Caracteres e Algoritmo de Shor *

Wagner R. Fortes **
Luiz Mariano P. de Carvalho ‡

Resumo

Este trabalho surgiu com o intuito de compreender algumas das ferramentas teóricas que compõem o algoritmo de Shor, em especial a transformada quântica de Fourier. Nele temos uma introdução à teoria das representações e caracteres de grupos, que têm como base a teoria de grupos e álgebra linear.

Abstract

This research had arisen in order to understand some theoretical tools that compose Shor's algorithm, more specifically the quantum Fourier transform. We address an introduction to representation theory and group characters, both are based on group theory and linear algebra.

* *Trabalho apresentado em uma versão resumida como poster no VIII Encontro de Modelagem Computacional e publicado nos anais deste mesmo encontro, Novembro de 2005, IPRJ-UERJ, Nova Friburgo-RJ*

Palavras chave: Teoria das Representações, Caracteres, Transformada Discreta de Fourier

** Aluno de Iniciação Científica, Bolsista do CNPq, Departamento de Matemática Aplicada, IME/UERJ, wfortes@gmail.com

‡ Departamento de Matemática Aplicada, IME/UERJ, luizmc@ime.uerj.br

1 Introdução

Inspirado pela potencialidade da computação quântica - que provavelmente terá profundas conseqüências, não só para a tecnologia, mas também para a teoria da informação - estudamos o algoritmo de Shor, famoso algoritmo quântico para fatoração de números inteiros, que foi criado em 1994 pelo físico norteamericano Peter Shor. Este algoritmo é um paradigma do que a computação quântica promete, pois representa um ganho inimaginável de velocidade de processamento que virá a modificar bruscamente os sistemas criptográficos de segurança, que estão fundamentados na fatoração de grandes números (problema muito difícil para computadores clássicos), podendo deixar segredos de estado, e transações financeiras vulneráveis.

Veja na tabela abaixo a comparação de tempo de fatoracão entre um algoritmo clássico e o algoritmo de Shor.

Comprimento do número a ser fatorado (em bits)	*Tempo de fatoração por algoritmo clássico*	*Tempo de fatoração com o algoritmo de Shor*
512	4 *dias*	34 *segundos*
1024	100 *mil anos*	4,5 *minutos*
2048	100 *mil bilhões de anos*	36 *minutos*
4096	100 *bilhões de quatrilhões de anos*	4,8 *horas*

Tabela 1: http://www.comciencia.br/reportagens/nanotecnologia/nano16.htm

Este e outros algoritmos quânticos que produzem resultados muito mais eficientes do que os produzidos pelos computadores clássicos estão para promover uma revolução na computação e na matemática pura. Com este incentivo aprofundamos nosso estudo em alguns aspectos do algoritmo que têm papel fundamental em seu desenvolvimento, mas para que possamos entender conceitos mais avançados, é importante que saibamos retornar e estudar com afinco os conceitos mais simples.

A Transformada Quântica de Fourier está freqüentemente presente em algoritmos quânticos. Para compreendê-la, introduziremos uma importante ferramenta: Teoria das Representações e Caracteres de grupos. Entretanto, notamos que tal ferramenta não se limita apenas às relações com a Transformada de Fourier, revelando, sobretudo, um rico e profundo estudo relacionando diversas áreas da matemática pura e aplicada. Através do desenvolvimento desse trabalho, esperamos reunir conteúdos que auxiliem trabalhos futuros. Algumas demonstrações e definições foram omitidas neste artigo, e podem ser encontradas nas obras [1] e [2] listadas na referência.

No segundo capítulo apresentamos o algoritmo de Shor e a Transformada de Fourier, depois veremos representações de grupos, FG-módulos, caracteres e seu produto interno (que são construídos pelas representações de grupos e originam grandes resultados quando utilizamos os conceitos de FG-módulo) e nossas conclusões que fazem as devidas conexões entre os caracteres e o algoritmo de Shor.

Por conveniência, em alguns casos, representaremos uma função, por exemplo, $\rho(x)$ por $x\rho$.

A não ser que se diga o contrário, neste trabalho estamos considerando G e H como grupos finitos, V,U e W como espaços vetoriais e um corpo F, que pode ser $\mathbb{R}$ ou $\mathbb{C}$.

2 Algoritmo de Shor e Transformada Quântica de Fourier

O algoritmo de Shor, é um algoritmo para um computador quântico que encontra os fatores primos de um número composto N em um número de passos que é polinomial em $\lceil \log_2 N \rceil$[1], isto é de grande importância pois não existe algoritmo clássico capaz de fatorar números em tempo polinomial em n, como faz o algoritmo de Shor. Este processo de fatoração pode ser reduzido ao cálculo de ordem[2] de um número x menor que N, escolhido aleatoriamente como pode ser visto em [3].

No nível quântico, todos os valores de j que produzem $x^j \equiv 1 \pmod N$ são "conhecidos". Mas esta informação não está disponível no nível clássico. E para descobrir eficientemente o período de uma função utilizamos a transformada de Fourier, que transforma uma função de período r em uma nova função de período proporcional a $\frac{1}{r}$, o que faz a diferença para a determinação de r, como pode ser visto em [3].

A transformada de Fourier de uma função $F : \{0, \ldots, N-1\} \to \mathbb{C}$
é uma nova função $\widetilde{F} : \{0, \ldots, N-1\} \to \mathbb{C}$ definida por

$$\widetilde{F}(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j \frac{k}{N}} F(j) \tag{2.1}$$

Ao invés de aplicar a transformada discreta de Fourier(DFT) em uma função iremos aplicá-la em um estado da base computacional. Então aplicando a DFT em um estado da base computacional $\{\mid 0\rangle, \ldots, \mid N-1\rangle\}$ temos

$$DFT(\mid k\rangle) = \mid \psi_k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j \frac{k}{N}} \mid j\rangle \tag{2.2}$$

onde o conjunto $\{\mid \psi_k\rangle : k = 0, \ldots, N-1\}$ forma uma nova base ortonormal,
assim $\langle \psi'_k \mid \psi_k \rangle = \delta_{k'k}$. Agora definimos a transformada de Fourier inversa que é similar a equação (2.2), porém com um sinal de menos no expoente. E como a DFT é um operador linear unitário, então DFT^{-1}=$\mathrm{DFT}^{\dagger}$[3].

E para que possamos entender seu funcionamento começaremos agora nosso estudo de representações e caracteres de grupos.

[1] Menor inteiro maior que $log_2 N$.

[2] A ordem de um número x módulo N é um número j que é o menor natural diferente de zero tal que $x^j \equiv 1 \pmod N$.

