}). \end{aligned}$$

Isto nos motiva a definir a transformada como a aplicação $T : L^2(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$, onde $M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ é o produto direto (ou soma direta externa) das álgebras de matrizes $M_{d_1}(\mathbb{C}), ..., M_{d_s}(\mathbb{C})$, que leva f na s-upla de matrizes associadas $(\widehat{f}(\varphi^{(1)}), ..., \widehat{f}(\varphi^{(s)})$. Pois com esta definição, dado que $T(a * b) = Ta \cdot Tb \Leftrightarrow \widehat{a * b}(\varphi^{(k)}) = \widehat{a}(\varphi^{(k)}) \cdot \widehat{b}(\varphi^{(k)})$ para todo $k \in \{1, ..., s\}$, os produtos são respeitados. A álgebra do contradomínio é simples (familiar). Agora que terminamos nossa tentativa de motivação, passemos a uma exposição mais sistemática.

Observação 3.5.1. *Em todo o restante desta seção, estaremos supondo que G é um grupo finito de ordem n, $\varphi^{(1)}$, ..., $\varphi^{(s)}$ é um sistema de representantes matriciais e unitários das classes de equivalência de representações irredutíveis de G, $d_i = \deg \varphi^{(i)}$ com $i \in \{1, ..., s\}$ são seus respectivos graus e $\chi_1, ..., \chi_s$ são seus respectivos caráteres.*

Definição 3.5.1 (Base e coeficientes de Fourier)**.** *Seja $f \in L^2(G)$. A base $\{\varphi^{(k)}_{ij} \ : \ 1 \leq k \leq s, \ 1 \leq i, j \leq d_k\}$ é dita base de Fourier, e os coeficientes $n\langle f, \varphi^{(k)}_{ij}\rangle$ com $k \in \{1, ..., s\}$ e, para cada k fixado, $i, j \in \{1, ..., d_k\}$ são chamados coeficientes de Fourier de f.*

Definição 3.5.2 (Transformada de Fourier)**.** *Definimos a aplicação $T : L^2(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ por $Tf = (\widehat{f}(\varphi^{(1)}), ..., \widehat{f}(\varphi^{(s)}))$, onde $\widehat{f}(\varphi^{(k)})_{ij} = n\langle f, \varphi^{(k)}_{ij}\rangle = \sum_{g\in G} f(g)\overline{\varphi^{(k)}_{ij}(g)}$. Dizemos que Tf é a transformada de Fourier de f e que T é a transformada de Fourier sobre o grupo finito G.*

Observação 3.5.2. *Como vimos na parte introdutória desta seção, $\widehat{f}(\varphi^{(k)}) = \sum_{g\in G} f(g)\overline{\varphi^{(k)}_{g}}$.*

Observação 3.5.3. *Se G é abeliano, a reformulação da transformada da seção 3 é*

$$\begin{aligned} T : L^2(G) &\longrightarrow \mathbb{C}^n = \mathbb{C} \times \cdots \times \mathbb{C} \\ f &\longmapsto (n\langle f, \chi_1\rangle, ..., n\langle f, \chi_n\rangle). \end{aligned}$$

Podemos pensar $\mathbb{C}^n = \mathbb{C} \times \cdots \times \mathbb{C}$ como o produto direto de n cópias da álgebra das matrizes 1×1 com entradas em $\mathbb{C}$. Uma vez que, para um grupo abeliano G, $s = n$ e $\{\varphi^{(k)}_{ij} \ : \ 1 \leq k \leq s, \ 1 \leq i, j \leq d_k\} = \{\chi_1, ..., \chi_n\}$, vemos que a definição atual de transformada é compatível com a nossa segunda versão para a Transformada de Fourier sobre um grupo abeliano.

Proposição 3.5.1 (Fórmula da inversão)**.** *Se f é uma função complexa definida sobre o grupo G, então*

$$f = \frac{1}{n}\sum_{k=1}^{s}\sum_{i,j=1}^{d_k} d_k \widehat{f}(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)}$$

Demonstração: Como vimos no início da seção, $f = \sum_{k=1}^{s} d_k \sum_{i,j=1}^{d_k} \langle f, \varphi_{ij}^{(k)}\rangle \varphi_{ij}^{(k)}$. Portanto

$$\begin{aligned} f &= \frac{1}{n}\sum_{k=1}^{s}\sum_{i,j=1}^{d_k} d_k n\langle f, \varphi_{ij}^{(k)}\rangle \varphi_{ij}^{(k)} \\ &= \frac{1}{n}\sum_{k=1}^{s}\sum_{i,j=1}^{d_k} d_k \widehat{f}(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)}. \end{aligned}$$

□

Proposição 3.5.2. *A transformada de Fourier $T : L^2(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ é um isomorfismo de espaços vetoriais.*

Demonstração: Notemos que $T(c_1f_1 + c_2f_2) = c_1Tf_1 + c_2Tf_2 \Leftrightarrow \widehat{c_1f_1 + c_2}f_2(\varphi^{(k)}) = c_1\widehat{f}_1(\varphi^{(k)}) + c_2\widehat{f}_2(\varphi^{(k)})$ para todo $k \in \{1, ..., s\}$. Fixando $k \in \{1, ..., s\}$, temos

$$\begin{aligned} \widehat{c_1f_1 + c_2}f_2(\varphi^{(k)}) &= \sum_{g\in G}(c_1f_1 + c_2f_2)(g)\overline{\varphi_g^{(k)}} \\ &= \sum_{g\in G} c_1f_1(g)\overline{\varphi_g^{(k)}} + c_2f_2(g)\overline{\varphi_g^{(k)}} \\ &= c_1\sum_{g\in G} f_1(g)\overline{\varphi_g^{(k)}} + c_2\sum_{g\in G} f_2(g)\overline{\varphi_g^{(k)}} \\ &= c_1\widehat{f}_1(\varphi_g^{(k)}) + c_2\widehat{f_2}(\varphi_g^{(k)}). \end{aligned}$$

Portanto, T é linear. Para provar que T é invertível, observemos que a fórmula da inversão fornece uma inversa à esquerda: $S : M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C}) \longrightarrow L^2(G)$ que leva $\mathbb{A} = (\mathbb{A}^{(1)}, ..., \mathbb{A}^{(s)})$ em $\frac{1}{n}\sum_{k=1}^{s}\sum_{i,j=1}^{d_k} d_k(\mathbb{A}^{(k)})_{ij}\varphi_{ij}^{(k)}$. Logo T é injetiva. E como $\dim L^2(G) = |G| = d_1^2 + \cdots + d_s^2 = \dim M_{d_1}(\mathbb{C}) + \cdots + \dim M_{d_s}(\mathbb{C}) = \dim (M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C}))$, segue que T é isomorfismo. □

.

Proposição 3.5.3. *A Transformada de Fourier sobre o grupo finito G leva a base $\{\delta_g \ : \ g \in G\}$ de $L^2(G)$ na base $\{T\delta_g \ : \ g \in G\}$ onde $T\delta_g = (\overline{\varphi_g^{(1)}}, ..., \overline{\varphi_g^{(s)}})$.*

Demonstração: $\widehat{\delta}_g(\varphi^{(k)}) = \sum_{x\in G}\delta_g(x)\overline{\varphi_x^{(k)}} = \overline{\varphi_g^{(k)}}$. □

No próximo resultado, provaremos que $T(a * b) = Ta \cdot Tb$, que é o que falta para concluirmos que a transformada é um isomorfismo de álgebras. Na verdade, já provamos isto no início da seção quando tentamos motivar as definições, mas devido a sua importância e por termos uma demonstração mais simples, vale a pena que tal resultado seja refeito.

Teorema 3.5.1 (Wederburn)**.** *A Transformada de Fourier* $T : L^2(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ *é um isomorfismo de álgebras.*

Demonstração: Para provarmos que T respeita os produtos, é suficiente, como vimos no comentário acima do Teorema 3.3.1, que verifiquemos que $T(\delta_g * \delta_h) = T\delta_g \cdot T\delta_h$ para $g, h \in G$ arbitrários, que, por sua vez, é equivalente a provar que $\widehat{\delta_g * \delta_h}(\varphi^{(k)}) = \widehat{\delta}_g(\varphi^{(k)}) \cdot \widehat{\delta}_h(\varphi^{(k)})$ para todo $k \in \{1, ..., s\}$. Ora

$$\widehat{\delta_g * \delta_h}(\varphi^{(k)}) = \widehat{\delta}_{gh}(\varphi^{(k)}) = \overline{\varphi_{gh}^{(k)}} = \overline{\varphi_g^{(k)}\varphi_h^{(k)}} = \widehat{\delta}_g(\varphi^{(k)})\widehat{\delta}_h(\varphi^{(k)}).$$

□

Proposição 3.5.4. *A Transformada de Fourier* $T : L^2(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ *leva a base de Fourier* $\{\varphi_{ij}^{(k)} : 1 \leq k \leq s,\ 1 \leq i, j \leq d_k\}$ *na base* $\{T\varphi_{ij}^{(k)} : 1 \leq k \leq s,\ 1 \leq i, j \leq d_k\}$*, onde* $T\varphi_{ij}^{(k)} = (0, ..., 0, \frac{n}{d_k}E_{ij}, 0, ...)$*, isto é,* $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(m)}) = 0$ *se* $m \neq k$*, e* $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(k)}) = \dfrac{n}{d_k}E_{ij}$*. Onde* E_{ij} *é a* ij*-ésima matriz de base canônica de* $M_{d_k}(\mathbb{C})$*.*

Demonstração: $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(m)})_{\alpha\beta} = n\langle\varphi_{ij}^{(k)}, \varphi_{\alpha\beta}^{(m)}\rangle$. Usando as relações de ortogonalidade de Schur (teorema 2.5.1), concluímos: se $m \neq k$, então $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(m)})_{\alpha\beta} = 0$ quaisquer que sejam os índices α e β. Se $\alpha \neq i$ ou $\beta \neq j$, então $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(k)})_{\alpha\beta} = 0$. E finalmente, $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(k)})_{ij} = \dfrac{n}{d_k}$. □

