IV Bienal da SBM

Ações e Representações de Grupos e Teoria de Números

Prof. Eliezer Batista

Departamento de Matemática

Universidade Federal de Santa Catarina

Maringá, Setembro de 2008

Conteúdo

Introdução

Esta pequena publicação consiste das notas de aula do Minicurso entitulado "Ações e Representações de Grupos, Com Aplicações à Teoria de Números", ministrado na IV Bienal da Sociedade Brasileira de Matemática, realizada em Maringá, PR, entre 29 de setembro e 3 de outubro de 2008.

Nosso objetivo ao propormos este mini-curso era mostrar aos alunos um aspecto importante da teoria de grupos, pouco explorada nas disciplinas de graduação, a saber, ações e representações de grupos. Em geral, as disciplinas dos cursos de graduação em Matemática, tanto de licenciatura como de bacharelado, apresentam a teoria de grupos somente do ponto de vista estrutural, ou seja, os grupos são pensados simplesmente como estruturas abstratas, das quais são investigadas apenas sua estrutura interna. no entanto, a história da matemática nos mostra que a verdadeira relevância dos grupos para uma variada gama de aplicações, somente pode ser explicitada quando seus elementos são vistos como bijeções em algum conjunto dado. Esta é a idéia básica de ações de grupos, todo o grupo pode ser visto como subgrupo de bijeções em algum conjunto. É nesta forma encarnada que a teoria de grupos permeia todas as áreas da matemática, não só a álgebra, como também a geometria, a análise a teoria de números, etc.

Dentre as diversas ações de grupos, possuem especial importância as ações como tranformações lineares invertíveis em algum espaço vetorial. Estas são as denominadas representações lineares de um grupo. A teoria de representações de grupos assumiu tamanha importância em Matemática que ela mesma se tornou um ramo de estudos independente. A razão deste destaque para a teoria das representações lineares está no poder de cálculo, pois combina a teoria de grupos com as ferramentas da álgebra linear. Basicamente, os elementos de um grupo podem ser vistos como matrizes invertíveis de uma certa ordem, assim, todos os procedimentos de fatorações matriciais são aplicáveis. Alguns teoremas clássicos em teoria de grupos são deduzidos

de forma muito mais direta utilizando-se representações de grupos.

Neste mini-curso, pretendemos introduzir as noções básicas de teoria de representações de grupos finitos. Em particular, um conceito fundamental na teoria de representações é o conceito de caracter. Um caracter de uma representação de um grupo G é um homomorfismo entre G e o grupo dos números complexos invertíveis, e basicamente corresponde ao traço da matriz na representação dada. No caso de grupos abelianos, as representações denominadas irredutíveis[1] do grupo são exatamente os caracteres. Este será o contexto que iremos nos ater ao longo destas notas.

A principal aplicação desta teoria será para o estudo de propriedades dos números inteiros, mais especificamente, sobre a distribuição dos números primos em seqüências aritméticas. Pretendemos apresentar as ferramentas necessárias de teoria de representações para podermos demonstrar o célebre teorema de Dirichlet cujo enunciado pode ser expresso da seguinte forma:

Teorema 0.1 *Sejam a e n números inteiros positivos com $mdc(a, n) = 1$, então existem infinitos números primos na seqüência aritmética $x = nk + a$.*

Utilizando a linguagem de congruências módulo n, podemos ainda enunciar este teorema dizendo que existem infinitos números primos $p \equiv a(\mathrm{mod} n)$.

Este teorema requer uma grande quantidade de conceitos matemáticos para a sua demonstração. Muitas destas ferramentas matemáticas foram desenvolvidas pelo próprio Dirichlet, entre elas a teoria dos caracteres. Mais especificamente, os caracteres que entram nesta demonstração são os do grupo dos elementos invertíveis do quociente $\mathbb{Z}_n$, lembremo-nos que se n for um número primo, então $\mathbb{Z}_n$ é um corpo, e portanto, todo elemento não nulo de $\mathbb{Z}_n$ faz parte deste grupo. No caso em que n não é um número primo, então somente farão parte deste subgrupo as classes dos números que são primos com n. A idéia original de dirichlet foi transformar estes caracteres em funções aritméticas definidas em todo o conjunto dos números inteiros e depois associar a esta função aritmética uma série infinita, permitindo-o utilizar as ferramentas da análise matemática para demonstrar um resultado que originalmente era de teoria de números. Esta junção de técnicas e áreas tão diversas da matemática faz deste teorema um resultado elegante, profundo, de grande interesse por si próprio e extremamente útil do ponto de

[1]Uma representação irredutível de um grupo G sobre um espaço vetorial $\mathbb{V}$ é uma representação que não deixa sub-espaços próprios $\mathbb{W} \subset \mathbb{V}$ invariantes pela ação do grupo.

vista do ensino de matemática, pois permite-nos apresentar em um único contexto, diversos conceitos novos e interessantes.