[3] $DFT^{\dagger} = \overline{DFT}^T$

3 Representações de grupos

Uma representação de um grupo nos dá uma forma de relacionar um grupo finito qualquer com um conjunto de matrizes. Mais precisamente, a representação de um grupo é um homomorfismo[4]
$\rho : G \to$ GL(n,F), onde n é o grau de ρ e GL(n,F) é o grupo de matrizes invertíveis $n \times n$ com entradas em F, em outras palavras, uma função $\rho : G \to$GL(n,F) é uma representação se e somente se $(gh)\rho = (g\rho)(h\rho), \quad \forall g, h \in G$.

Durante nosso curso de graduação, na maioria das vezes, não conseguimos perceber a importância de um homomorfismo e nem vemos sua aplicabilidade, estando sempre em maior destaque os isomorfismos[5]. Porém neste trabalho poderemos perceber o poder de um homomorfismo bem como sua aplicabilidade.

E como conseqüência de nossa definição temos $g^{-1}\rho = (g\rho)^{-1}$, pois

$$I_n = (e_G)\rho = (gg^{-1})\rho = (g\rho)(g^{-1}\rho) \Longrightarrow (g\rho)^{-1}I_n = (g^{-1}\rho) \Longrightarrow g^{-1}\rho = (g\rho)^{-1}.$$

Note que se definirmos nossa função ρ como $g\rho = I_n$, para todo g pertencente G onde I_n é a matriz identidade $n \times n$, então

$$(gh)\rho = I_n = I_nI_n = (g\rho)(h\rho), \quad \forall g, h \in G$$

ou seja, ρ é uma representação de G. Com isso verificamos que todo grupo tem pelo menos uma representação.

Vejamos alguns exemplos bem simples de representações de grupos cíclicos.

Exemplo 3.1. *Seja G o grupo cíclico* $C_3 =< a : a^3 = e_G >= \{e_g, a, a^2\}$[6]

(I)Uma representação possível é $\rho : C_3 \to GL(2, \mathbb{C})$ *onde*

$$e_G\rho = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad a\rho = \begin{pmatrix} \frac{-1}{2} & \frac{\sqrt{3}i}{2} \\ \frac{\sqrt{3}i}{2} & \frac{-1}{2} \end{pmatrix}; \qquad a^2\rho = \begin{pmatrix} \frac{-1}{2} & \frac{-\sqrt{3}i}{2} \\ \frac{-\sqrt{3}i}{2} & \frac{-1}{2} \end{pmatrix}.$$

(II)Uma outra representação possível para o mesmo grupo é $\sigma : C_3 \to GL(2, \mathbb{R})$ *onde*

$$e_G\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad a\sigma = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}; \qquad a^2\sigma = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

[4]Se G e H são grupos, então um homomorfismo de G em H é uma função $\vartheta : G \to H$ que satisfaz

$$(g_1g_2)\vartheta = (g_1\vartheta)(g_2\vartheta) \quad \forall g_1, g_2 \in G.$$

[5]O isomorfismo é um homomorfismo bijetivo.

[6]Grupo gerado quando operamos a com ele mesmo, onde a tem ordem 3.

Exemplo 3.2. *Seja agora G o grupo cíclico* $C_2 =< a : a^2 = e_G >= \{e_G, a\}$[7] *Peguemos uma representação* $\psi : C_2 \to GL(3, \mathbb{R})$ *definida*

$$e_G\psi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \qquad a\psi = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Diremos que duas representações ρ e σ de mesmo grau, são equivalentes se
$g\sigma = T^{-1}(g\rho)T$, para algum T, onde T é uma matriz $n \times n$ invertível e para todo g∈G. Com isso podemos encontrar uma nova representação σ a partir de uma representação ρ, pois

$$(gh)\sigma = T^{-1}((gh)\rho)T = T^{-1}(g\rho)TT^{-1}(h\rho)T = (g\sigma)(h\sigma).$$

para todo $g, h \in G$.

Através de nossa definição, representações equivalentes formam uma classe de equivalência.

Exemplo 3.3. *Seja G=*C_3 *e consideremos a representação de* ρ *de G que aparece no exemplo (3.1(I)). Então*

$$a\rho = \begin{pmatrix} \frac{-1}{2} & \frac{\sqrt{3}i}{2} \\ \frac{\sqrt{3}i}{2} & \frac{-1}{2} \end{pmatrix}$$

E peguemos uma matriz

$$T = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{-1}{2} \end{pmatrix} \quad \textit{cuja inversa é} \quad T^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

E com isso obtemos uma representação σ *de* C_3 *fazendo*

$$a\sigma = T^{-1}a\rho T = \begin{pmatrix} e^{\frac{2\pi i}{3}} & 0 \\ 0 & e^{-\frac{2\pi i}{3}} \end{pmatrix}$$

A verificação de que σ *de fato é uma representação é bem simples neste caso.*
Assim σ *e* ρ *são equivalentes.*

4 FG-Módulos

Lembremos antes que um espaço vetorial V é construído utilizando-se um grupo abeliano G_0 e um corpo qualquer F, onde a operação intrínseca de G_0 é a soma (representamos como $(G_0,+)$) e definimos uma multiplicação entre os elementos do grupo G_0 e o corpo F, dessa forma podemos representar simbolicamente um espaço vetorial V como V($(G_0,+)$,F,$\cdot$).

[7] Grupo gerado quando operamos a com ele mesmo, onde a tem ordem 2.

Em geral o espaço vetorial mais conhecido é o $\mathbb{R}^n$, onde o grupo abeliano G_0 é o produto cartesiano $\underbrace{\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}}_{n \quad fatores} = \mathbb{R}^n$ com a operação de soma e o corpo F poderá ser $\mathbb{R}$ ou $\mathbb{C}$, que costumamos representar como $\mathbb{R}^n(\mathbb{R})$ ou $\mathbb{R}^n(\mathbb{C})$ respectivamente.

Com isso, diremos que o espaço vetorial V sobre F é um FG-módulo se o produto vg (v $\in V$, $g, h \in G$), onde o grupo G não é necessariamente o grupo abeliano G_0 que constrói o espaço vetorial V, obedece aos seguintes axiomas definidos em uma base ordenada $\mathfrak{B} = [v_1, v_2, \ldots, v_n]$ de V:

1. $v_i g \in V$;
2. $v_i(gh) = (v_i g)h$;
3. $v_i e_G = v_i$;
4. $(\lambda_1 v_1 + \ldots + \lambda_n v_n)g = \lambda_1(v_1 g) + \ldots + \lambda_n(v_n g)$.

onde $1 \leq i \leq n$; e e_G representa o elemento neutro do grupo G.