Seja $\langle\cdot,\cdot\rangle_k$ o produto hermitiano usual de $M_{d_k}(\mathbb{C})$, isto é, dados $\mathcal{A}^{(k)}, \mathcal{B}^{(k)} \in M_{d_k}(\mathbb{C})$,

$$\langle\mathcal{A}^{(k)}, \mathcal{B}^{(k)}\rangle_k = \text{Traço } \mathcal{A}^{(k)}(\mathcal{B}^{(k)})^* = \sum_{i,j=1}^{d_k} (\mathcal{A}^{(k)})_{ij}\overline{(\mathcal{B}^{(k)})}_{ij}.$$

Obtemos naturalmente um produto hermitiano em $M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ pondo, para $\mathcal{A} = (\mathcal{A}^{(1)}, ..., \mathcal{A}^{(s)})$ e $\mathcal{B} = (\mathcal{B}^{(1)}, ..., \mathcal{B}^{(s)})$,

$$\langle\mathcal{A}, \mathcal{B}\rangle = \sum_{k=1}^{s}\langle\mathcal{A}^{(k)}, \mathcal{B}^{(k)}\rangle_k = \sum_{k=1}^{s}\text{Traço } \mathcal{A}^{(k)}(\mathcal{B}^{(k)})^*.$$

Na próxima proposição, veremos que a transformada de Fourier é uma isometria quando consideramos no seu contra-domínio o produto hermitiano acima com alguns pequenos ajustes. Como foi na versão deste resultado para grupos abelianos, daremos duas demonstrações; a segunda será bem mais curta que a primeira, pois usará a proposição

anterior, na qual vimos que a imagem da base de Fourier tem um aspecto bastante simples. Antes de começarmos, recorde que se E_{ij} e E_{kl} são elementos da base canônica de uma álgebra de matrizes, então $E_{ij} \cdot E_{kl} = 0$ se $j \neq k$, e $E_{ij} \cdot E_{jl} = E_{il}$.

Proposição 3.5.5 (Fórmula de Plancherel)**.** *Dados $a, b \in L^2(G)$, vale a fórmula:*

$$\langle a, b\rangle = \frac{1}{n^2}\sum_{k=1}^{s} d_k \, \textit{Traço} \, \left[\widehat{a}(\varphi^{(k)})\widehat{b}(\varphi^{(k)})^*\right].$$

Ou seja, considerando o produto hermitiano

$$\langle \mathcal{A}, \mathcal{B}\rangle = \frac{1}{n^2}\sum_{k=1}^{s} d_k \, \textit{Traço} \, \mathcal{A}^{(k)}(\mathcal{B}^{(k)})^*,$$

onde $\mathcal{A} = (\mathcal{A}^{(1)}, ..., \mathcal{A}^{(s)})$ e $\mathcal{B} = (\mathcal{B}^{(1)}, ..., \mathcal{B}^{(s)})$, a transformada de Fourier é uma transformação unitária.

Demonstração 1: Vamos desenvolver o lado direito da igualdade

$$\begin{aligned}
D &= \frac{1}{n^2}\sum_{k=1}^{s} d_k \text{Traço} \, \left[\widehat{a}(\varphi^{(k)})\widehat{b}(\varphi^{(k)})^*\right] \\
&= \frac{1}{n^2}\sum_{k=1}^{s} d_k \sum_{i,j=1}^{d_k} \widehat{a}(\varphi^{(k)})_{ij}\overline{\widehat{b}(\varphi^{(k)})}_{ij} \\
&= \frac{1}{n^2}\sum_{k=1}^{s} d_k \sum_{i,j=1}^{d_k} \left(\sum_{g\in G} a(g)\overline{\varphi_{ij}^{(k)}(g)}\right)\overline{\left(\sum_{h\in G} b(h)\overline{\varphi_{ij}^{(k)}(h)}\right)} \\
&= \frac{1}{n^2}\sum_{k=1}^{s} d_k \sum_{i,j=1}^{d_k} \sum_{g,h\in G} a(g)\overline{b(h)}\varphi_{ij}^{(k)}(h)\overline{\varphi_{ij}^{(k)}(g)} \\
&= \frac{1}{n^2}\sum_{k=1}^{s} d_k \sum_{g,h\in G} a(g)\overline{b(h)}\left(\sum_{ij=1}^{d_k}\varphi_{ij}^{(k)}(h)\overline{\varphi_{ij}^{(k)}(g)}\right) \\
&= \frac{1}{n^2}\sum_{k=1}^{s} d_k \sum_{g,h\in G} a(g)\overline{b(h)}\left(\text{Traço} \, \varphi_h^{(k)}(\varphi_g^{(k)})^*\right).
\end{aligned}$$

Como Traço $\varphi_h^{(k)}(\varphi_g^{(k)})^* =$ Traço $\varphi_h^{(k)}\varphi_{g^{-1}}^{(k)} =$ Traço $\varphi_{hg^{-1}}^{(k)} = \chi_k(hg^{-1})$, e como $d_k = \chi_k(1_G)$, obtemos

$$\begin{aligned}
D &= \frac{1}{n^2}\sum_{k=1}^{s}\sum_{g,h\in G} a(g)\overline{b(h)}\chi_k(1_G)\chi_k(hg^{-1}) \\
&= \frac{1}{n^2}\sum_{g,h\in G} a(g)\overline{b(h)}\sum_{k=1}^{s}\chi_k(1_G)\chi_k(hg^{-1}).
\end{aligned}$$

Como a classe de conjunção de 1_G é $\{1_G\}$, usando as segundas relações de ortogonalidade para caráteres (teorema 2.6.6) obtemos que

$$\sum_{k=1}^{s}\chi_k(1_G)\chi_k(hg^{-1}) = \begin{cases} 0 \text{ se } hg^{-1} \notin \{1_G\} (\Leftrightarrow h \neq g), \\ \dfrac{|G|}{|\{1_G\}|} = n \text{ se } h = g. \end{cases}$$

Portanto

$$\begin{aligned} D &= \frac{1}{n^2}\sum_{g\in G} a(g)\overline{b(g)}n \\ &= \frac{1}{n}\sum_{g\in G} a(g)\overline{b(g)} \\ &= \langle a, b\rangle. \end{aligned}$$

□

Demonstração 2: É suficiente provar que T leva uma base ortonormal em um conjunto ortonormal, e a base adequada para a nossa investigação é a base de Fourier normalizada, pois, como vimos na proposição anterior, $T\varphi_{ij}^{(m)} = (0, ..., 0, \frac{n}{d_m}E_{ij}, 0, ...,)$, com $\frac{n}{d_m}E_{ij}$ na m-esima entrada, e $T\varphi_{\alpha\beta}^{(l)} = (0, ..., 0, \frac{n}{d_l}E_{\alpha\beta}, 0, ...,)$, com $\frac{n}{d_l}E_{\alpha\beta}$ na l-esima entrada. Segue imediatamente que $\langle T\sqrt{d_m}\varphi_{ij}^{(m)}, T\sqrt{d_l}\varphi_{\alpha\beta}^{(l)}\rangle = \sqrt{d_m}\sqrt{d_l}\langle T\varphi_{ij}^{(m)}, T\varphi_{\alpha\beta}^{(l)}\rangle = 0$ caso m seja diferente de l.
Suponhamos $m = l$. Então

$$\begin{aligned} \langle T\sqrt{d_m}\varphi_{ij}^{(m)}, T\sqrt{d_m}\varphi_{\alpha\beta}^{(m)}\rangle &= d_m\langle T\varphi_{ij}^{(m)}, T\varphi_{\alpha\beta}^{(m)}\rangle \\ &= d_m\frac{1}{n^2}d_m\text{Traço } \frac{n}{d_m}E_{ij}\left(\frac{n}{d_m}E_{\alpha\beta}\right)^* \\ &= \text{Traço } E_{ij}E_{\beta\alpha}. \end{aligned}$$

Se $j \neq \beta$, temos $E_{ij}E_{\beta\alpha} = 0$ e portanto Traço $E_{ij}E_{\beta\alpha} = 0$. Se $j = \beta$ e $i \neq \alpha$, temos Traço $E_{ij}E_{\beta\alpha}$ = Traço $E_{i\alpha} = 0$. Finalmente, se $j = \beta$ e $i = \alpha$, temos Traço $E_{ij}E_{\beta\alpha}$ = Traço $E_{ii} = 1$. Portanto a base $\{T\sqrt{d_k}\varphi_{ij}^{(k)} \ : \ i \leq k \leq s, \ 1 \leq i, j \leq d_k\}$ é ortonormal, como queríamos demonstrar. □

No próximo resultado, calcularemos a imagem da base $\{\chi_1, ..., \chi_s\}$ de $Z(L^2(G))$ formada pelos caráteres irredutíveis de G. Como consequência, uma vez que restringindo a transformada obtemos um isomorfismo de álgebras entre os centros, deduziremos que $Z(M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})) = \{(\lambda_1 I, ..., \lambda_s I) \ : \ \lambda_i \in \mathbb{C}\}$ onde I representa a matriz identidade de sua respectiva álgebra de matrizes. Uma outra forma de obter este resultado é usando o fato que $Z(M_{d_k}(\mathbb{C})) = \{\lambda I \ : \ \lambda \in \mathbb{C}\}$, o qual for provado na proposição 3.2.3, e lembrando que o centro de um produto direto é o produto direto dos centros.