Estas notas estão divididas da seguinte maneira: No primeiro capítulo, abordaremos as noções básicas de teoria de grupos e ações de grupos, apresentando os conceitos de órbita, pontos fixo, sub-grupo estabilizador, etc. Mostraremos alguns resultados básicos, como o teorema de Lagrange, e sua versão para ações de grupos, a equação de classes, o lema de Burnside, etc, depois aplicaremos estes resultados para obtermos de forma alternativa alguns resultados padrão de teoria de números, como o pequeno teorema de Fermat e o teorema sobre a função totiente de Euler, conforme a referência [7].

No segundo capítulo, introduziremos o conceito de representação de grupo, mostraremos que para grupos finitos, basta nos atermos às representações unitárias[2] e irredutíveis. Demonstraremos o lema de Schur, que implica que para grupos abelianos todas as representações irredutíveis serão unidimensionais. Finalmente, provaremos alguns resultados concernentes À ortogonalidade dos caracteres da srepresentações irredutíveis.

No terceiro capítulo, trataremos especificamente da demonstração do teorema de Dirichlet, fornecendo as condições necessárias para sua demonstração. É, com certeza, o capítulo mais difícil, pois além de envolver conceitos de teoria de números e de toeria de grupos, também teremos que lidar com elementos de análise, mais especificamente com resultados sobre a convergência de séries infinitas. As séries de Dirichlet contituem-se em uma ferramenta sofisticada no estudo da teoria de números, parte de um conjunto de técnicas que se chama teoria analítica dos números. Ainda hoje existem problemas de pesquisa envolvendo o uso destas séries.

No apêndice, mostaremos alguns resultados básicos de teoria de números, em particular, aqueles que versam sobre funções aritméticas, que serão úteis ao longo de todo o texto.

Esperamos que, ao final deste mini-curso, o estudante interessado tenha percebido a importância da teoria de representações de grupos e que possa se aventurar mais sobre outros aspectos mais avançados desta teoria.

[2]Basicamente, uma representação unitária de um grupo G é uma representação na qual todo elemento de G é associado a um matriz unitária, ou seja, uma matriz complexa cuja transposta do seu conjugado complexo é igual à sua matriz inversa. No caso de representações unidimensionais, que será o nosso caso, as representações unitárias tomam valores na circunferência de raio igual a 1 no plano complexo.

Capítulo 1

Ações de Grupos

Um dos conceitos mais importantes na matemática moderna certamente é o conceito de grupo. Podemos ver a ubiqüidade dos grupos em quase todas as áreas da matemática, como na própria álgebra, na geometria, nas equações diferenciais, na teoria de números, bem como nas ciências naturais, como a física e a química. A idéia principal que confere aos grupos esta importância capital é a noção de simetria. Sempre em ciência tentamos reconhecer padrões e simetrias em nossos objetos de estudo, sejam eles uma molécula, um pêndulo físico, uma equação diferencial, um sólido geométrico, as raízes de uma equação polinomial, etc. A partir do momento em que identificamos as simetrias de nosso sistema, estamos introduzindo um grupo de transformações, ou seja um conjunto de bijeções que preservam as propriedades importantes deste sistema. O grupo é uma abstração deste conjunto de bijeções neste conjunto específico, podemos falar dos elementos de um grupo de maneira intrínseca, auto-contida, sem qualquer referência a um conjunto externo onde ele age. Esta é a perspectiva da maioria dos livros de álgebra existentes na atualidade. No entanto, no nível das aplicações, os grupos somente são relevantes quando "encarnados", em grupos de transformações. Para entendermos melhor esta inter relação entre o ponto de vista abstrato, do grupo como uma estrutura existente por si própria, e o ponto de vista concreto, do grupo agindo em outros conjuntos como bijeções, primeiro precisamos das definições básicas.

1.1 Grupos, Subgrupos e Homomorfismos

Definição 1.1 *Um grupo é um par $(G, \cdot)$ onde G é um conjunto não vazio e*

$$\begin{array}{rccc} \cdot : & G \times G & \to & G \\ & (a, b) & \mapsto & a \cdot b \end{array}$$

é uma função, denominada operação do grupo, satisfazendo

1. *(Associatividade) Para todos os elementos $a, b, c \in G$ temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
2. *(Elemento neutro) Existe um elemento $e \in G$ tal que para todo $a \in G$ tenhamos $a \cdot e = e \cdot a = a$.*
3. *(Elemento inverso) A todo elemento $a \in G$ associa-se um elemento a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

Exercício 1.1 *Mostre que existe um único elemento neutro em um grupo.*

Exercício 1.2 *Mostre que existe um único elemento inverso para cada elemento $a \in G$.*

Dentre todos os grupos existentes, uma classe em particular será muito útil no decorrer de todo o nosso trabalho: os grupos abelianos

Definição 1.2 *Um grupo $(G, \cdot)$ é dito ser abeliano, ou comutativo se para todos os elementos $a, b \in G$ tivermos $a \cdot b = b \cdot a$, ou seja, a operação do grupo satisfaz À propriedade da comutatividade*

Antes de irmos para os exemplos, uma última definição.