As letras F e G de FG-módulo indicam que V é um espaço vetorial sobre F e que G é o grupo do qual pegamos os elementos para a multiplicação vg ($v \in V$ e $g \in G$). Com isso podemos representar o FG-módulo como FG(V,G,$\odot$), onde $\odot$ é o símbolo que representa a multiplicação de um elemento de V por um elemento de G.

Se $V = F^n$ e definimos $vg = v(g\rho)$ (o produto vg será na verdade o produto de v pela representação de g), satisfazemos os axiomas acima e transformamos um espaço vetorial em um FG-Módulo (neste trabalho utilizaremos FG-módulos definidos desta forma e quando for conveniente representaremos o elemento neutro de FG-módulos por 0). Além disso $g\rho := [g]_{\mathfrak{B}}$, onde $[g]_{\mathfrak{B}}$ é a matriz representação de g escrita em uma base $\mathfrak{B}$ de V.

Existem muitas representações de um grupo, todas da forma $g \to [g]_{\mathfrak{B}}$ para alguma base $\mathfrak{B}$, mas observe que trabalhar com representações equivalentes significa mudar de base:

$$[g]_{\mathfrak{B}} = T^{-1}[g]_{\mathfrak{B}'}T \quad \forall g \in G.$$

4.1 Redutibilidade

Sejam V um FG-módulo e W um subespaço do espaço vetorial V. Se W é um FG-módulo, então será um FG-submódulo de V. Para verificar se W é um FG-submódulo de V, basta verificar se $wg \in W$ ($\forall w \in W \quad e \quad g \in G$), pois os outros axiomas já têm sua veracidade garantida por W ser subespaço de V.

Dizemos que um FG-módulo V é redutível se ele tem algum FG-submódulo além de $\{e_V\}$ e de V, caso contrário dizemos que ele é irredutível.

Definição 4.1. *Sejam V e W FG-módulos. Dizemos que $\vartheta : V \to W$ é um FG-homomorfismo se ϑ é uma transformação linear e $(vg)\vartheta = (v\vartheta)g$.*

Lema 4.1. *Seja e_V elemento neutro do FG-módulo V e g qualquer elemento de G. Então $e_V g = e_V$.*

Dem:

$(e_V)g = (e_V + e_V)g = e_V g + e_V g \Longrightarrow e_V g = e_V$. ■

Proposição 4.1. *Seja $\vartheta : V \to W$ um FG-homomorfismo. Então $Ker(\vartheta)$[8] é um FG-submódulo de V e $Im(\vartheta)$[9] é um FG-submódulo de W.*

Dem:

Devemos primeiro perceber que $Ker(\vartheta)$ é um subespaço de V e $Im(\vartheta)$ é um subespaço de W, pois ϑ é uma transformação linear. Então só precisamos verificar que o 1º axioma é atendido.

Agora, para v$\in Ker(\vartheta)$ e $g \in G$, temos

$$(vg)\vartheta = (v\vartheta)g = e_W g = e_W,$$

então $vg \in Ker(\vartheta)$. Com isso $Ker(\vartheta)$ é um FG-submódulo de V.

Agora seja $w \in Im(\vartheta)$, então $w = v\vartheta$ para algum $v \in V$. E para todo $g \in G$, temos

$$wg = (v\vartheta)g = (vg)\vartheta \in Im(\vartheta),$$

e então $Im(\vartheta)$ é um FG-submódulo de W. ■

Se existe ϑ^{-1} que é a inversa de ϑ então $V \cong$ W(V é isomorfo a W) e com isso ϑ e ϑ^{-1} são FG-isomorfismos. Como conseqüência, sabemos que dimU=dimW e V é irredutível se e somente se W é irredutível.

[8] $Ker(\vartheta) = \{v \in V : v\vartheta = e_W\}$. O Kernel é também chamado de Núcleo.
[9] $Im(\vartheta)$ é a imagem da função ϑ.

Teorema 4.1. *Seja V um FG-módulo com uma base $\mathfrak{B}$ (a base de um FG-módulo é a mesma base escolhida para o espaço vetorial que o compõe.), e W é um FG-módulo escrito em uma base $\mathfrak{B}'$. Então V e W são isomorfos se e somente se as representações*

$$\rho : g \mapsto [g]_{\mathfrak{B}} \quad e \quad \sigma : g \mapsto [g]_{\mathfrak{B}'}$$

são equivalentes.

Dem:

Vejamos primeiro que V e W são isomorfos se e somente se existem bases $\mathfrak{B}_1$ de V e $\mathfrak{B}_2$ de W tal que $[g]_{\mathfrak{B}_1} = [g]_{\mathfrak{B}_2} \quad \forall g \in G$.

Para ver isso, suponhamos que ϑ é um FG-isomorfismo de V em W, e $v_1, \cdots, v_n$ é uma base $\mathfrak{B}_1$ de V, e $v_1\vartheta, \cdots, v_n\vartheta$ é uma base $\mathfrak{B}_2$ de W. Desde que $(v_i g)\vartheta = (v_i\vartheta)g$ para cada i, então $[g]_{\mathfrak{B}_1} = [g]_{\mathfrak{B}_2}$.

Por outro lado, suponhamos que $v_1, \cdots, v_n$ é uma base $\mathfrak{B}_1$ de V, e $w_1, \cdots, w_n$ é uma base $\mathfrak{B}_2$ de W tal que $[g]_{\mathfrak{B}_1} = [g]_{\mathfrak{B}_2}$, para todo $g \in G$. Seja ϑ uma transformação linear invertível de V em W tal que $v_i\vartheta = w_i$, para todo i. Desde que $[g]_{\mathfrak{B}_1} = [g]_{\mathfrak{B}_2}$, deduzimos que $(v_i g)\vartheta = (v_i\vartheta)g \quad \forall i$, e então ϑ é um FG-isomorfismo.

Voltando à nossa demonstração, vamos assumir que V e W são FG-módulos isomorfos. Acabamos de ver que existem bases $\mathfrak{B}_1$ de V e $\mathfrak{B}_2$ de W tal que $[g]_{\mathfrak{B}_1} = [g]_{\mathfrak{B}_2} \quad \forall g \in G$. Definamos a representação ϕ de G por $\phi : g \mapsto [g]_{\mathfrak{B}_1}$. Então para alguma matriz T invertível $g\phi = T^{-1}g\rho$ para todo g pertencente a G, isto é, ϕ é equivalente a ρ. Então ρ e σ são equivalentes.