Proposição 3.5.6. *A Transformada de Fourier $T : L^2(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ leva a base $\{\chi_1, ..., \chi_s\}$ de $Z(L^2(G))$ na base $\{T\chi_1, ..., T\chi_s\}$ de $Z(M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C}))$, onde $T\chi_k = (0, ..., 0, \frac{n}{d_k}I, 0, ..., 0)$, ou seja, $\widehat{\chi}_k(\varphi^{(m)}) = 0$ se $m \neq k$, e $\widehat{\chi}_k(\varphi^{(k)}) = \frac{n}{d_k}I$.*

Demonstração: $\chi_k = \sum_{i=1}^{d_k} \varphi_{ii}^{(k)} \Rightarrow T\chi_k = \sum_{i=1}^{d_k} T\varphi_{ii}^{(k)} \Rightarrow \widehat{\chi}_k(\varphi^{(m)}) = \sum_{i=1}^{d_k} \widehat{\varphi_{ii}^{(k)}}(\varphi^{(m)})$ para todo $m \in \{1, ..., s\}$. Assim $\widehat{\chi}_k(\varphi^{(m)}) = 0$ se $m \neq k$, e

$$\begin{aligned} \widehat{\chi}_k(\varphi^{(k)}) &= \sum_{i=1}^{d_k} \widehat{\varphi_{ii}^{(k)}}(\varphi^{(k)}) \\ &= \sum_{i=1}^{d_k} \frac{n}{d_k} E_{ii} \\ &= \frac{n}{d_k} I. \end{aligned}$$

□

Corolário 3.5.1. *Se $f \in Z(L^2(G))$, então $Tf = (\frac{n}{d_1}\langle f, \chi_1\rangle I, ..., \frac{n}{d_s}\langle f, \chi_s\rangle I)$, isto é, $\widehat{f}(\varphi^{(k)}) = \frac{n}{d_k}\langle f, \chi_k\rangle I$ para todo $k \in \{1, ..., s\}$.*

Demonstração: $f = \sum_{i=1}^{s} \langle f, \chi_i\rangle \chi_i \Rightarrow Tf = \sum_{i=1}^{s} \langle f, \chi_i\rangle T\chi_i$. Segue que

$$\begin{aligned} \widehat{f}(\varphi^{(k)}) &= \sum_{i=1}^{s} \langle f, \chi_i\rangle \widehat{\chi}_i(\varphi^{(k)}) \\ &= \langle f, \chi_k\rangle \frac{n}{d_k} I. \end{aligned}$$

□

Corolário 3.5.2. *$\frac{d_1}{n}\chi_1 + \cdots + \frac{ds}{n}\chi_s$ é a identidade de $L^2(G)$.*

Demonstração: $T\left(\frac{d_1}{n}\chi_1 + \cdots + \frac{ds}{n}\chi_s\right) = (I, ..., I)$, que é a identidade de $M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$. □

Os dois próximos resultados são versões da proposição 3.3.6 para o contexto desta seção, no qual o grupo finito G não é necessariamente abeliano. Ou seja, investigaremos o comportamento dos elementos da base $\{\chi_1, ..., \chi_s\}$ de $Z(L^2(G))$ e da base de Fourier $\{\varphi_{ij}^{(k)} : 1 \leq k \leq s,\ 1 \leq i, j \leq d_k\}$, com respeito a convolução. No caso abeliano demos duas demonstrações e em uma delas foi possível evitar o uso da transformada de Fourier sobre o grupo abeliano G. Não conseguimos repetir este feito aqui, o que deixa a transformada ainda mais imprescindível.

Proposição 3.5.7. *Seja $\{\chi_1, ..., \chi_s\}$ a base de $Z(L^2(G))$ formada pelos caráteres irredutíveis de G. Então $\chi_k * \chi_l = 0$ se $k \neq l$, e $\chi_k * \chi_k = \frac{n}{d_k}\chi_k$.*

Demonstração:

$$\begin{aligned} \chi_k * \chi_l &= T^{-1}(T(\chi_k * \chi_l)) \\ &= T^{-1}(T\chi_k \cdot T\chi_l) \\ &= T^{-1}((0, ..., 0, \frac{n}{d_k}I, 0, ..., 0) \cdot (0, ..., 0, \frac{n}{d_l}I, 0, ..., 0)) \end{aligned}$$

Portanto se $k \neq l$, $\chi_k * \chi_l = T^{-1}(0) = 0$, e

$$\begin{aligned}\chi_k * \chi_k &= T^{-1}((0,...,0,\frac{n^2}{d_k^2}I,0,...,0)) \\ &= \frac{n}{d_k}T^{-1}((0,...,0,\frac{n}{d_k}I,0,...,0)) \\ &= \frac{n}{d_k}\chi_k.\end{aligned}$$

□

Proposição 3.5.8. *Seja* $\{\varphi_{ij}^{(k)} : 1 \leq k \leq s,\ 1 \leq i,j \leq d_k\}$ *a base de Fourier de* $L^2(G)$. *Então* $\varphi_{ij}^{(k)} * \varphi_{\alpha\beta}^{(l)} = 0$ *se* $k \neq l$ *ou* $j \neq \alpha$, *e* $\varphi_{ij}^{(k)} * \varphi_{j\beta}^{(k)} = \frac{n}{d_k}\varphi_{i\beta}^{(k)}$.

Demonstração: $\varphi_{ij}^{(k)} * \varphi_{\alpha\beta}^{(l)} = T^{-1}\left(T\varphi_{ij}^{(k)} \cdot T\varphi_{\alpha\beta}^{(l)}\right)$. Como $\widehat{\varphi_{ij}^{(k)}}(\varphi^{(m)}) = 0$ se $m \neq k$, e $\varphi_{\alpha\beta}^{(l)}(\varphi^{(m)}) = 0$ se $m \neq l$, temos, caso k seja diferente de l, que $\varphi_{ij}^{(k)} * \varphi_{\alpha\beta}^{(l)} = T^{-1}(0) = 0$. Suponhamos agora $k = l$ e $j \neq \alpha$.

$$\varphi_{ij}^{(k)} * \varphi_{\alpha\beta}^{(k)} = T^{-1}((0,...,0,\frac{n^2}{d_k^2}E_{ij}E_{\alpha\beta},0,...,0)).$$

Como $E_{ij}E_{\alpha\beta} = 0$ neste caso, temos $\varphi_{ij}^{(k)} * \varphi_{\alpha\beta}^{(k)} = 0$. Finalmente,

$$\begin{aligned}\varphi_{ij}^{(k)} * \varphi_{j\beta}^{(k)} &= T^{-1}((0,...,0,\frac{n^2}{d_k^2}E_{ij}E_{j\beta},0,...,0)) \\ &= T^{-1}(\frac{n}{d_k}(0,...,0,\frac{n}{d_k}E_{i\beta},0,...,0)) \\ &= \frac{n}{d_k}\varphi_{i\beta}^{(k)}.\end{aligned}$$

□

A próxima proposição é a versão da proposição 3.3.7 para grupos finitos arbitrários, a qual será usada em uma generalização de aplicação que fizemos na seção anterior aos grafos de Cayley. Assim como foi nos resultados acima, não conseguimos adaptar a demonstração que evita o uso da transformada de Fourier, mas as outras duas adequam-se sem maiores problemas.

Proposição 3.5.9. *Seja* $a \in Z(L^2(G))$. *Considere-se o operador convolução por* a, *isto é, a aplicação* $A : L^2(G) \longrightarrow L^2(G)$ *definida por* $A(b) = a * b$. *Então* A *é linear e* $\varphi_{ij}^{(k)}$ *é autovetor de* A *com autovalor* $\frac{n}{d_k}\langle a, \chi_k\rangle$. *Consequentemente a base de Fourier* $\{\varphi_{ij}^{(k)} : 1 \leq k \leq s,\ 1 \leq i,j \leq d_k\}$ *é base ortogonal de autovetores.*

Demonstração1: A linearidade de A é óbvia.

$$A(\varphi_{ij}^{(k)}) = a * \varphi_{ij}^{(k)} = T^{-1}(Ta \cdot T\varphi_{ij}^{(k)})$$

Usando a proposição 3.5.4 e o corolário 3.5.1, obtemos

$$\begin{aligned} A(\varphi_{ij}^{(k)}) &= T^{-1}((0,...,0,\frac{n}{d_k}\langle a,\chi_k\rangle I\frac{n}{d_k}E_{ij},0,...,0)) \\ &= \frac{n}{d_k}\langle a,\chi_k\rangle T^{-1}((0,...,0,\frac{n}{d_k}E_{ij},0,...,0)) \\ &= \frac{n}{d_k}\langle a,\chi_k\rangle\varphi_{ij}^{(k)}. \end{aligned}$$

□

Demonstração 2: Vamos usar os dois últimos resultados. Como $a \in Z(L^2(G))$, $a = \sum_{k=1}^{s}\langle a,\chi_k\rangle\chi_k$. Assim, $A(\varphi_{ij}^{(l)}) = a*\varphi_{ij}^{(l)} = \left(\sum_{k=1}^{s}\langle a,\chi_k\rangle\chi_k\right)*\varphi_{ij}^{(l)} = \sum_{k=1}^{s}\langle a,\chi_k\rangle\left(\chi_k*\varphi_{ij}^{(l)}\right)$. Mas $\chi_k*\varphi_{ij}^{(l)} = \left(\sum_{\alpha=1}^{d_k}\varphi_{\alpha\alpha}^{(k)}\right)*\varphi_{ij}^{(l)} = 0$ se $k \neq l$, portanto

$$\begin{aligned} A(\varphi_{ij}^{(l)}) &= \langle a,\chi_l\rangle\chi_l*\varphi_{ij}^{(l)} \\ &= \langle a,\chi_l\rangle\left(\sum_{\alpha=1}^{d_l}\varphi_{\alpha\alpha}^{(l)}\right)*\varphi_{ij}^{(l)} \\ &= \langle a,\chi_l\rangle\left(\sum_{\alpha=1}^{d_l}\varphi_{\alpha\alpha}^{(l)}*\varphi_{ij}^{(l)}\right) \\ &= \langle a,\chi_l\rangle\varphi_{ii}^{(l)}*\varphi_{ij}^{(l)} \\ &= \langle a,\chi_l\rangle\frac{n}{d_l}\varphi_{ij}^{(l)}. \end{aligned}$$

□

4 ALGUMAS APLICAÇÕES DA TRANSFORMADA DE FOURIER EM GRUPOS

Este capítulo é dedicado a algumas aplicações da teoria que construímos até aqui.

4.1 Grafos de Cayley

Iniciaremos o capítulo com uma versão para grupos não-necessarimente abelianos da aplicação aos grafos de Cayley que fizemos na seção 4 do capitulo anterior. Ou seja, calcularemos os autovalores da matriz de adjacência do grafo de Cayley de um grupo G com respeito a um subconjunto simétrico X, entretanto, diferentemente do caso abeliano, teremos que considerar uma classe restrita de tais grafos.

Para cumprir nosso objetivo, usaremos a transformada de Fourier sobre o grupo finito G, a qual pressupõe que está fixado um sistema completo de representantes matriciais e unitários das classes de representações irredutíveis de G, $\varphi^{(1)}$, ..., $\varphi^{(s)}$, com $d_i = \deg \varphi^{(i)}$ seus respectivos graus, e com χ_1, ..., χ_s seus respectivos caráteres.