Definição 1.3 *Um subconjunto não vazio H de um grupo G é dito ser um sub-grupo de G se para quaisquer $a, b \in H$, tivermos que $a \cdot b^{-1} \in H$.*

Exercício 1.3 *Mostre que se $H \subseteq G$ é subgrupo, então*

1. *O elemento neutro $e \in G$ pertence a H e é seu elemento neutro.*
2. *Se $a \in H$, então $a^{-1} \in H$.*
3. *Se $a, b \in H$, então $a \cdot b \in H$.*

Exemplo 1.1: O conjunto dos números inteiros, $\mathbb{Z}$, com a operação definida pela soma é um grupo abeliano. É fácil ver que a soma satisfaz à associatividade e à comutatividade, o elemento neutro da soma é o número 0 e o elemento inverso de um número inteiro n é o seu oposto, $-n$.

Exercício 1.4 *Dê exemplos de sub-grupos aditivos de $\mathbb{Z}$.*

Definição 1.4 *Um grupo é dito ser finito, se G está em correspondência 1 a 1 com o conjunto $I_n = \{1, 2, \ldots, n\}$ para algum número natural $n \geq 1$. A ordem do grupo, denotada por $|G|$, será a cardinalidade do conjunto G, que é exatamente este n natural para o qual existe a bijeção.*

Exercício 1.5 *Mostre que, se $|G| = n$ então para todo elemento $a \in G$ temos que $a^n = e$.*

Exemplo 1.2: O conjunto das classes de congruência de números inteiros módulo n, $\mathbb{Z}_n$, com a operação soma também é um grupo abeliano. A soma de classes é definida como $[k] + [l] = [k + l]$. É fácil ver que esta operação está bem definida, isto é, que o resultado da soma independe do representante na classe de equivalência, ou seja, se $k' \equiv k(\mathrm{mod} n)$ e $l' \equiv l(\mathrm{mod} n)$, então $[k'] + [l'] = [k] + [l]$. As propriedades da soma nos números inteiros são herdadas automaticamente pela soma em $\mathbb{Z}_n$. Este grupo é finito e sua ordem é exatamente n.

Note que, tanto para o caso do grupo $\mathbb{Z}$ quanto para os grupos $\mathbb{Z}_n$ basta conhecermos um elemento, no caso o número 1, ou sua classe em $\mathbb{Z}_n$ que conseguimos determinar todos os outros elementos do grupo.

Definição 1.5 *Um grupo G para o qual existe um elemento $a \in G$ de forma que todo outro elemento g pode ser escrito como $g = a^n$ para $n \in \mathbb{Z}$ é chamado um grupo cíclico.*

Exercício 1.6 *Mostre que, de fato, a operação soma em $\mathbb{Z}_n$ está bem definida.*

Exemplo 1.3: Ainda no conjunto $\mathbb{Z}_n$, o conjunto de todos os elementos inversíveis pela operação de multiplicação, $[k][l] = [kl]$. Novamente, esta operação está bem definida no conjunto das classes.

Exercício 1.7 *Mostre que a multiplicação está bem definida em $\mathbb{Z}_n$.*

As propriedades associativa e comutativa da multiplicação são gerantidas diretamente da multiplicação nos inteiros. O elemento neutro multiplicativo é dado pela classe [1]. Para caracterizarmos os elementos inversíveis, vamos mostrar a seguinte proposição:

Proposição 1.1 *Um elemento* $[k] \in \mathbb{Z}_n$ *é inversível, se, e somente se,* $mdc(k, n) = 1$.

Demonstração: ($\Rightarrow$) Suponha que $[k] \in \mathbb{Z}_n$ seja inversível, então existe um elemento $[x] \in \mathbb{Z}_n$, tal que $[k][x] = [1]$. Isto corresponde a dizer que $kx \equiv 1(\text{mod}n)$, ou ainda, $kx = nq + 1$. Sendo assim, podemos escrever $kx - nq = 1$, significando que existe uma combinação linear inteira entre k e z que resulta em1, e isto é equivalente a dizer que $\text{mdc}(k, n) = 1$.

($\Leftarrow$) Por outro lado, se $\text{mdc}(k, n) = 1$, temos que existem inteiros x e y tais que $kx+ny = 1$. Tomando as classes de equivalência, teremos $[kx+ny] = [1]$, ou ainda $[k][x] + [n][y] = [1]$, mas como a classe $[n]$ em $\mathbb{Z}_n$ é igual à classe $[0]$, temos que $[k][x] = [1]$, ou seja, a classe $[k] \in \mathbb{Z}_n$, é inversível. ■

Portanto, desta proposição, podemos concluir que o grupo multiplicativo dos elementos inversíveis em $\mathbb{Z}_n$, é o conjunto das classes dos inteiros $0 < k < n$ que são primos com n. Vamos denotar este grupo por $\mathbb{Z}_n^{\times}$. Este grupo também é finito, já que é um subconjunto de $\mathbb{Z}_n$, cuja ordem é dada pelo pela quantidade de números inteiroa positivos menores que n e que são primos com n, este número é denotado por $\varphi(n)$ e a função $\varphi; \mathbb{Z}_+^* \to \mathbb{Z}$ que a cada número inteiro positivo associa esta quantidade é chamada função totiente de Euler, que será estudada posteriormente e terá um papel fundamental ao longo de todo o texto.