Por outro lado, suponha que ρ e σ são equivalentes. Então, existe uma base $\mathfrak{B}''$ de V tal que, $g\sigma = [g]_{\mathfrak{B}''}$ para todo $g \in G$; isto é, $[g]_{\mathfrak{B}''} = [g]_{\mathfrak{B}'}$ para todo $g \in G$. Então pelo que vimos ainda pouco, V e W são FG-módulos isomorfos. ∎

4.2 Soma Direta

Sejam U e W FG-submódulos de V, tal que V pode ser escrito como soma direta de U e W, isto é, $V = U \oplus$W.

Sejam $u_1, \ldots, u_n$ base $\mathfrak{B}_1$ de U e $w_1, \ldots, w_m$ base $\mathfrak{B}_2$ de W, então uma base $\mathfrak{B}$ de V é $u_1, \ldots, u_n, w_1, \ldots, w_m$ e para $g \in G$

$$[g]_{\mathfrak{B}} = \begin{pmatrix} [g]_{\mathfrak{B}_1} & 0 \\ 0 & [g]_{\mathfrak{B}_2} \end{pmatrix}. \tag{4.3}$$

Este resultado pode ser estendido naturalmente, quando podemos escrever V como soma direta de r FG-submódulos de V, ou seja, se $V = U_1 \oplus U_2 \oplus \cdots \oplus U_r$, uma soma direta de FG-submódulos U_i, e $\mathfrak{B}_i$ é uma base de U_i teremos para $g \in G$

$$[g]_{\mathfrak{B}} = \begin{pmatrix} [g]_{\mathfrak{B}_1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & [g]_{\mathfrak{B}_r} \end{pmatrix}. \tag{4.4}$$

Agora veremos nossos primeiros resultados importantes sobre teoria das representações.

5 Teorema de Maschke

Teorema 5.1. *Se U é um FG-submódulo de um FG-módulo V, então existe um FG-submódulo W de V tal que*

$$V = U \oplus W.$$

Dem:

Podemos escrever $V = U \oplus W_0$, para algum subespaço vetorial W_0 do espaço vetorial V. E para $v \in V$ temos $v = u + w$ para únicos vetores $u \in U$ e $w \in W_0$.

Sabemos que definindo a função $\phi : V \to V$ como $v\phi = u$, ϕ é uma projeção de V com Núcleo(Kernel) W_0 e imagem U.

Então se conseguirmos modificar a projeção acima para obter uma nova projeção ϑ que também seja um FG-homomorfismo de V em V com imagem U, teremos chegado ao fim da prova, pois W_0 será o Kernel de ϑ, isto é, será um FG-submódulo de V.

Assim, verifiquemos que

$$v\vartheta = \frac{1}{\mid G \mid} \sum_{g \in G} (vg)\phi g^{-1} \quad (v \in V)$$

é a função que procuramos; onde $\mid G \mid$ é o número de elementos do grupo G, chamado de ordem de G.

Seja $x \in G$ e h=xg. Então ϑ é um FG-homomorfismo:

$$(vx)\vartheta = \frac{1}{\mid G \mid} \sum_{g \in G} ((vx)g)\phi g^{-1} = \frac{1}{\mid G \mid} \sum_{h \in G} (vh)\phi h^{-1}x = (\frac{1}{\mid G \mid} \sum_{h \in G} (vh)\phi h^{-1})x = (v)\vartheta x$$

pois como g varre todos os elementos de G, h também varrerá.

E ϑ é uma projeção com imagem U:

$$u\vartheta = \frac{1}{\mid G \mid} \sum_{g \in G} (ug)\phi g^{-1} = \frac{1}{\mid G \mid} \sum_{g \in G} (ug)g^{-1} = \frac{1}{\mid G \mid} \sum_{g \in G} u = u. \tag{5.5}$$

Assim é fácil verificar que como $v = u + w$, então $v\vartheta \in U$ e $(v\vartheta)\vartheta = v\vartheta$. Também podemos ver pela equação (5.5) que $Im(\vartheta) = U$ e $W_0 = Ker(\vartheta)$. ∎

Assim todo FG-módulo pode ser escrito como uma soma direta de FG-submódulos irredutíveis. Com este resultado podemos restringir nosso estudo da teoria das representações a FG-Módulos irredutíveis.

6 Lema de Schur

Lema 6.1. *Sejam V e W $\mathbb{C}G$-módulos irredutíveis.*
(1') Se $\vartheta : V \to W$ é um $\mathbb{C}G$-homomorfismo então ϑ é um $\mathbb{C}G$-isomorfismo , ou $v\vartheta = 0$

$\forall v \in V$

(2') Se $\vartheta : V \to V$ é um $\mathbb{C}G$-isomorfismo então ϑ é um múltiplo da identidade (λI_V, onde I_V é a matriz identidade de ordem igual a dimensão de V).

Dem:

(1') Suponha que $v\vartheta \neq 0$ para algum $v \in V$.Então a $Im(\vartheta) \neq \{0\}$. Como a imagem é um $\mathbb{C}$G-submódulo de W, e W é irredutível, $Im(\vartheta) = W$. Além disso $Ker(\vartheta)$ é um $\mathbb{C}$G-submódulo de V e como o $Ker(\vartheta) \neq V$ e V é irredutível, $Ker(\vartheta)$=$\{0\}$. Assim ϑ é invertível, pois $Ker(\vartheta)$=$\{0\}$ e $Im(\vartheta) = W$, e então ϑ é um $\mathbb{C}$G-isomorfismo.

(2') Como o endomorfismo[10] ϑ tem um autovalor $\lambda \in \mathbb{C}$, então $Ker(\vartheta - \lambda I_V)$ é um $\mathbb{C}$G-submódulo diferente de zero de V. Desde que V é irredutível, $Ker(\vartheta - \lambda I_V)$=V. E então

$$v(\vartheta - \lambda I_V) = 0 \quad \forall v \in V.$$

Isto é, $\vartheta = \lambda I_V$, como queríamos. ∎

Proposição 6.1. *Se U é um $\mathbb{C}G$-módulo diferente de zero onde todo $\mathbb{C}G$-endomorfismo de U é um múltiplo escalar da identidade, então U é irredutível.*

Dem:

Por contradição, vamos supor que U seja redutível, ou seja, pelo teorema de Maschke
$U = U_1 \oplus U_2$.