Teorema 4.1.1. *Sejam $G = \{g_1, ..., g_n\}$ um grupo finito e $X \subset G$ um subconjunto simétrico. Suponhamos adicionalmente que $gXg^{-1} = X$ para todo $g \in G$, isto é, que X é fechado por conjugação. Então os autovalores da matriz de adjacẽncia do grafo de Cayley de G com respeito a X são λ_1, ..., λ_s onde*

$$\lambda_k = \frac{1}{d_k} \sum_{x \in X} \chi_k(x).$$

Demonstração: Notemos que a proposição 3.4.7 não assume que o grupo G é abeliano, portanto os autovalores que queremos calcular são os autovalores do operador

$$\begin{aligned} F : L^2(G) &\longrightarrow L^2(G) \\ a &\longmapsto \delta_X * a \end{aligned}$$

Se $\delta_X \in Z(L^2(G))$, então a proposição 3.5.9 garante que a base de Fourier, $\{\varphi_{ij}^{(k)} : 1 \leq k \leq s,\ 1 \leq i, j \leq d_k\}$, é base de autovetores e que o autovalor correspondente a $\varphi_{ij}^{(k)}$ é $\frac{n}{d_k}\langle \delta_X, \chi_k \rangle$. É aqui que usamos nossa hipótese adicional sobre X: de $gXg^{-1} = X$ para todo $g \in G$, concluímos, para quaisquer $g, h \in G$, que $ghg^{-1} \in X \Leftrightarrow h \in X$, portanto $\delta_X(ghg^{-1}) = \delta_X(h)$, ou seja, δ_X é, de fato, um elemento de $Z(L^2(G))$.

Dado que $\frac{n}{d_k}\langle \delta_X, \chi_k\rangle = \frac{1}{d_k}\sum_{x\in X}\overline{\chi_k(x)}$, e argumentando de forma idêntica ao que foi feito na demonstração do Teorema 3.4.1, obtemos que $\frac{1}{d_k}\sum_{x\in X}\overline{\chi_k(x)} = \frac{1}{d_k}\sum_{x\in X}\chi_k(x)$. □

4.2 Unidades em um Anel de Grupo

Nesta seção, vamos considerar a álgebra $\mathbb{C}G = \{\sum_{g\in G}\lambda_g g \ : \ \lambda_g \in \mathbb{C}\}$ introduzida na seção 2.4, com uma pequena diferença no produto hermitiano que usaremos aqui:

$$\left\langle \sum_{g\in G}\lambda_g g, \sum_{g\in G}\mu_g g \right\rangle = \frac{1}{|G|}\sum_{g\in G}\lambda_g\overline{\mu_g}.$$

Dessa forma, e tendo em vista o corolário 3.2.1, a diferença entre as álgebras $\mathbb{C}G$ e $L^2(G)$ é essencialmente notacional. Aliás, denotando um elemento $r \in \mathbb{C}G$ por $r = \sum_{g\in G} r(g)g$, temos, para $s \in \mathbb{C}G$, $rs = \sum_{g,h\in G} r(g)s(h)gh$. Ou podemos interpretar r e s como elementos de $L^2(G)$ e escrever $rs = \sum_{g\in G} rs(g)g$, onde $rs(g) = \sum_{g\in G} r(gh^{-1})s(h)$ (aqui, aproveitamos a convolução). Claro que tudo que foi feito no capítulo anterior pode ser interpretado com $\mathbb{C}G$ no lugar de $L^2(G)$.

Um subanel interessante de $\mathbb{C}G$, chamado o anel inteiro do grupo finito G, é

$$\mathbb{Z}G = \left\{ \sum_{g\in G} k(g)g \ : \ k(g) \in \mathbb{Z}, \ \forall g \in G \right\}.$$

A teoria das unidades (elementos invertíveis) de $\mathbb{Z}G$ é essencialmente devida a G. Higman (HIGMAN, 1940). A seguir, daremos uma demonstração de um dos resultados de Higman e também provaremos que se $\mathbb{Z}G$ e $\mathbb{Z}G'$ são anéis de grupos isomorfos (para G e G' finitos e abelianos) então os grupos G e G' são isomorfos.

Iniciaremos com a dedução de uma expressão alternativa para a inversa da transformada de Fourier. Como sempre, está fixado $\varphi^{(1)}$, ..., $\varphi^{(s)}$, um sistema completo de representantes matriciais e unitários das classes de representações irredutíveis de G, d_1, ..., d_s são seus respectivos graus, e χ_1, ..., χ_s seus caráteres. Lembre que, de acordo com a proposição 3.5.5, a transformada de Fourier:

$$\begin{array}{rcl} T : \mathbb{C}G & \longrightarrow & M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C}) \\ g & \longmapsto & (\varphi_g^{(1)}, ..., \varphi_g^{(s)}) \end{array}$$

é uma isometria.

Proposição 4.2.1 (Fórmula da inversão de Fourier)**.** *Sejam* $\mathcal{A} = (\mathcal{A}^{(1)}, ..., \mathcal{A}^{(s)}) \in M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ *e* $u \in \mathbb{C}G$ *tais que* $T(u) = \mathcal{A}$*. Então, para todo* $g \in G$*, vale:*

$$u(g) = \frac{1}{|G|}\sum_{j=1}^{s} d_j \, \textit{Traço}\left(\varphi_g^{(j)}\mathcal{A}^{(j)*}\right).$$

Demonstração: Como $\{\sqrt{|G|}g \ : \ g \in G\}$ é uma base ortonormal para $\mathbb{C}G$, temos que $\{\sqrt{|G|}T(g) \ : \ g \in G\}$ é base ortonormal de $M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$. Seja $A \in M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_1}(\mathbb{C})$ e considere a representação de $\mathcal{A}$ na base $\{\sqrt{|G|}T(g) \ : \ g \in G\}$:

$$\mathcal{A} = \sum_{g \in G} \mathcal{A}_g \sqrt{|G|} T(g) \ , \ \mathcal{A}_g \in \mathbb{C}, \ \forall g \in G.$$

Temos que:

$$\begin{aligned} \mathcal{A}_g &= \langle \mathcal{A}, \sqrt{|G|}T(g) \rangle_\star \\ &= \sum_{j=1}^{s} \frac{d_j}{|G|^2} \text{Traço} \left(\mathcal{A}^{(j)} \sqrt{|G|} \varphi^{(i)}(g)^* \right) \\ &= \sum_{j=1}^{s} \frac{d_j}{|G|^{3/2}} \text{Traço} \left(\varphi^{(j)}(g^{-1}) \mathcal{A}^{(j)} \right). \end{aligned}$$

Aplicando T^{-1} a $\mathcal{A}$, obtemos:

$$u = \sum_{j=1}^{s} \left[\frac{d_j}{|G|} \text{Traço} \left(\varphi^{(i)}(g^{-1}) \mathcal{A}^{(i)} \right) \right] g,$$

Como desejado. □

Lema 4.2.1. *Seja $u \in Z(\mathbb{C}G)$ uma unidade de torção (isto é, u é uma unidade cuja ordem é finita). Então, $\forall g \in G$, vale:*

$$\overline{u(g)} = u^{-1}(g^{-1}).$$

Demonstração: Como u tem ordem finita, a matriz $T(v)$ tem ordem finita, e o mesmo ocorre com $T(gu)$. Segue que os autovalores de $T(ug)$ são todos raizes da unidade (e que $T(gu)$ é diagonalizável). Digamos que $T(u) = (A) = (\mathcal{A}^{(1)}, ..., \mathcal{A}^{(s)})$. Então:

$$\begin{aligned} \overline{\text{Traço} \left(\varphi^{(j)}_{g^{-1}} \mathcal{A}^{(j)*} \right)} &= \text{Traço} \left(\varphi^{(j)}_{g^{-1}} \mathcal{A}^{(j)*} \right)^{-1} \\ &= \text{Traço} \left((\mathcal{A}^{(j)*})^{-1} \varphi^{(j)}_g \right) \\ &= \text{Traço} \left(\varphi^{(j)}_g (\mathcal{A}^{(j)-1})^* \right), \end{aligned}$$

onde usamos o fato de que o conjugado de uma raiz da unidade é o seu inverso, na primeira igualdade. Comparando com a fórmula da proposição acima, concluímos que $\overline{u(g)} = u^{-1}(g^{-1})$. □

Teorema 4.2.1 (Higmam)**.** *Seja G um grupo abeliano finito. O grupo das unidades de torção do anel $\mathbb{Z}G$ é igual a $\pm G = \{u \in \mathbb{C}G \ : \ u(g) = \pm 1$ para um único $g \in G$, e $u(h) = 0$ para $h \neq g\}$.*

Demonstração: Afirmamos que $\sum\limits_{g \in G} |u(g)|^2 = 1$, para todo unidade de torção u. Isto segue diretamento do lema anterior:

$$\sum_{g \in G} |u(g)|^2 = \sum_{g \in G} u(g)\overline{u(g)} = \sum_{g \in G} u(g) u^{-1}(g^{-1}).$$

Mas

$$\left(\sum_{g\in G} u(g)g\right)\left(\sum_{g\in G} u^{-1}(g^{-1})g^{-1}\right) = 1_G \in G,$$

logo $\sum_{g\in G} u(g)u^{-1}(g^{-1}) = 1$.