Exemplo 1.4: O Conjunto das bijeções em um conjunto X, com a operação de grupo dada pela composiçãol de funções. É fácil mostrar que a composta de duas funções bijetivas também é bijetiva.

Exercício 1.8 *Mostre que, de fato, a composta de bijeções é bijeção.*

Neste grupo o elemento neutro é a função identidade em X, denotada por Id_X. O elemento inverso de $f : X \to X$ é dado pela função inversa $f^{-1} : X \to X$.

Exercício 1.9 *Mostre que uma função $f : X \to X$ é bijetiva, se, e somente se, existe uma função $g : X \to X$ tal que $f \circ g = Id_X$ e $g \circ f = Id_X$, ou seja, g é a função inversa de f.*

Antes de continuarmos com os exemplos, vamos mostrar que todo grupo pode ser visto como um subgrupo de um grupo de bijeções.

Definição 1.6 *Dados dois grupo G e H, uma função $\varphi : G \to H$ é dita ser um homomorfismo de grupos se $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, para todos os elementos $a, b \in G$. Se o homomorfismo é injetivo, dizemos que ele é um monomorfismo. Se o homomorfismo é sobrejetivo, dizemos que ele é um epimorfismo. Se o homomorfismo é bijetivo, dizemos que ele é um isomorfismo.*

Denotaremos $G \cong H$ quando os grupos G e H forem isomorfos.

Exercício 1.10 *Mostre que, se $\varphi : G \to H$ é um homomorfismo de grupos, então*

1. *$\varphi(e_G) = e_H$.*
2. *Para qualquer $a \in G$, temos que $\varphi(a^{-1}) = (\varphi(a))^{-1}$.*

Proposição 1.2 *Todo grupo G é isomorfo a um sub-grupo do grupo das bijeções em G.*

Demonstração: Seja $a \in G$, defina a função

$$\begin{array}{rccc} L_a : & G & \to & G \\ & b & \mapsto & a \cdot b \end{array}$$

Vejamos que L_a é injetiva. De fato, se $L_a(b) = L_a(c)$, isto significa que $a \cdot b = a \cdot c$. Multiplicando esta última igualdade à esquerda por a^{-1}, teremos $a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c$, e portanto, $b = c$, o que implica que L_a é injetiva.

Para vermos que L_a é sobrejetiva, tome $b \in G$, podemos escrever $b = a \cdot a^{-1} \cdot b$, ou seja, $b = L_a(a^{-1} \cdot b)$. Portanto L_a é sobrejetiva.

Disto concluimos que $L(G) \subseteq \mathrm{Bij}(G)$. Sejam agora $a, b, c \in G$, temos que

$$L_a \circ L_b(c) = L_a(b \cdot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = L_{a \cdot b}(c).$$

Temos também que, para todo elemento $a \in G$

$$L_e(a) = e \cdot a,$$

portanto, $L_e = \mathrm{Id}_G$. Finalmente, temos que para todo $a \in G$,

$$L_{a^{-1}} \circ L_a = L_{a^{-1}\cdot a} = L_e = \mathrm{Id}_G,$$

de maneira análoga, podemos mostrar que $L_a \circ L_{a^{-1}} = \mathrm{Id}_G$. Portanto $L_{a^{-1}} = (L_a)^{-1}$.

Sejam $a, b \in G$, temos que

$$L_a \circ (L_b)^{-1} = L_a \circ L_{b^{-1}} = L_{a\cdot b^{-1}} \in L(G),$$

logo $L(G)$ é sub-grupo de $\mathrm{Bij}(G)$. Resta-nos mostrar que G está em correspondência 1 a 1 com $L(G)$, ou seja, falta-nos verificar que a função

$$\begin{array}{rccc} L: & G & \to & L(G) \subseteq \mathrm{Bij}(G) \\ & a & \mapsto & L_a \end{array},$$

que é um homomorfismo de grupos, conforme foi mostrado, também é bijetiva.