Então uma projeção $(u_1 + u_2) \to u_1$ para todo $u_1 \in U_1$ e $u_2 \in U_2$ é um $\mathbb{C}$G-endomorfismo, mas não é um múltiplo escalar de 1_U o que é uma contradição. Logo U é irredutível. ∎

7 Teoria das representações de grupos abelianos

Seja G um grupo finito e abeliano, e V um $\mathbb{C}$G-Módulo irredutível. Para um $x \in G$ fixo o endomorfismo $(v)\vartheta_x = vx$ de V (espaço vetorial) é um $\mathbb{C}$G-homomorfismo, pois:

$$(vg)\vartheta_x = (vg)x = vxg = v\vartheta_x g \quad \forall g \in G.$$

E pela parte (1') do Lema de Schur sabemos que este endomorfismo é um $\mathbb{C}$G-isomorfismo, que pela parte (2') do Lema de Schur:

$$v\vartheta_x = vx = \lambda_x v \qquad \forall v \in V.$$

$vx = \lambda_x v$ pertence ao subespaço que contém v.

[10] Um endomorfismo de grupos é um homomorfismo $\vartheta : G \to G$.
Um endomorfismo de um espaço vetorial V é uma transformação linear de V em V.

Isto implica que o espaço gerado por v é um $\mathbb{C}$G-submódulo de V e, mais do que isso, todo subespaço de V é um $\mathbb{C}$G-submódulo, mas como V é irredutível deduzimos que a dimensão de V é igual a dimensão de seus subespaços, e como a dimensão do espaço gerado por v é igual a 1, então dim(V)=1. Com isso provamos a

Proposição 7.1. *Se G é Abeliano então todo $\mathbb{C}G$-módulo irredutível tem dimensão 1.*

A recíproca também é válida.

Pode-se provar que todo grupo abeliano finito é isomorfo a um produto direto de grupos cíclicos.

Com isso podemos determinar as representações irredutíveis de todos os produtos diretos

$$G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$$

onde $n_1, \cdots, n_r$ são inteiros positivos. Isto cobre todas as representações irredutíveis de todos os grupos abelianos finitos.

Seja c_i o gerador de C_{n_i}, podemos escrever

$$g_i = (1, \cdots, c_i, \cdots, 1) \quad (c_i \text{ está na i-ésima posição}).$$

Então

$$G = \langle g_1, \cdots, g_r \rangle^{11}, \quad \text{com} \quad g_i^{n_i} = 1.$$

onde n_i é a ordem de g_i, e estamos representando e_G pelo símbolo 1.

Agora, seja ρ uma representação irredutível de grau 1 de G sobre $\mathbb{C}$. Então para $1 \leqslant i \leqslant r$, existe $\lambda_i \in \mathbb{C}$ tal que

$$g_i\rho = \lambda_i.$$

Além disso $\lambda_i^{n_i} = g_i^{n_i}\rho = 1$, isto é, λ_i é uma n_i-ésima raiz da unidade.

E para um $g \in G$ temos

$$g\rho = (g_1^{j_1}, \cdots, g_r^{j_r})\rho = (\lambda_1^{j_1}, \cdots, \lambda_r^{j_r}) \tag{7.6}$$

Uma representação ρ de G que satisfaz a equação (7.6) pode ser representada como $\rho = \rho_{\lambda_1^{j_1}, \cdots, \lambda_r^{j_r}}$

E existem $n_1 n_2 \cdots n_r = \mid G \mid$ dessas representações que não são equivalentes duas a duas, pois $G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ e n_i é a ordem de C_i.

7.1 Diagonalização

Sejam $H = \langle g \rangle$ um grupo cíclico de ordem n e $V = U_1 \oplus \cdots \oplus U_r$, um $\mathbb{C}$H-módulo que pode ser escrito como uma soma direta de $\mathbb{C}$H-submódulos irredutíveis U_i de V, onde cada U_i tem dimensão 1. Sejam

[11] Grupo gerado quando operamos entre si os elementos $g_1, \cdots, g_r$.

também u_i o vetor que gera U_i e ω=$e^{\frac{2\pi i}{n}}$ (o número i do expoente é o número imaginário pertencente a $\mathbb{C}$). então para cada i existe um inteiro m_i tal que

$$u_i g = \omega^{m_i} u_i.$$

onde ω^{m_i} é uma representação de grau 1 de g.

Então se $\mathfrak{B}$ é uma base $u_1, \cdots, u_r$ de V podemos escrever

$$[g]_{\mathfrak{B}} = \begin{pmatrix} \omega^{m_1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \omega^{m_r} \end{pmatrix} \tag{7.7}$$

para enxergar isso, basta olhar para a matriz (4.4)

Agora podemos estender para um grupo finito qualquer G.

Proposição 7.2. *Seja G um grupo finito e V um $\mathbb{C}G$-módulo. Se $g \in G$, então existe uma base $\mathfrak{B}$ de V tal que a matriz $[g]_{\mathfrak{B}}$ é diagonal. Se g tem ordem n, então as entradas da diagonal de $[g]_{\mathfrak{B}}$ são n-ésimas raízes da unidade.*

Dem:

Seja H um subgrupo cíclico de G tal que $H = \langle g \rangle$. Como V também é um $\mathbb{C}$H-módulo, o resultado é imediato. Além disso suas entradas são n-ésimas raízes da unidade como na equação (7.7) ∎

8 Caracteres

Suponha que todo $\rho : G \to$GL(n,F) é uma representação de um grupo G. A cada matriz $g\rho \quad (g \in G)$ de grau n vamos associar um número complexo. Esta função que associa um número complexo a cada matriz de uma representação se chamará caracter desta representação.

Esta função tem propriedades fundamentais que auxiliam em toda teoria das representações e tem participação especial na Transformada de Fourier. Quando antes trabalhávamos com n^2 valores para cada matriz $g\rho$ agora será somente um para cada matriz.

Definição 8.1. *Suponha que V é um $\mathbb{C}G$-módulo com base $\mathfrak{B}$. Então o caracter de V é a função $\chi : G \to \mathbb{C}$ definida por $\chi(g) = tr[g]_{\mathfrak{B}} = \sum_{i=1}^{n} a_{ii}$.*

Antes de seguir em frente vamos relembrar algumas propriedades básicas do traço de uma matriz.