Se $u \in \mathbb{Z}G$ for uma unidade de torção, $u(g) \in \mathbb{Z}\ \forall g \in G$, e $u(g) = \pm 1$ para um único $g \in G$. Logo $u = \pm g$. □

Teorema 4.2.2. *Sejam G e G' grupos abelianos finitos tais que os aneis de grupos $\mathbb{Z}G$ e $\mathbb{Z}G'$ são isomorfos. Então G e G' são isomorfos.*

Demonstração: Sejam U e U' os grupos dos unidades em $\mathbb{Z}G$ e $\mathbb{Z}G'$ respectivamente. Note U e U' são grupos abelianos não necessariamente finitos e que $\mathbb{Z}G \simeq \mathbb{Z}G'$ implica $U \simeq U'$. Num grupo abeliano finito H, os elementos de torção formam um subgrupo H_0. Usando esta notação, temos $U_o \simeq U_0'$. Ora, de acordo com o teorema anterior, $U_0 \simeq G \times \mathbb{Z}_2$ e $U_0' \simeq G' \times \mathbb{Z}_2$, onde $\mathbb{Z}_2 = \{\pm 1\}$. Portanto $G \times \mathbb{Z}_2 \simeq G' \times \mathbb{Z}_2$. Usando agora o teorema de estrutura dos grupos abelianos finitamente gerados (o qual pode ser encontrado, por exemplo, em (ASH, 2000)) concluímos que $G \simeq G'$. □

4.3 Caminhadas Aleatórias em Grupos e Probabilidades

Sejam G um grupo finito e X uma variável aleatória com valores em G, ou seja, X é uma função do espaço de probabilidade Ω (isto é, um conjunto finito com medida de probabilidade) em G. A distribução da variável aleatória X é a função $P : G \longrightarrow [0,1]$ definida por $P(g) = \text{Prop}\,[X = g]$.

Observemos que $\sum_{g\in G} P(g) = 1$, e se $P : G \longrightarrow [0,1]$ é uma função que satisfaz esta condição, então P é a distribuição de alguma variável aleatória com valores em G. (De fato, basta tomarmos $\Omega = G$, $\text{Prob}\,\{S\} = \sum_{g\in S} P(g)$, $\forall S \subset G$, e $X = id_G$.)

Definição 4.3.1 (Distribuição de probabilidade)**.** *Uma distribução de Probabilidade (ou simplesmente uma probabilidade) em um grupo finito G é uma função $P : G \longrightarrow [0,1]$ tal que $\sum_{g\in G} P(g) = 1$. Se S é um subconjunto de G, definimos $P(S) = \sum_{g\in S} P(g)$. O suporte da probabilidade P é o conjunto $Sup(P) = \{g \in G\ :\ P(g) \neq 0\}$.*

Definição 4.3.2 (Distribuição uniforme)**.** *Seja G um grupo finito. A distribuição uniforme de G é dada por*

$$U(g) = \frac{1}{|G|},\ \forall g \in G.$$

Notemos que as funções $\delta_g : G \longrightarrow \mathbb{C}$ podem ser vistas como distribuições de probabilidade, simplesmente restringindo seus contra-domínios ao intervalo $[0,1]$. Enquanto

a distribução uniforme U representa a ausência de tendências, as distribuições δ_g são completamente tendenciosas.

Consideremos a álgebra $L^2(G)$. Podemos ver probabilidades em G como elementos de $L^2(G)$. O próximo lema relaciona probabilidades e a convolução.

Lema 4.3.1. *Sejam X e Y variáveis aletórias independentes e com valores em G, e sejam P e Q as respectivas distribuições de probabilidade. A variável aleatória XY tem distribução de probabilidade $P * Q$.*

Demonstração: Sejam $g, h \in G$. Se $Y = h$, então $XY = g \Leftrightarrow X = gh^{-1}$. Disto e da independência de X e Y, segue que

$$\text{Prop}\,[XY = g] = \sum_{h \in G} P(gh^{-1})Q(h) = (P * Q)(g).$$

□

Note que devemos verificar que $P * Q$ é de fato uma distribuição de probabilidade. Faremos isto a seguir.

Proposição 4.3.1. *Sejam P e Q probabilidades em G. A convolução $P * Q$ é uma probabilidade em G cujo suporte é dado por*

$$Sup\,(P * Q) = Sup\,(P) \cdot Sup\,(Q)\,.$$

Demonstração: Visto que $(P * Q)(g) = \sum\limits_{h \in G} P(gh^{-1})Q(h)$ temos que $(P * Q)(g) \geq 0$ e $(P * Q)(g) \leq \sum\limits_{h \in G} Q(h) = 1$. Por outro lado,

$$\begin{aligned}
\sum_{g \in G} (P * Q)(g) &= \sum_{g \in G} \sum_{h \in G} P(gh^{-1})Q(h) \\
&= \sum_{h \in G} \left(\sum_{g \in G} P(gh^{-1}) \right) Q(h) \\
&= \sum_{h \in G} Q(h) \\
&= 1.
\end{aligned}$$

Decerto $(P * Q)(g) \neq 0 \Leftrightarrow P(gh^{-1})$ e $Q(h) \neq 0$ para algum $h \in G$. Pondo $x = gh^{-1}$ e $y = h$, temos que $(P * Q)(g) \neq 0$ se, e somente se, existem $x \in \text{Sup}\,(P)$ e $y \in \text{Sup}\,(Q)$ tais que $xy = g$. Portanto $\text{Sup}\,(P * Q) = \text{Sup}\,(P) \cdot \text{Sup}\,(Q)$. □

Nosso próximo passo é introduzir uma noção de distância entre distribuições de probabilidades e estudar algumas de suas propriedades.

Definição 4.3.3. *A norma L^1 em $L(G)$ é definida por: $\|f\|_1 = \sum_{g\in G}|f(g)|$, $\forall f \in L(G)$. Se P é uma probabilidade em G, então $\|P\|_1 = 1$.*

Vejamos algumas propriedades da norma L^1.

Proposição 4.3.2. *Sejam $a, b \in L(G)$. Então:*

(1) $\|a\|_1 \geq 0$ *e* $\|a\|_1 = 0 \Leftrightarrow a = 0$.

(2) $\|\lambda a\|_1 = |\lambda|\|a\|_1$, *para todo* $\lambda \in \mathbb{C}$.

(3) $\|a + b\|_1 \leq \|a\|_1 + \|b\|_1$ *(desigualdade triangular)*

(4) $\|a * b\|_1 \leq \|a\|_1 \cdot \|b\|_1$.

Demonstração: Vamos provar apenas o item (4).

$$\begin{aligned}
\|a * b\|_1 &= \sum_{g\in G}|a * b(g)| \\
&= \sum_{g\in G}\left|\sum_{h\in G}a(gh^{-1})b(h)\right| \\
&\leq \sum_{g\in G}\sum_{h\in G}|a(gh^{-1})||b(h)| \\
&= \sum_{h\in G}|b(h)|\sum_{g\in G}|a(gh^{-1})| \\
&= \|b\|_1\|a\|_1.
\end{aligned}$$

□

Definição 4.3.4 (Variação total)**.** *A distância variação total entre as probabilidades P e Q em um grupo G é definida por:*

$$\|P - Q\|_{VT} = \max_{S\subset G}|P(S) - Q(S)|.$$

O próximo lema descreve conjuntos onde o máximo acima é atingido.

Lema 4.3.2. *Sejam P e Q probabilidades em G, e sejam $B = \{g \in G \ : \ P(g) \geq Q(g)\}$ e $C = \{g \in G \ : \ Q(g) \geq P(g)\}$. Então*

$$\|P - Q\|_{VT} = P(B) - Q(B) = Q(C) - P(C).$$

Demonstração: Se $P = Q$, o resultado é trivialmente válido. Suponhamos então $P \neq Q$. Existe $g \in G$ tal que $P(g) > Q(g)$, pois se fosse $P(g) \leq Q(g)$, para todo $g \in G$, teríamos, como $\sum_{g\in G}P(g) = \sum_{g\in G}Q(g) = 1$, $P = Q$.

Por definição, vale $\|P-Q\|_{VT} \geq |P(B)-Q(B)| = P(B)-Q(B)$. Seja $A \subset G$ tal que $\|P-Q\|_{VT} = |P(A)-Q(A)|$ e seja $A^c = G - A$. Então:

$$\begin{aligned} |P(A^c)-Q(A^c)| &= |(1-P(A))-(1-Q(A))| \\ &= |P(A)-Q(A)| \\ &= \|P-Q\|_{VT}. \end{aligned}$$

Seja $g \in G$ tal que $P(g) > Q(g)$. Subtituindo A por seu completar A^c se necessário, podemos supor que $g \in A$. Há duas possibilidades para $|P(A)-Q(Q)|$: $P(A)-Q(A)$ ou $Q(A)-P(A)$. Afirmamos que a primeira alternativa é a correta. De fato, $Q(A-\{g\})-P(A-\{g\}) = (Q(A)-Q(g))-(P(A)-P(g)) > Q(A)-P(A)$, e A não poderia ser máximo. De maneira análoga, se $h \in G$ for tal que $Q(h) > P(h)$, então temos $P(A-\{h\})-Q(A-\{h\}) > P(A)-Q(A)$ nova contradição. Segue que $A \subset B$. Porém da definição de B segue $P(B)-Q(B) \geq P(A)-Q(A)$, portanto $A = B$, e por um argumento semelhante, obtemos o restante da demonstração. □

Proposição 4.3.3. *Vale a identidade:*

$$\|P-Q\|_{VT} = \frac{1}{2}\|P-Q\|_1$$

para todas as probabilidades P, Q num grupo G.

Demonstração: Este resultado é uma consequência do lema anterior. Para mais detalhes consulte (STEINBERG, 2011) na página 136. □

Finalmente vamos introduzir a noção de caminhada aleatória em um grupo G. Sejam G um grupo finito e P uma probabilidade em G. Vamos denotar a k-ésima potência de P na álgebra $L(G)$ por P^{*k}.

Definição 4.3.5 (Caminhada aleatória)**.** *Sejam P e G como no parágrafo acima. A caminhada aleatória em G definida por P é a sequência de probabilidades $(P^{*k})_{k=0}^{\infty}$.*

Formalmente, consideramos uma sequência de variáveis aleatórias independentes X_1, X_2, ... com a mesma distribuição de probabilidade P, e seja Y_0 a variável aleatória com distribuição de probabilidade $\delta_{1_G} \in L(G)$. Defina a sequência $Y_k = X_k Y_{k-1}$, $k \geq 1$. A variável aleatoria Y_k fornece a posição do caminhante no k-ésimo passo da caminhada aleatória. Visto que a distribuição de probabilidade de Y_k é $P^{*k} * \delta_{1_G} = P^{*k}$, podemos identificar a caminhada aleatória como a sequência Y_0, Y_1, ..., Y_k, ... Sequências de variáveis aleatórias deste tipo são chamadas de cadeias de Markov.