Para a injetividade de L, suponha que $L_a = L_b$, isto significa que, para qualquer $c \in G$ temos $L_a(c) = L_b(c)$, ou ainda $a \cdot c = b \cdot c$. Em particular, para $c = e$, o elemento neutro de G, temos $a = a \cdot e = b \cdot e = b$. A sobrejetividade sobre $L(G)$ é óbvia, pois toda bijeção em $L(G)$ é da forma L_a para algum $a \in G$. Portanto G pode ser identificado com o subgrupo $L(G)$ em $\mathrm{Bij}(G)$. De fato, mostramos mais, mostramos que o grupo G é isomorfo ao grupo $L(G)$. ■

Exemplo 1.5: Um caso particular do exemplo anterior é o conjunto das bijeções de um conjunto finito de n elementos. Como todos os conjuntos de n elementos estão em bijeção com $I_n = \{1, 2, \ldots, n\}$, então podemos simplesmente considerar o grupo das bijeções, ou permutações, em I_n, que vamos denotar por S_n. A ordem de S_n é igual a $n!$. Como corolário da proposição anterior, podemos enunciar o seguinte resultado.

Corolário 1.1 *(Teorema de Cayley) Todo grupo finito é isomorfo a um subgrupo de um grupo de permutações.*

Um elemento genérico do grupo de permutações S_n pode se esrito da seguinte maneira

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}.$$

Vamos exemplificar com $n = 3$. Em S_3 temos os elementos

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Este é o menor grupo não abeliano existente.

A composição de duas permutações é feita como composta de funções (leitura da direita para a esquerda[1]). Assim, por exemplo

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \pi_4.$$

Exercício 1.11 *Escreva a tábua de composição de S_3 e verifique os subgrupos de S_3.*

Exemplo 1.6: O grupo diedral D_3, ou grupo de simetrias de um triângulo equilátero. Seus elementos consistem de todos os movimentos rígidos em $\mathbb{R}^3$ que deixam um triângulo equilátero invariante, ou seja, a identidade, as rotações de $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ no plano do triângulo e ao redor do seu baricentro, as rotações de π ao redor dos eixos que contém as medianas do triângulo.

Exercício 1.12 *Escreva a tábua de composição de D_3 e verifique que $D_3 \cong S_3$.*

Exemplo 1.7: O grupo $U(1)$ dos números complexos de módulo 1, também denotado por $\mathbb{S}^1$, ou seja, a circunferência unitária no plano complexo. É fácil ver que se $z, w \in \mathbb{C}$ são dois números complexos tais que $|z| = |w| = 1$, então $|zw| = |z|.|w| = 1$. As propriedades da multiplicação dos números complexos garante-nos que este é um grupo abeliano. A diferença entre este grupo e os grupos apresentados nos exemplos anteriores é que este grupo é contínuo. Isto significa que, além de ser um grupo infinito, ele, como conjunto possui uma estrutura topológica, que nos permite falar em proximidade entre os elementos. Esta estrutura topológica em $\mathbb{S}^1$ é dada pela distância usual no plano. temos também que a operação de grupo é uma função contínua. A continuidade da operação diz que elementos próximos,

[1]Muito embora alguns autores adotem a convenção oposta para que a leitura seja da esquerda para a direita

quando multiplicados, darão resultados próximos. Mais do que contínuo, ainda é possível provar que a operação deste grupo é diferenciável, o que faz deste grupo um tipo especial e importantíssimo de grupo, denominado grupo de Lie.

Uma caracterização útil dos elementos de $\mathbb{S}^1$ pode ser dada pela forma exponencial dos números complexos: um número complexo z de módulo unitário pode ser escrito na forma

$$z = e^{i\theta} = \cos\theta + i\sin\theta.$$

Ao multiplicarmos dois elementos deste grupo, temos

$$e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}.$$

Os exemplos restantes de grupos serão todos grupos contínuos e nos serão úteis para as discussões posteriores.

Exemplo 1.8: Os grupos lineares, ou grupos de transformações lineares invertíveis em um espaço vetorial de dimensão finita: Seja $\mathbb{V}$ um espaço vetorial de dimensão n sobre um corpo $\mathbb{K}$ (no que se segue, em nossas notas deste minicurso, o corpo considerado será o dos números complexos, $\mathbb{C}$, salvo raras excessões, quando consideraremos o corpo dos reais, $\mathbb{R}$). Como a composta de transformações lineares invertíveis também é uma transformação linear invertível e a identidade é uma transformação linear invertível, temos facilmente que este conjunto forma um grupo. Denotaremos este grupo por $GL(\mathbb{V})$ ou $GL(n,\mathbb{K})$. Utilizaremos a primeira notação quando estivermos apenas enfatizando as transformações lineares em abstrato e a segunda notação quando estivermos falando da transformação linear em sua forma matricial. Sendo assim $GL(n,\mathbb{K})$ ainda pode ser visto como o grupo das matrizes invertíveis $n \times n$ com entradas no corpo $\mathbb{K}$.

Exemplo 1.9: Existem alguns sub-grupos dos grupos lineares que são importantes para aplicações: Os sub-grupos lineares especiais $SL(n,\mathbb{K})$ são compostos das matrizes invertíveis $n \times n$ com entradas em K e cujo determinante é unitário.