Proposição 8.1. *Sejam $A = (a_{ij}) \quad e \quad B = (b_{ij})$ matrizes $n \times n \quad e \quad T$ uma matriz invertível de grau n, então:*

$$tr(A + B) = tr(A) + tr(B) \tag{8.8}$$

$$tr(AB) = tr(BA) \tag{8.9}$$

$$tr(T^{-1}AT) = tr(A) \tag{8.10}$$

Dem:

A entrada ii de $A+B$ é $a_{ii}+b_{ii}$, e de AB é $\sum_{j=1}^{n} a_{ij}b_{ji}$. então

$$(8.8) \quad tr(A+B) = \sum_{i=1}^{n}(a_{ii}+b_{ii}) = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = tr(A) + tr(B);$$

$$(8.9) \quad tr(AB) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ji} = \sum_{j=1}^{n}\sum_{i=1}^{n} b_{ji}a_{ij} = tr(BA) \quad e$$

$$(8.10) \quad tr(T^{-1}AT) = tr((T^{-1}A)T) = tr(T(T^{-1}A)) = tr(A).$$

■

Repare que o caracter de V não depende da base:

$$[g]_{\mathfrak{B}'} = T^{-1}[g]_{\mathfrak{B}}T, \text{ assim, pela propriedade (8.10)} \quad \chi([g]_{\mathfrak{B}'}) = \chi([g]_{\mathfrak{B}}) \quad \forall g \in G.$$

Naturalmente vamos definir o caracter de uma representação ρ como o caracter χ do correspondente $\mathbb{C}$G-módulo $\mathbb{C}^n$, $\chi(g) = tr(g\rho) \quad g \in G$ e dizemos que a dim(V) é o grau de χ.

Daí seguem dois importantes resultados imediatos:

Proposição 8.2. (I) *$\mathbb{C}G$-módulos isomorfos têm o mesmo caracter*

(II) *Se x e y são elementos conjugados de G, então $\chi(x) = \chi(y), \forall \chi$ de G.*

Dem:

(I) Suponha que V e W são $\mathbb{C}$G-módulos isomorfos. Então pelo Teorema (4.1), existe uma base $\mathfrak{B}_1$ de V e uma base $\mathfrak{B}_2$ de W tal que

$$[g]_{\mathfrak{B}_1} = [g]_{\mathfrak{B}_2} \quad \forall g \in G.$$

Conseqüentemente $tr[g]_{\mathfrak{B}_1} = tr[g]_{\mathfrak{B}_2}$ e então V e W têm o mesmo caracter.

(II) Assumindo que x e y são elementos conjugados de G, então $x = g^{-1}yg$ para algum $g \in G$. Seja $\mathfrak{B}'$ uma base do $\mathbb{C}$G-módulo V. Então

$$[x]_{\mathfrak{B}} = [g^{-1}yg]_{\mathfrak{B}} = [g^{-1}]_{\mathfrak{B}}[y]_{\mathfrak{B}}[g]_{\mathfrak{B}}.$$

Então pela propriedade do traço, $tr[x]_{\mathfrak{B}} = tr[y]_{\mathfrak{B}}$. Com isso $\chi(x) = \chi(y)$, onde χ é o caracter de V. ■

Da Proposição (8.2(I)) podemos entender que representações equivalentes têm o mesmo caracter.

Se V é um $\mathbb{C}$G-módulo unidimensional, então para cada $g \in$ G, existe $\lambda_g \in \mathbb{C}$ tal que

$$vg = \lambda_g v, \quad \forall v \in V.$$

Além disso

$$\chi(g) = \lambda_g \quad (g \in G)$$

e χ tem grau 1, sendo assim chamado de caracter linear e é irredutível.

Observação 8.1. *Repare que uma representação de um grupo abeliano coincide com seu caracter, pois a representação de um grupo abeliano tem dimensão 1, ou seja, é uma matriz 1×1 e esta única entrada é o valor do traço desta matriz, ou seja, seu caracter.*

Proposição 8.3. *Os caracteres lineares são os únicos caracteres não nulos de G que são homomorfismos de G em* $\mathbb{C}$.

Dem:

Como vimos, o caracter de G é uma função de G em $\mathbb{C}$, mas esta função pode ser escrita como composição das funções $f : G \to GL(n, F)$ e $h : GL(n, F) \to \mathbb{C}$. Mas a função f é uma representação do grupo G, que é um homomorfismo por definição, então para que o caracter de G seja um homomorfismo a função h tem que ser um homomorfismo. E como h é a função traço, ela só será homomorfismo se GL(n,F) for abeliano, e isso só acontecerá se n=1 ,ou seja, se o caracter de G for um caracter linear. ■

Vejamos algumas informações sobre os valores dos caracteres

Proposição 8.4. *Se g tem ordem m então:*
(I')$\chi(1) = dim(V)$ *(onde o 1 representa o elemento neutro de G)*
(II')$\chi(g)$ *é uma soma de m-ésimas raízes da unidade*
(III')$\chi(g^{-1}) = \overline{\chi(g)}$
(IV') g é o conjugado de $g^{-1} \Rightarrow \chi(g)$ *é um número real*

Dem:

(I') Seja n dim(V), e seja $\mathfrak{B}$ uma base de V. Então a matriz $[1]_{\mathfrak{B}}$ do elemento identidade 1 relativo a $\mathfrak{B}$ é igual a I_n, Consequentemente

$$\chi(1) = tr[1]_{\mathfrak{B}} = trI_n = n,$$

e então $\chi(1) = dim(V)$.

(II') Sabemos que existe uma base $\mathfrak{B}$ de V tal que

$$[g]_{\mathfrak{B}} = \begin{pmatrix} \omega_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \omega_n \end{pmatrix} \tag{8.11}$$

onde cada ω_i é uma n-ésima raíz da unidade. Então

$$\chi(g) = \omega_1 + \cdots + \omega_n,$$

uma soma de m-ésimas raízes da unidade.

(III') Perceba que $\chi(g^{-1}) = \omega_1^{-1} + \cdots + \omega_n^{-1}$. Toda m-ésima raíz da unidade ω satisfaz $\omega^{-1} = \overline{\omega}$, desde que para todo real ϑ,

$$(e^{i\vartheta})^{-1} = e^{-i\vartheta},$$

que é o conjugado complexo de $e^{i\vartheta}$. Então

$$\chi(g^{-1}) = \overline{\omega}_1 + \cdots + \overline{\omega}_n.$$

(IV') Se g é o conjugado de g^{-1} então $\chi(g) = \chi(g^{-1})$. E também $\chi(g^{-1}) = \overline{\chi(g)}$, então $\chi(g) = \overline{\chi(g)}$; isto é, $\chi(g)$ é um número real. V ∎

Proposição 8.5. *Se $V = U_1 \oplus \ldots \oplus U_r$, onde U_i é um $\mathbb{C}G$-submódulo irredutível de V então o caracter de V é a soma dos caracteres dos $U_i's$, isto é, se χ é o caracter de V e χ_i é o caracter de U_i então podemos escrever $\chi = \sum_{i=1}^{r} \chi_i$.*

Dem:

Este resultado é imediato, só precisamos ver a matriz

$$[g]_{\mathfrak{B}} = \begin{pmatrix} [g]_{\mathfrak{B}_1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & [g]_{\mathfrak{B}_r} \end{pmatrix},$$

que está indicada em (4.4) para sua conclusão. ∎

9 Produto interno de caracteres

O conjunto de todas as funções de G em $\mathbb{C}$ formam um espaço vetorial sobre $\mathbb{C}$, se adotamos as regras naturais de adição de funções e multiplicação de funções por números complexos. Isto é, se ϑ, ϕ são funções de G em $\mathbb{C}$, e $\lambda \in \mathbb{C}$, então definimos $\vartheta + \phi : G \to \mathbb{C}$ por:

$$(\vartheta + \phi)(g) = \vartheta(g) + \phi(g) \quad (g \in G)$$

e também definimos $\lambda\vartheta : G \to \mathbb{C}$ por

$$\lambda\vartheta(g) = \lambda(\vartheta(g)) \quad (g \in G)$$

Agora podemos definir seu produto interno

Definição 9.1. *Suponha que ϑ e ϕ são funções de G em $\mathbb{C}$. Definimos seu produto interno como*

$$\langle \vartheta, \phi \rangle = 1/|G| \sum_{g \in G} \vartheta(g)\overline{\phi(g)}.$$

Para que o número complexo $\langle \vartheta, \phi \rangle$ seja o produto interno entre ϑ e ϕ deve satisfazer alguns axiomas. Vamos verificar agora que o produto interno definido acima satisfaz tais axiomas:

(A1) $\langle \vartheta, \phi \rangle = \overline{\langle \phi, \vartheta \rangle} \quad \forall \phi, \vartheta$;

Pela proposição $(8.4(III'))$ podemos escrever

$$\sum_{g \in G} \vartheta(g)\overline{\phi(g)} = \sum_{g \in G} \overline{\vartheta(g)}\phi(g).$$

E como o produto de caracteres é comutativo, nossa definição satisfaz o primeiro axioma.

(A2) $\langle \lambda_1\vartheta_1 + \lambda_2\vartheta_2, \phi \rangle = \lambda_1\langle \vartheta_1, \phi \rangle + \lambda_2\langle \vartheta_2, \phi \rangle \quad \forall \lambda_1, \lambda_2 \in \mathbb{C}$ e $\forall$ vetores $\vartheta_1, \vartheta_2, \phi$;

$$\begin{aligned} \langle \lambda_1\vartheta_1 + \lambda_2\vartheta_2, \phi \rangle &= \textstyle\sum_{g \in G}(\lambda_1\vartheta_1 + \lambda_2\vartheta_2)(g)\overline{\phi(g)} \\ &= \textstyle\sum_{g \in G}[(\lambda_1\vartheta_1)(g)\overline{\phi(g)} + (\lambda_2\vartheta_2)(g)\overline{\phi(g)}] \\ &= \lambda_1 \textstyle\sum_{g \in G} \vartheta_1(g)\overline{\phi(g)} + \lambda_2 \sum_{g \in G} \vartheta_2(g)\overline{\phi(g)} \\ &= \lambda_1\langle \vartheta_1, \phi \rangle + \lambda_2\langle \vartheta_2, \phi \rangle. \end{aligned}$$

(A3) $\langle \vartheta, \vartheta \rangle > 0$ se $\vartheta \neq 0$ e $\langle \vartheta, \vartheta \rangle = 0 \Leftrightarrow \vartheta = 0$.

$\langle \vartheta, \vartheta \rangle = \sum_{g \in G} \vartheta(g)\overline{\vartheta(g)}$

É produto de complexos conjugados que se diferente de zero é sempre um número real positivo, e só é zero quando ϑ é identicamente nulo.

Definição 9.2. *Os $\mathbb{C}G$-módulos irredutíveis $V_1, \ldots, V_k$ são ditos ser um conjunto completo de $\mathbb{C}G$-módulos irredutíveis não isomorfos, se todo $\mathbb{C}G$-módulo irredutível é isomorfo a algum V_i, e não existem dois $V_i's$ isomorfos entre si.*

Proposição 9.1. *Para qualquer grupo G finito existe um conjunto completo de $\mathbb{C}G$-módulos irredutíveis não isomorfos e este conjunto é finito.*

Para provar esta proposição precisamos ainda de muitos conceitos que ficaram de fora deste trabalho e que portanto ficará sem sua demostração.

Com isto pode-se demonstrar que caracteres irredutíveis[12] de G formam um conjunto ortonormal de vetores no espaço vetorial de funções de G em $\mathbb{C}$, isto é, para caracteres irredutíveis distintos χ e ψ de G, temos $\langle \chi, \chi \rangle = 1$ e $\langle \chi, \psi \rangle = 0$.

[12]caracteres de $\mathbb{C}$G-módulos irredutíveis.

Seja χ_i o caracter de V_i da Definição (9.2) ($1 \leqslant i \leqslant k$) então como vimos acima

$$\langle \chi_i, \chi_j \rangle = \delta_{ij} \quad \forall i, j, \tag{9.12}$$

onde δ_{ij} é a função delta de Kronecker (isto é, δ_{ij} é 1 se $i = j$ e 0 se $i \neq j$). Com isso, os caracteres irredutíveis $\chi_1 + \cdots + \chi_k$, dos $\mathbb{C}$G-módulos da definição (9.2), são todos distintos.

Agora, seja V um $\mathbb{C}$G-módulo redutível, então podemos escrevê-lo como uma soma de $\mathbb{C}$G-módulos irredutíveis , cada um deles isomorfo a algum V_i, então existem naturais $d_1, \cdots, d_k$ tal que

$$V \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k), \tag{9.13}$$

onde para cada i,tal que $1 \leq i \leq k$ existem d_i fatores V_i. Assim o caracter ψ de V é dado por

$$\psi = d_1\chi_1 + \cdots + d_k\chi_k,$$

além disso,

$$\langle \psi, \chi_i \rangle = \langle \chi_i, \psi \rangle = d_i \quad e \quad \langle \psi, \psi \rangle = d_1^2 + \cdots + d_k^2. \tag{9.14}$$

Teorema 9.1. *Seja $\chi_1, \cdots, \chi_k$ caracteres irredutíveis de G. Então $\chi_1, \cdots, \chi_k$ são vetores linearmente independentes no espaço vetorial de todas as funções de G em $\mathbb{C}$.*

Dem:

Assumamos que

$$\lambda_1\chi_1 + \cdots + \lambda_k\chi_k = 0 \quad (\lambda_i \in \mathbb{C}).$$

Então para todo i, usando (9.12), temos

$$0 = \langle \lambda_1\chi_1 + \cdots + \lambda_k\chi_k, \chi_i \rangle = \lambda_i.$$

Daí concluímos que $\chi_1, \cdots, \chi_k$ são linearmente independentes. ∎

Teorema 9.2. *Seja V um $\mathbb{C}$G-módulo com caracter ψ. Então V é irredutível se e somente se $\langle \psi, \psi \rangle = 1$*

Dem:

Como vimos anteriormente, se V é irredutível então $\langle \psi, \psi \rangle = 1$.