Exemplo 4.3.1 (Caminhada aleatória simples)**.** *Sejam G um grupo finito, S um subconjunto simétrico de G, e Γ o grafo de Cayley de G com respeito a S. A caminhada*

aleatória simples em G é a caminhada aleatória em G definida pela probabilidade $\frac{1}{|S|}\delta_S$. O caminhante parte de $1_G \in G$, e se no k-ésimo passo ele se encontrar no vértice $g \in G$, escolhe-se $s \in S$ aleatoriamente e o cominhante vai para sg. Como, por definição de Γ, os vértices adjacentes a g são precisamente os elementos de G da forma sg, com $s \in S$, vemos que o formalismo das caminhadas aleatórias representa bem a idéia de um bêbado andando aleatoriamente pelo grafo Γ.

Exemplo 4.3.2 (Caminhada de Ehrenfest)**.** *Sejam A e B duas urnas contendo um total de n bolas. Supomos inicialmente que todas as bolas estão na urna A. Em cada unidade de tempo, uma das bolas é escolhida aleatoriamente e é trasferida para a outra urna. Podemos representar a configuração de bolas por uma n-upla $v = (c_1, ..., c_n) \in (\mathbb{Z}_2)^n$, onde $c_i = [0]$ se a i-ésima bola estiver na urna A e $c_i = [1]$ se a i-ésima bola estiver na urna B. A configuração inicial é $([0], ..., [0])$. Sejam $e_i \in (\mathbb{Z}_2)^n$ tais que a i-ésima coordenada é $[1]$ e as demais coordenadas são $[0]$. A operaração de mudar a i-ésima bola de uma urna a partir da configuração v corresponde a $e_i + v$. O processo estocástico de transferir bolas entre urnas corresponde à caminhada aleatória no grupo $(\mathbb{Z}_2)^n$ definida pela probabilidade:*

$$P = \frac{1}{n}(\delta_{e_1}, ..., \delta_{e_n}).$$

Este processo é conhecido como caminhada de Ehrenfest. Note que a caminhada de Ehrenfest é um exemplo de caminhada aleatória simples com Γ dado pelo grupo $G = (\mathbb{Z}_2)^n$ e $S = \{e_1, ..., e_n\} \subset G$.

Vamos agora considerar o problema de embaralhar um baralho como uma caminhada aleatória no grupo simétrico S_n. Consideremos um baralho com n cartas empilhadas. Um embaralhamento corresponde a reordenar a pilha de cartas, isto é, os elementos de S_n agem sobre as posições das cartas na pilha. Por exemplo, $(1...n)$ corresponde a mover a última carta para a primeira posição. Isto faz com que cada carta baixe uma posição na pilha: a primeira carta passa a ocupar a segunda posição, a segunda carta a terceira, e assim por diante. A seguir veremos alguns métodos de embaralhamento.

Exemplo 4.3.3 (Topo para a posição aleatória)**.** *O método "topo para posição aleatória"(tppa) leva a carta do topo do baralho a qualquer uma das posições aleatoriamente, ou seja, todas as posições são equiprováveis. O tppa é definido pela distribuição de probabilidade:*

$$P = \frac{1}{n}\delta_I + \sum_{i=2}^{n}\frac{1}{n}\delta_{(i\ i-1...1)},$$

onde $I \in S_n$ é a permutação identidade e $(i\ i-1...1)$ é o ciclo que leva a carta do topo para a i-ésima posição.

Exemplo 4.3.4 (Transposições aleatórias)**.** *O método das transposições aleatórias consiste em tomar uma carta com cada mão, podendo ser a mesma carta para ambas as mãos, e*

trocá-las de posição. Dados $1 \leq i, j \leq n$ *existem duas maneiras de escolher a transposição* (ij) *se* $i \neq j$*, e apenas uma maneira de escolher a mesma carta com ambas mãos. Logo as respectivas probabilidades são* $\frac{2}{n^2}$ *e* $\frac{1}{n^2}$*. Note que a probabilidade de escolher a mesma carta é* $\frac{1}{n}$*, já que há* n *maneiras de fazer uma tal escolha. Assim a transposição aleatória é uma caminhada aleatória em* S_n *definida pela probabilidade:*

$$Q(\sigma) = \begin{cases} \frac{1}{n} \text{ se } \sigma = I, \\ \frac{2}{n^2} \text{ se } \sigma \text{ é uma transposição}, \\ 0 \text{ nos demais casos.} \end{cases}$$

O próximo exemplo é um método bastante popular de embaralhamento.

Exemplo 4.3.5 (Método cortar e intercalar (C e I))**.** *Segundo este método, "corta-se" o baralho ao meio e coloca-se as duas pilhas de cartas lado a lado. Tomando uma pilha com cada mão, intercalam-se as pilhas fazendo cartas de cada pilha cair alternadamente sobre as cartas de outra pilha, se possivel uma a uma. Abaixo, discutiremos o método* C *e* I *proposto por Gilbert, Shannen e Reed.*

Considere um baralho com n cartas, e uma moeda. Jogamos a moeda n vezes. Se o número de caras obtido for k, o jogador pega as k cartas do topo com a mão direita e a pilha com as $n - k$ cartas restantes com a mão esquerda. Se X for a variável aleatória que conta o número de cartas na pilha do topo, então:

$$\text{Prob}\{X = k\} = \binom{n}{k}\frac{1}{2^n},$$

e dizemos que X é uma variável aleatória binomial. Observe que é maior a probabilidade de o corte ocorrer próximo ao meio do baralho. Na continuação, o jogador deixa cair uma carta de cada mão, de maneira que se ele tiver a cartas na mão direita e b cartas na mão esquerda, então a probabilidade de deixar cair uma carta da mão direita é $\frac{a}{a+b}$, e a probabilidade de deixar cair uma carta da mão esquerda é $\frac{b}{a+b}$, ou seja, as probabilidades são proporcionais ao número de cartas em cada mão. Observe que neste modelo pode ocorrer $k = 0$ ou $k = n$, casos em que não há reordenamento do baralho. Porém a probabilidade de tais eventos é 2^{-n}, que é relativamente pequena.

Definição 4.3.6 (Sequência ascendente)**.** *Uma sequência ascendente em uma permutação* σ *de* $\{1, ..., n\}$ *é uma subsequência crescente de comprimento máximo na sequência* $\sigma(1)$*, ...,* $\sigma(n)$*.*

Exemplo 4.3.6. *Seja* $\sigma = (4\ 6\ 1)(2\ 5)(3\ 7) \in S_7$*. Então a sequência* $\sigma(1)$*, ...,* $\sigma(n)$ *é* $4, 5, 7, 6, 2, 1, 3$*, e uma sequência ascendente em* σ *é* $4, 5, 7$*.*

Vamos supor que é feito um embaralhamento pelo método C e I. As cartas nas posições $1, ..., k$ *são intercaladas com as cartas nas posições* $k+1, ..., n$*, com as ordens de cada pilha preservadas. Isto quer dizer que se a k-ésima carta da primeira pilha cai primeiro, ela pode ser seguida de uma carta da primeira ou segunda pilha, porém a primeira carta a cair da segunda pilha será a n-ésima. Assim, se ao final do embaralhamento a permutação das posições for* σ*, teremos examente duas sequências ascendentes:* $\sigma(1)$*, ...,* $\sigma(k)$ *e* $\sigma(k+1)$*, ...,* $\sigma(n)$*. Como consequência, se P for distribução de probabilidade em* S_n*, então* $P(\sigma) = 0$ *a menos* σ *tenha no máximo duas sequências ascendentes (é razoável supormos a situação do parágrafo anterior). Faremos a seguir o cálculo da probabilidade de* σ *ocorrer, quando* σ *tem exatamente duas sequências ascendentes, bem como da probabilidade da permutação ser a identidade.*

Suponhamos que fez-se um corte e a pilha de cartas do topo tem k cartas. Há n posições para por estas cartas e, uma vez escolhidas estas posições com ordenamento preservado, as posiçẽs de todas as cartas são conhecidas. logo há $\binom{n}{k}$ *permutações possíveis. Afirmamos que tais permutações são equiprováveis.*

Fixemos uma σ *como no parágrafo precedente. De acordo com nosso modelo, a probabilidade de uma carta provir da pilha do topo, seja T tal evento, é* $\frac{a}{a+b}$*, e a probabilidade da carta provir da base, chamemos este evento B, é* $\frac{b}{a+b}$*, onde* $a = k$ *e* $b = n - k$ *no nosso caso. Logo a probabilidade de ocorrer T para a primeira carta é* $\frac{k}{n}$*, e de ocorrer B para a primeira carta é* $\frac{n-k}{n}$*. Para a segunda carta, o denominador será* $n-1$ *e o numerador será* $k-1$ *ou* $n-k-1$*, dependendo da ocorrência de T ou de B para a primeira carta. Continuando para cada posição, os denominadores serão* n*,* $n-1$*,* $n-2$*, ..., 2, 1, e os numeradores serão precisamente os números* k*,* $k-1$*, ..., 1 e* $n-k$*,* $n-k-1$*, ..., 1. Logo a probabilidades de qualquer sequência de T′s ou de B′s é* $\frac{k!(n-k)!}{n!} = \frac{1}{\binom{n}{k}}$*. Portanto as sequências de T′s e B′s são todas equiprováveis, dado que o corte do baralho ocorre na posição K.*

As permutações correspondentes às sequências de T′s e B′s contêm duas sequências ascendentes, sendo uma de comprimento k e a outra de comprimento $n-k$*. A probabilidade de o corte ocorrer na k-ésima posição segue, como vimos, uma distribuição binominal, sendo dada por* $\binom{n}{k} \cdot \frac{1}{2^n}$*. Logo, se* $1 \leq k \leq n-1$ *e* $\sigma \neq I$ *é uma permutação com sequências ascendentes* $\sigma(1)$*, ...,* $\sigma(k)$*,* $\sigma(k+1)$*, ...,* $\sigma(n)$*, a probabilidade de obtermos* σ *após um corte e uma intercalação é*

$$\binom{n}{k} \cdot \frac{1}{2^n} \cdot \frac{1}{\binom{n}{k}} = \frac{1}{2^n}.$$