Exercício 1.13 *Mostre que, de fato, $SL(n,\mathbb{K})$ é sub-grupo de $GL(n,\mathbb{K})$.*

Considere $\mathbb{V}$ é um espaço vetorial real de dimensão n e com um produto escalar euclidiano

$$\begin{array}{rccc} \langle\cdot,\cdot\rangle: & \mathbb{V}\times\mathbb{V} & \to & \mathbb{R} \\ & (v,w) & \mapsto & \langle v,w\rangle \end{array}$$

onde, se $v = (v^1, v^2, \ldots, v^n)$ e $w = (w^1, w^2, \ldots, w^n)$, então

$$\langle v, w \rangle = \sum_{i=1}^{n} v^i w^i.$$

O grupo das transformações lineares que preserva o produto escalar é chamado grupo ortogonal, denotado por $O(n)$. Um elemento de $O(n)$ é uma transformação linear A tal que

$$\langle Av, Aw \rangle = \langle v, w \rangle.$$

Exercício 1.14 *Mostre que $O(n)$ é sub-grupo de $GL(n, \mathbb{R})$.*

Exercício 1.15 *Mostre que a matriz em uma determinada base de uma transformação linear ortogonal é tal que sua transposta é igual à sua inversa, isto é, $\hat{A}^T = \hat{A}^{-1}$ (OBS: Estas matrizes são denominadas matrizes ortogonais).*

Exercício 1.16 *Mostre que o determinante de uma matriz ortogonal é igual a 1 ou -1.*

A intersecção dos grupos ortogonal e especial produz um outro sub-grupo interessante de transformações lineares que são as ortogonais especiais, cujo grupo é denotado por $SO(n) = O(n) \cap SL(n, \mathbb{R})$.

Exercício 1.17 *Considere o caso particular $n = 2$. Escreva as matrizes de $SO(2)$ e conclua que elas são matrizes de rotação*

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Considere agora $\mathbb{V}$ é um espaço vetorial complexo de dimensão n e com uma forma sesquilinear, ou produto hermitiano

$$\begin{array}{rccc} \langle \cdot, \cdot \rangle : & \mathbb{V} \times \mathbb{V} & \to & \mathbb{C} \\ & (v, w) & \mapsto & \langle v, w \rangle \end{array}$$

onde, se $v = (v^1, v^2, \ldots, v^n)$ e $w = (w^1, w^2, \ldots, w^n)$, então

$$\langle v, w \rangle = \sum_{i=1}^{n} \bar{v}^i w^i.$$

O grupo das transformações lineares que preserva o produto hermitiano é chamado grupo unitário, denotado por $U(n)$. Um elemento de $U(n)$ é uma transformação linear A tal que

$$\langle Av, Aw\rangle = \langle v, w\rangle.$$

Exercício 1.18 *Mostre que $U(n)$ é sub-grupo de $GL(n, \mathbb{C})$.*

Exercício 1.19 *Mostre que a matriz em uma determinada base de uma transformação linear unitária é tal que sua transposta conjugada*[2] *é igual à sua inversa, isto é, $\hat{A}^* = \hat{A}^{-1}$ (OBS: Estas matrizes são denominadas matrizes unitárias).*

Exercício 1.20 *Mostre que o determinante de uma matriz unitária é igual a um número complexo de módulo* 1.

A intersecção dos grupos unitário e especial produz um outro sub-grupo interessante de transformações lineares que são as unitárias especiais, cujo grupo é denotado por $SU(n) = U(n) \cap SL(n, \mathbb{R})$.

Exercício 1.21 *Verifique que o grupo $U(1)$ é, de fato, a circunferência unitária, conforme o exemplo anterior.*

Exercício 1.22 *Mostre que o grupo $U(1)$ é isomorfo ao grupo de rotações $SO(2)$ pelo isomorfismo*

$$\begin{array}{rccc} \varphi: & U(1) & \to & SU(2) \\ & e^{i\theta} & \mapsto & R_\theta \end{array}$$

Como um último tópico a ser abordado nesta seção, mostraremos como um sub-grupo H de um grupo G pode introduzir uma relação de equivalência em G.

Definição 1.7 *Dado um sub-grupo H de um grupo G e um elemento $g \in G$, definimos a classe lateral à esquerda de g associada a H como o conjuunto*

$$gH = \{k \in G | g^{-1} \cdot k \in H\}.$$

Similarmente, a classe lateral à direita de g em relação a H é o conjunto

$$Hg = \{k \in G | k \cdot g^{-1} \in H\}.$$

[2] A matriz transposta conjugada de A, ou hermitiana conjugada, é a matriz trasposta da matriz cujas entradas são os conjugados complexos das entradas da matriz A. Denotamos a hermitiana conjugada por A^*.

Podemos também caracterizar a classe lateral à esquerda gH como o conjunto dos elementos $k \in G$ tais que podem ser escritos como $k = g \cdot h$ para algum $h \in H$. Durante toda nossa discussão, utilizaremos classes laterais à esquerda, a menos que se diga o contrário.