Por outro lado, se $\langle \psi, \psi \rangle = d_1^2 + \cdots + d_k^2 = 1$, como visto em (9.14), então algum $d_i = 1$ ($d_i \in \mathbb{N}$) e os outros são zero. Assim $V \cong V_i$ para algum i e V é irredutível. ∎

Teorema 9.3. *Sejam V e W $\mathbb{C}$G-módulos com caracteres χ e ψ respectivamente. Então V e W são isomorfos se e somente se $\chi = \psi$.*

Dem:

Na Proposição (8.2) já provamos que $\mathbb{C}$G-módulos isomorfos têm o mesmo caracter, vejamos a outra parte da demonstração:

Suponha que $\chi = \psi$. E vamos considerar novamente o conjunto $V_1, \cdots, V_k$ da Definição (9.2) com caracteres $\chi_1 \cdots \chi_k$. E como fizemos na equação (9.13) vamos fazer agora utilizando números naturais c_i, d_i $(1 \leq i \leq k)$, assim

$$V \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

com c_i fatores V_i para cada i, e

$$W \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

com d_i fatores V_i para cada i.

E pelas equações (9.14),

$$c_i = \langle \chi, \chi_i \rangle, \quad d_i = \langle \psi, \chi_i \rangle.$$

e como $\chi = \psi$, $c_i = d_i$ para todo i, então $V \cong W$. ∎

O conjunto $\mathfrak{C}$ de todas as funções $\psi : G \to \mathbb{C}$ tal que $\psi(x) = \psi(y)$ sempre que x e y são elementos conjugados de G, é um subespaço do espaço de funções de G em $\mathbb{C}$, e chamamos cada uma dessas funções de função classe em G . Então se l é o número de classes de conjugação de G, então $\dim\mathfrak{C} = l$, desde que podemos formar uma base composta pelas funções que assumem o valor 1 em exatamente uma classe de conjugação e o valor zero nas outras. Repare que a função caracter é uma função classe.

Além disso, o número de caracteres irredutíveis de G é igual ao número de classes conjugadas de G. Este resultado também será adotado sem demonstração pois foge do contexto do trabalho, mas pode ser encontrada em [2].

Os caracteres irredutíveis $\chi_1, \cdots, \chi_k$ de G formam uma base do espaço vetorial de todas as funções classe em G . Com isso

$$f = \sum_{i=1}^{k} \lambda_i \chi_i \tag{9.15}$$

onde $\lambda_i = \langle f, \chi_i \rangle$.

Pois, desde que $\chi_1, \cdots, \chi_k$ são linearmente independentes, ele geram um subespaço de $\mathfrak{C}$ de dimensão k. Como vimos que $\dim\mathfrak{C} = l$ (número de classes conjugadas de G) e que é igual ao número de caracteres irredutíveis, então l=k.

Assim $\chi_1, \cdots, \chi_k$ geram $\mathfrak{C}$, e formam uma base para $\mathfrak{C}$.

Observação 9.1. *Repare que quando utilizamos um grupo abeliano, seus caracteres irredutíveis formam uma base para o espaço vetorial de todas as funções de G em $\mathbb{C}$, pois nesse caso cada elemento de G forma uma classe de conjugação e $\mid G \mid = dim\mathfrak{C}$.*

Este fato é de suma importância pois vamos nos utilizar dele para a construção da Transformada de Fourier.

10 Conclusões

A função $\widehat{f}$:G$\rightarrow \mathbb{C}$ definida por:

$$\widehat{f}(g_i) = \widehat{f}_i = \sqrt{n}\lambda_i$$

é chamada de Transformada Discreta de Fourier, onde λ_i é o coeficiente de χ_i na equação (9.15):

$$f = \sum_{i=1}^{k} \lambda_i \chi_i$$

e n é a ordem do grupo G.

O coeficiente λ_i é facilmente obtido através do produto interno de χ_i e f:

$$\langle f, \chi_i \rangle = \lambda_i.$$

Assim temos outra maneira de escrever a transformada de Fourier, aliás, da forma mais usual:

$$\widehat{f}(g_i) = \sqrt{n}\langle f, \chi_i \rangle = \frac{1}{\sqrt{n}} \sum_{g \in G} f(g)\overline{\chi_i(g)} = \frac{1}{\sqrt{n}} \sum_{g \in G} \overline{\chi_i(g)} f(g)$$

Como o grupo G que utilizaremos é cíclico, podemos escrever $G = C_n = \langle g : g^n = 1 \rangle$ e um elemento genérico de G como g^k onde g é o elemento gerador do grupo e $0 \leq k \leq n-1$, além disso, G tem exatamente n (ordem de G) caracteres, como vimos na observação (9.1); esses caracteres são lineares, distintos entre si, e os representaremos como χ_j, onde $0 \leq j \leq n-1$. Assim

$$\chi_j(g^k) = e^{-2\pi i j \frac{k}{n}},$$

onde o i que aparece no expoente é o número imaginário pertencente a $\mathbb{C}$.

Para o algoritmo de Shor a transformada de Fourier utiliza $G = \mathbb{Z}_n$ onde o elemento gerador é o 1 e o elemento neutro da operação associada (soma) é o 0. Assim a Transformada de Fourier de uma função $f : \mathbb{Z}_n \rightarrow \mathbb{C}$ será

$$\widehat{f}(k) = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} e^{2\pi i j \frac{k}{n}} f(j) = \frac{1}{\sqrt{n}} \sum_{j \in \mathbb{Z}_n} e^{2\pi i j \frac{k}{n}} f(j) \ ,$$

como visto na seção (2).

Referências

[1] Kisnney Emiliano de Almeida and Luiz Mariano Carvalho. A transformada discreta de Fourier aplicada à computação quântica. In *Anais do VII Encontro de Modelagem Computacional*, pages 1–10, 2004. CD-ROM.

[2] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, 1987.

[3] Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2nd edition, 2001.

[4] Renato Portugal, Carlile Campos Lavor, Luiz Mariano Carvalho, and Nelson Maculan. *Uma Introdução à Computação Quântica*, volume 8 of *Not. Mat. Apl.* SBMAC, São Carlos, 2004.