Se o corte ocorrer na posição k, qualquer que seja k, a probabilidade de termos $\sigma = I$ *é* $\frac{1}{2^n}$*, pois I corresponde a uma dentre* 2^n *possibilidades, qual seja* $\underbrace{T \cdots T}_{k} \underbrace{B \cdots B}_{n-k}$*. Como k*

varia de 0 *a* n*, a probabilidade de de obtermos a permutação identidade (isto é, de não embaralhamos o baralho) é* $\dfrac{n+1}{2^n}$*. Deste modo concluímos a modelagem do método* C *e* I *como uma caminhada aleatória no grupo* S_n*.*

Proposição 4.3.4. *O método de corte e intercalação de Gilbert, Shannon e Reed corresponde a uma caminhada aleatória no grupo* S_n *definida pela distribução de probabilidade:*

$$P(\sigma) = \begin{cases} \frac{n+1}{2^n} \text{ se } \sigma = I, \\ \frac{1}{2^n} \text{ se } \sigma \text{ tiver exatamente duas sequências ascendentes,} \\ 0 \text{ nos demais casos.} \end{cases}$$

Definição 4.3.7 (Caminhada ergódica)**.** *Uma caminhada aleatória em um grupo* G *definida pela probabilidade* P *é ergódica se exister um inteiro* $N > 0$ *tal que* $P^{*N}(g) > 0$ *para todo* $g \in G$*, isto é,* $Sup\left(P^{*N}\right) = G$*.*

Proposição 4.3.5. *Seja* P *uma probabilidade definida em um grupo finito* G *e suponha que*

(a) $P(1_G) > 0$ *e*

(b) $Sup\,(P)$ *gera o grupo* G*.*

Então a caminhada aleatória definida por P *é ergódica.*

Demonstração: Seja $S = \mathrm{Sup}\,(P)$. Note que $S^k \subset S^{k+1}$, $\forall k \geq 0$, pois $1_G \in S$. Como S gera G, existe $N > 0$ tal que $S^N = G$. Mas S^N é o suporte de P^{*N}, ou seja, $P^{*N}(g) > 0$, para todo $g \in G$. □

Usando a proposição acima, vê-se, de maneira relativamente simples, que todos os métodos de embaralhamento vistos até agora correspondem a caminhadas aleatórias ergódicas.

Definição 4.3.8 (Convergência de probabilidades)**.** *Uma sequência de probabilidades* (P_n) *no grupo finito* G *converge para a probabilidade* P *se, para todo* $\varepsilon > 0$*, existe* $N > 0$ *tal que* $\|P_n - P\|_{VT} < \varepsilon$ *se* $n \geq N$*.*

Teorema 4.3.1. *Seja* $(P^{*k})_{k=0}^{\infty}$ *uma caminhada aleatória ergódica em um grupo finito* G *definida pela probabilidade* P*. Então a sequência* (P^{*k}) *converge para a distribuição uniforme* U*.*

O teorema acima implica que uma caminhada aleatória ergódica num grupo finito por ser usada para gerar elementos deste grupo aleatoriamente. A demonstração para

o caso G abeliano será feita posteriormente. O caso geral é tratado, por exemplo, em: (CECCHERINI-SILBERSTEIN; SCARABOTTI; TOLLI, 2008).

A seguir, dentre outros coisas, definiremos o espectro de uma caminhada aleatória e apresentaremos o lema da cota superior.

Sejam G um grupo finito e P uma distribuição de probabilidades em G. Associado a P está o operador convolução por P:

$$\begin{aligned} M : L(G) &\longrightarrow L(G) \\ a &\longmapsto P * a \end{aligned}$$

e, em particular, vale que $M^k(\delta_{1_G}) = P^{*k}$, ou seja, estudar as potências de M é equivalente a estudar a caminhada aleatória em G definida por P. O principal ingrediente no estudo qualitativo das potências de um operador linear é o seu espectro.

Definição 4.3.9 (Espectro da caminhada)**.** *O espectro da caminhada aleatória no grupo finito G definida pela probabilidade P é o conjunto dos autovalores (levando em conta suas multiplicidades) do operador $M : L(G) \longrightarrow L(G)$ dado por $M(a) = P * a$. O espectro será denotado por spec(P).*

É facil provar que a distribução uniforme U é autovetor com autovalor 1 de qualquer operador M do tipo acima. Também é simples verificar que todo autovalor de M tem módulo no máximo 1.

Teorema 4.3.2. *Seja G um grupo abeliano finito, e seja P uma distribuição de probabilidade em G. Temos que spec$(P) = \{\widehat{P}(\chi) \ : \ \chi \in \widehat{G}\}$, e a multiplicidade de $\lambda \in$ spec(P) é o número de caráteres χ para os quais $\widehat{P}(\chi) = \lambda$. Uma base ortonormal para o auto-espaço associado a λ é formada pelos caráteres χ tais que $\widehat{P}(\chi) = \lambda$.*

Demonstração: Segue imediatamente da Proposição 3.3.7. □

Exemplo 4.3.7. *Consideremos a caminhada de Ehrenfest, introduzida no Exemplo 4.3.2. Vamos definir $\alpha : (\mathbb{Z}_2)^n \longrightarrow 2^{\{1,\ldots,n\}}$, onde $2^{\{1,\ldots,n\}}$ denota o conjunto das partes de $\{1, ..., n\}$, por $\alpha(c_1, ..., c_n) = \{i \ : \ c_i = [1]\}$. Dado $Y \in 2^{\{1,\ldots,n\}}$, definimos:*

$$\begin{aligned} \chi_Y : (\mathbb{Z}_2)^n &\longrightarrow \mathbb{C} \\ v &\longmapsto (-1)^{|\alpha(v)\cap Y|} \end{aligned}$$

e observamos que $\widehat{G}$ é precisamente $\{\chi_Y \ : \ Y \in 2^{\{1,\ldots,n\}}\}$. Visto que

$$\chi_Y(e_i) = \begin{cases} -1 \text{ se } i \in Y, \\ 1 \text{ se } i \notin Y. \end{cases}$$

temos:

$$\begin{aligned}\widehat{P}(\chi_Y) &= 2^n\langle P, \chi_Y\rangle \\ &= \sum_{g\in(\mathbb{Z}_2)^n} P(g)\overline{\chi_Y(g)} \\ &= \frac{1}{n}\left[\sum_{i\in Y}\chi_Y(e_i) + \sum_{i\notin Y}\chi_Y(e_i)\right] \\ &= \frac{1}{n}\left[-|Y| + (n-|Y|)\right] \\ &= n - \frac{2|Y|}{n}.\end{aligned}$$

Concluímos que os autovalores da caminhada de Ehrenfest são

$$\lambda_j = 1 - \frac{2j}{n},\ 0 \leq j \leq n$$

e que os respectivos multiplicidades são $\binom{n}{j}$*, ou seja, o número de subconjuntos de* $\{1, ..., n\}$ *com* j *elementos.*

Passemos à discussão sobre o lema da cota superior de Diaconis e Shahshahani. Precisaremos do seguinte resultado.

Lema 4.3.3. *Seja* $\|\ \|$ *a norma induzida pelo produto interno em* $L^2(G)$*. Tem-se que* $\|f\|_1 \leq |G|\|f\|$*,* $\forall f \in L^2(G)$*.*

Demonstração: Sejam χ_1 o carácter trivial e $|f|$ a função definida por $|f|(g) = |f(g)|$. Segue que $\|f\|_1 = |G|\langle|f|, \chi_1\rangle \leq |G|\|f\|\|\chi_1\| = |G|\|f\|$. □

Teorema 4.3.3 (Lema da cota superior)**.** *Seja* G *um grupo abeliano finito e seja* $\widehat{G}^* = \{\chi \in \widehat{G}\ :\ \chi \neq \chi_1\}$*, onde* χ_1 *é o caráter trivial. Então, dada uma probabilidade* Q *em* G*, tem-se:*

$$\|Q - U\|_{TV}^2 \leq \frac{1}{4}\sum_{\chi\in\widehat{G}^*}|\widehat{Q}(\chi)|^2.$$

Demonstração: Usando a Proposição 4.3.3 e o lema anterior, obtemos:

$$\|Q - U\|_{VT}^2 = \frac{1}{4}\|Q - U\|_1^2 \leq \frac{1}{4}|G|^2\|Q - U\|^2. \tag{4.3.1}$$

E usando a identidade de Plancherel (Proposição 3.3.5), deduzimos:

$$|G|^2\|Q - U\|^2 = |G|\|\widehat{Q} - \widehat{U}\|^2 = |G|\left[\langle\widehat{Q}, \widehat{Q}\rangle - 2\langle\widehat{Q}, \widehat{U}\rangle + \langle\widehat{U}, \widehat{U}\rangle\right]. \tag{4.3.2}$$

Mas $\widehat{U} = \delta_{\chi_1}$ e temos também que, se P é uma probabilidade em G, $\widehat{P}(\chi_1) = 1$. Concluímos que:

$$\langle\widehat{U}, \widehat{U}\rangle = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\widehat{U}(\chi)\overline{\widehat{U}(\chi)} = \frac{1}{|G|},$$

$$\langle \widehat{Q}, \widehat{U} \rangle = \frac{\widehat{Q}(\chi_1)}{|G|} = \frac{1}{|G|} \text{ e que}$$

$$\langle \widehat{Q}, \widehat{Q} \rangle = \frac{1}{|G|} + \frac{1}{|G|} \sum_{\chi \in \widehat{G}^*} \widehat{Q}(\chi)\overline{\widehat{Q}(\chi)}.$$

Subtituindo estas conclusões em (4.3.2), obtemos:

$$|G|^2 \|Q - U\|^2 = \sum_{\chi \in \widehat{G}^*} |\widehat{Q}(\chi)|^2$$

e o resultado segue da desigualdade (4.3.1). □

Corolário 4.3.1. *Sejam G um grupo abeliano finito e P uma probabilidade em G. Então:*

$$\|P^{*k} - U\|_{VT}^2 \leq \frac{1}{4} \sum_{\chi \in \widehat{G}^*} |\widehat{P}(\chi)|^{2k}.$$

Observação 4.3.1. $|\widehat{P}(\chi)| = \left| \sum_{g \in G} P(g)\overline{\chi(g)} \right| \leq \sum_{g \in G} P(g)|\overline{\chi(g)}| = \sum_{g \in G} P(g) = 1$. *Se P define uma caminhada aleatória ergódica, então $\widehat{P}(\chi) < 1$ se $\chi \neq \chi_1$. De fato, $\widehat{P}(\chi) = 1$ implica $\widehat{P}^N(\chi) = 1$. Mas:*

$$\widehat{P}^N(\chi) = |G|\langle P^{*N}, \chi \rangle = \sum_{g \in G} P^{*N}(g)\overline{\chi(g)},$$

donde $\widehat{P}^N(\chi)$ é a soma convexa de pontos do círculo $|z| = 1$ com coeficientes todos positivos e ao menos dois pontos distintos. Tal soma está no interior do círculo.