Proposição 1.3 *Duas classes laterais à esquerda g_1H e g_2H ou são disjuntas ou são iguais*

Demonstração: Suponha que exista um elemento $k \in g_1H \cap g_2H$, então existem $h_1, h_2 \in H$ tais que

$$k = g_1 \cdot h_1 = g_2 \cdot h_2.$$

Multiplicando-se esta última igualdade à direita por h_1^{-1}, temos que

$$g_1 = g_2 \cdot h_2 \cdot h_1^{-1} \in g_2H.$$

Logo para qualquer $g_1 \cdot h \in g_1H$ concluímos que

$$g_1 \cdot h = g_2 \cdot h_2 \cdot h_1^{-1} \cdot h \in g_2H.$$

Analogamente, podemos provar também que $g_2H \subseteq g_1H$ e portanto, as duas classes são iguais. ■

Uma outra propriedade importante das classes laterais à esquerda é que elas estão em bijeção com o sub-grupo H.

Exercício 1.23 *Mostre que a aplicação $L_g : H \to gH$ é uma bijeção (não homomorfismo) entre H e gH.*

Um último resultado relativo às classes laterais de grupos finitos refere-se ao célebre teorema de Lagrange. Que basicamente nos diz a quantidade de classes laterais relativas a um determinado sub-grupo.

Teorema 1.1 *Seja G um grupo finito e H um sub-grupo. Então a quantidade de classes laterais relativas e H é igual a*

$$\#C = \frac{|G|}{|H|}.$$

Demonstração: Pela proposição anterior, podemos ver que as classes laterais são disjuntas duas a duas. Então, escolhamos um representante para cada classe: $g_1, g_2, \ldots, g_n$, o que queremos saber é qual o valor deste número n. Pelo exercício anterior, verificamos que todas as classes g_1H, g_2H, ..., g_nH estão em bijeção com H, logo o número de elementos de cada classe é igual à ordem do sub-grupo H. Assim, a ordem do grupo G pode ser escrita como o produto do número de classes laterais pelo número de elementos em cada classe lateral, ou seja $|G| = n|H|$, sendo assim,

$$\#C = n = \frac{|G|}{|H|}. \qquad \blacksquare$$

Como corolário imediato do teorema de Lagrange, podemos enunciar que

Corolário 1.2 *A ordem de um sub-grupo de um grupo finito é sempre um divisor da ordem do grupo.*

Exercício 1.24 *Um grupo cíclico é um grupo gerado por um único elemento. Isto é, se G é um grupo cíclico, então existe um elemento $a \in G$ tal que todo outro elemento $x \in G$ pode ser escrito na forma $x = a^k$ para algum número inteiro k. Mostre que se G é um grupo cíclico e $|G| = n$, então para todo divisor d de n existe exatamente um subgrupo de ordem d.*

1.2 Ações de Grupos

Como vimos na seção anterior, todo grupo é isomorfo a um sub-grupo de um grupo de bijeções em um conjunto (em particular, das bijeções no próprio grupo). As situações onde um grupo pode ser visto como grupo de bijeções são as que realmente aparecem nas aplicações da teoria. É somente agindo como um grupo de bijeções que o grupo se concretiza, se incorpora e pode ser utilizado como uma ferramenta poderosa para o estudo das simetrias.

Definição 1.8 *Uma ação de um grupo G em um conjunto X é um homomorfismo de G no grupo das bijeções em X, que será denotado por Bij(X).*

Vamos fixar as notações: Vamos denotar uma ação por

$$\begin{array}{rccc} \alpha: & G & \to & \mathrm{Bij}(X) \\ & g & \mapsto & \alpha_g \end{array}$$

e portanto α_g é uma bijeção no conjunto X, qua associa a cada elemento $x \in X$ outro elemento $\alpha_g(x)$. Como α é um homomorfismo, então temos que

1. $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$ para todos elementos $g, h \in G$ e $x \in X$.
2. $\alpha_e = \mathrm{Id}_X$, ou seja, $\alpha_e(x) = x$ para todo $x \in X$.
3. $\alpha_g^{-1} = \alpha_{g^{-1}}$ para todo $g \in G$ (isto, na verdade, é facilmente concluído a partir dos dois ítens anteriores).

Antes de mostrarmos exemplos de ações de grupos sobre conjuntos, vamos a mais algumas definições adicionais

Definição 1.9 *Seja α uma ação de um grupo G sobre um conjunto X e considere um elemento $x \in X$. Definimos a órbita do elemento x como sendo o conjunto*

$$\mathcal{O}_x = \{\alpha_g(x) | g \in G\}.$$

Exercício 1.25 *Mostre que duas órbitas pela ação de um grupo ou são disjuntas ou coincidentes.*

O resultado enunciado no exercício anterior nos leva à conclusão que a ação de um grupo sobre um conjunto provoca uma partição neste, composta pelas órbitas.