Nosso próximo passo é, aplicando o lema da cota superior, provar parcialmente um interessante teorema devido a Diaconis, entretanto precisaremos de dois lemas que enunciaremos a seguir. As respectivas demonstrações serão omitidas, pois são simples e não utilizam nossas construções.

Lema 4.3.4. *Suponha que $1 \leq j \leq \left\lfloor \frac{n+1}{2} \right\rfloor$, onde $\lfloor x \rfloor$ denota o maior inteiro menor ou igual ao número real x. Então*

$$\binom{n}{j-1} \leq \binom{n}{j}.$$

Lema 4.3.5. *Se $0 \leq x \leq 1$, então $(1-x)^{2k} \leq e^{-2kx}$, para todo $k \geq 0$.*

Teorema 4.3.4 (Diaconis)**.** *Seja P a distribuição de probabilidade no grupo $(\mathbb{Z}_2)^n$ dada por:*

$$P = \frac{1}{n+1} \left(\delta_{(0,\ldots,0)} + \delta_{e_1} + \cdots + \delta_{e_n} \right)$$

e seja c uma constante positiva. Se $k \geq (n+1)(\log n + c)$, então vale a desigualdade:

$$\|P^{*k} - U\|_{VT}^2 \leq \frac{1}{2}(e^{e^{-c}} - 1).$$

Por outro lado, se $k \leq \dfrac{(n+1)(\log n - c)}{4}$, *onde* $0 < c < \log n$ *e* n *é suficientemente grande, então*

$$\|P^{*k} - U\|_{VT} \geq 1 - 20e^{-c}.$$

(log *denota o logaritmo na base* e).

Demonstração: Sejam $Y \subset \{1, ..., n\}$ e χ_Y o caráter de $(\mathbb{Z}_2)^n$ introduzido no Exemplo 4.3.7. Usando o argumento visto neste exemplo, obtemos:

$$\widehat{P}(\chi_Y) = \frac{n+1-2|Y|}{n+1} = 1 - \frac{2|Y|}{n+1}.$$

Note que $\chi_1 = \chi_\phi$. De acordo com o Corolario 4.3.1, temos:

$$\|P^{*k} - U\| \leq \frac{1}{4}\sum_{j=1}^{n}\binom{n}{j}\left(1 - \frac{2j}{n+1}\right)^{2k},$$

onde estamos usando o fato de haver exatamente $\binom{n}{j}$ subconjuntos Y com j elementos. Vamos escrever:

$$\|P^{*k} - U\| \leq \frac{1}{4}\left[\sum_{j=1}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n}{j}\left(1 - \frac{2j}{n+1}\right)^{2k} + \sum_{j=\lfloor\frac{n+1}{2}\rfloor+1}^{n}\binom{n}{j}\left(1 - \frac{2j}{n+1}\right)^{2k}\right] \tag{4.3.3}$$

Fazendo a substituição $l = n + 1 - j$ no segundo somatório, obtemos:

$$\begin{aligned}\sum_{j=\lfloor\frac{n+1}{2}\rfloor+1}^{n}\binom{n}{j}\left(1 - \frac{2j}{n+1}\right)^{2k} &= \sum_{l=1}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n}{n+1-l}\left(\frac{2l}{n+1} - 1\right)^{2k} \\ &= \sum_{l=1}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n}{l-1}\left(1 - \frac{2l}{n+1}\right)^{2k} \\ &\leq \sum_{l=1}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n}{l}\left(1 - \frac{2l}{n+1}\right)^{2k},\end{aligned}$$

Aqui usamos o primeiro dos dois lemas acima. Portanto (4.3.3) pode ser reescrita como:

$$\|P^{*k} - U\|_{VT}^2 \leq \frac{1}{2}\sum_{j=1}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n}{j}\left(1 - \frac{2j}{n+1}\right)^{2k}$$

Observemos que:

$$\binom{n}{j} = \frac{n!}{j!(n-j)!} \leq \frac{n^j}{j!}.$$

Usando o segundo dos dois lemas anteriores, podemos escrever:

$$\|P^{*k} - U\|_{VT}^2 \leq \frac{1}{2}\sum_{j=1}^{\lfloor\frac{n+1}{2}\rfloor}\frac{n^j}{j!}e^{-\frac{4kj}{n+1}}$$

Supondo $k \geq \dfrac{(n+1)(\log n + c)}{4}$, obtemos $e^{\frac{-4kj}{n+1}} \leq e^{-j\log n - jc} = \dfrac{e^{-jc}}{n^j}$. Portanto,

$$\begin{aligned} \|P^{*k} - U\|_{VT}^2 &\leq \frac{1}{2}\sum_{j=1}^{\lfloor \frac{n+1}{2} \rfloor} \frac{1}{j!} e^{-jc} \\ &\leq \frac{1}{2}\sum_{j=1}^{\infty} \frac{(e^{-c})^j}{j!} \\ &\leq \frac{1}{2}(e^{e^{-c}} - 1). \end{aligned}$$

Como desejado. □

Observação 4.3.2. *A distribuição de probabilidade considerada no teorema acima define a chamada caminhada de Eherenfest preguiçosa: existe uma probabilidade não nula de todas as bolas permanecerem nas urnas onde estão numa dada unidade de tempo.*

Observação 4.3.3. *Diaconis e Shahshahani provaram uma versão do lema da cota superior para grupos finitos arbitrários (o leitor interessado pode consultar (DIACONIS; SHAHSHAHANI, 1981) ou (DIACONIS, 1988)). É interessante comparar as cotas obtidas para $\|P^{*k} - U\|_{VT}$, isto é, para a velocidade com que P^{*k} converge para U. Por exemplo, no embaralhamento pelo método de corte e intercalação, $k = 7$ já torna o baralho praticamente aleatório.*

Finalizaremos mostrando que toda caminhada aleatória ergódica num grupo abeliano finito converge para a distribuição uniforme.

Teorema 4.3.5. *Seja P uma distribuição de probabilidade em um grupo finito abeliano tal que a caminhada aleatória (P^{*n}) é ergódica. Então $P^{*n} \longrightarrow U$.*

Demonstração: De acordo com o Corolário 4.3.1 temos

$$\|P^{*k} - U\|_{VT}^2 \leq \frac{1}{4}\sum_{\chi \in \widehat{G}^*} |\widehat{P}(\chi)|^{2k}.$$

Logo é suficiente verificarmos que $|\widehat{P}(\chi)| < 1$, para todo caráter não trivial χ de G. Como $|\widehat{P}(\chi)| < 1 \Leftrightarrow |\widehat{P}^m(\chi)| < 1$, para algum $m > 0$, podemos supor que $P(g) > 0$, para todo $g \in G$, pela ergodicidade da caminhada. A desigualdade

$$|\widehat{P}(\chi)| = |G||\langle P, \chi\rangle| = \left|\sum_{g\in G} P(g)\overline{\chi(g)}\right| \leq \sum_{g\in G} \left|P(g)\overline{\chi(g)}\right|$$

é uma igualdade se, e somente se, para todo $g \in G$, $P(g)\overline{\chi(g)}$ for múltiplo não negativo de um mesmo número complexo (veja o lema 6.3.1 de (STEINBERG, 2011)). Visto que $P(1_G) > 0$, $\overline{\chi(1_G)} = 1$ e existe $g \in G$ tal que $\overline{\chi(g)} \neq 1$, temos que $P(1_G)\overline{\chi(1_G)} = P(1_G)$ e $P(g)\overline{\chi(g)}$ não podem ser multipos não-negativos de um mesmo número complexo. (Lembre que $p(g) > 0$ e $\overline{\chi(g)}$ é raiz da unidade). Concluímos que a desigualdade acima é estrita, o que finaliza a demonstração. □

REFERÊNCIAS

ASH, R. B. *Abstract Algebra: the basic graduate year*. [S.l.: s.n.], 2000. Citado na página 67.

CECCHERINI-SILBERSTEIN, T.; SCARABOTTI, F.; TOLLI, F. *Harmonic analysis on finite groups: representation theory, Gelfand pairs and Markov chains*. [S.l.]: Cambridge University Press, 2008. v. 108. Citado na página 75.

DIACONIS, P. Group representations in probability and statistics. *Lecture Notes-Monograph Series*, JSTOR, v. 11, p. i–192, 1988. Citado na página 79.

DIACONIS, P.; SHAHSHAHANI, M. Generating a random permutation with random transpositions. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, Springer, v. 57, n. 2, p. 159–179, 1981. Citado na página 79.

FULTON, W.; HARRIS, J. *Representation theory: a first course*. [S.l.]: Springer Science & Business Media, 2013. v. 129. Citado na página 7.

HIGMAN, G. The units of group-rings. *Proceedings of the London Mathematical Society*, Wiley Online Library, v. 2, n. 1, p. 231–248, 1940. Citado na página 65.

JAMES, G.; LIEBECK, M. W. *Representations and characters of groups*. [S.l.]: Cambridge University Press, 2001. Citado na página 7.

SERRE, J.-P. *Linear representations of finite groups*. [S.l.]: Springer Science & Business Media, 2012. v. 42. Citado na página 7.

STEINBERG, B. *Representation Theory of Finite Groups: An Introductory Approach*. [S.l.]: Springer Science & Business Media, 2011. Citado 7 vezes nas páginas 7, 22, 23, 38, 41, 70 e 79.

TERRAS, A. *Fourier analysis on finite groups and applications*. [S.l.]: Cambridge University Press, 1999. Citado 2 vezes nas páginas 7 e 37.