Definição 1.10 *Considere uma ação α de um grupo G sobre um conjunto X. O sub-grupo estabilizador de um elemento $x \in X$ é definido como*

$$Stab_x = \{g \in G | \alpha_g(x) = x\}$$

Exercício 1.26 *Mostre que $Stab_x$ é, de fato, um sub-grupo de G.*

De forma semelhante, podemos falar do sub-grupo estabilizador de um sub-conjunto $Y \subseteq X$

$$Stab_Y = \{g \in G | \alpha_g(Y) \subseteq Y\}.$$

Note que os elementos de um sub-conjunto não precisam ficar fixos pela ação do grupo, apenas que suas órbitas precisam estar contidas neste sub-conjunto. Quando $\mathrm{Stab}_Y = G$, dizemos que $Y \subseteq X$ é um sub-conjunto invariante pela ação do grupo G.

Uma definição dual é o conjunto dos pontos fixos pela ação de um determinado elemento ou sub-grupo de G.

Definição 1.11 *O sub-conjunto dos pontos fixos de um elemento $g \in G$ é o conjunto*

$$Fix_g = \{x \in X | \alpha_g(x) = x\}.$$

Se $H \subseteq G$ é um sub-grupo de G, o conjunto dos pontos fixos pela ação de H é definido por

$$Fix_H = \{x \in X | \alpha_g(x) = x, \ \forall g \in H\}.$$

Definição 1.12 *Uma ação α de G em X é dita ser*

1. *Fiel, se $Fix_g = X$, então $g = e$.*
2. *Livre, se $Fix_g \neq \emptyset$, então $g = e$.*
3. *Transitiva, se $\mathcal{O}_x = X$, para todo elemento $x \in X$.*

Exemplo 1.10: Seja $G = \mathbb{R}$ o grupo aditivo dos reais. Considere $\mathbb{V}$ um espaço vetorial e $\mathbf{v} \in \mathbb{V}$ um vetor neste espaço. Então podemos indicar as translações em $\mathbb{V}$ na direção de V como a ação $T^{(\mathbf{v})}$ de $\mathbb{R}$ em $\mathbb{V}$ dada por $T_x^{(\mathbf{v})}(\mathbf{w}) = \mathbf{w} + x\mathbf{v}$.

Exemplo 1.11: Na mesma linha do exemplo anterior, Considere $\mathbb{A}$ um conjunto e uma ação T do grupo aditivo de um espaço vetorial $\mathbb{V}$ em $\mathbb{A}$ por translações. Se T é livre e transitiva, então dizemos que o conjunto $\mathbb{A}$, junto com o espaço $\mathbb{V}$ e a ação T forma um espaço afim. Se a dimensão de $\mathbb{V}$ é igual a n, dizemos que o espaço afim tem dimensão n.

Exercício 1.27 *Considere, para os números reais fixos $a_1, \ldots, a_n, b \in \mathbb{R}$ o seguinte subconjunto de pontos do $\mathbb{R}^n$:*

$$P = \{(x^1, \ldots, x^n) \in \mathbb{R}^n | a_1 x^1 + \cdots + a_n x^n = b\}.$$

Mostre que P é um espaço afim com dimensão $n - 1$.

Exemplo 1.12: Seja G um grupo. Este grupo pode agir sobre si mesmo de várias maneiras, dentre as quais destacamos duas de particular interesse:

a) A ação regular à esquerda: $L_g(h) = gh$, para todo $g, h \in G$.

b) A ação adjunta: $Ad_g(h) = ghg^{-1}$, para todo $g, h \in G$.

Exercício 1.28 *Mostre que a ação regular à esquerda é livre e transitiva.*

Exercício 1.29 *Mostre que, na ação adjunta, para todo $g \in G$ a aplicação $Ad_g : G \to G$ é um isomorfismo do grupo G nele mesmo.*

Exercício 1.30 *Faça explicitamente com o grupo S_3 o cálculo da ação adjunta, verifique as órbitas, os pontos fixos, os estabilizadores, etc.*

Exercício 1.31 *Mostre que $h \in G$ é um ponto fixo de Ad_g, se, e somente se, h comuta com g.*

Exercício 1.32 *Seja $H \subseteq g$ um subconjunto invariante pela ação adjunta em G.*

a) *Mostre que H é sub-grupo de G. Este tipo de sub-grupo é denominado sub-grupo normal.*

b) *Mostre que as classes laterais à direita e à esquerda geradas por um sub-grupo normal coincidem.*

c) *Finalmente, mostre que o conjunto das classes laterais à esquerda (ou à direita) forma um grupo, com a operação $gH \cdot kH = gkH$.*

Exemplo 1.13: Seja $G = \mathbb{Z}$ o grupo aditivo dos inteiros e $X = \mathbb{S}^1$ a circunferência unitária no plano

$$\mathbb{S}^1 = \{(\cos\theta, \sin\theta) \in \mathbb{R}^2 | \theta \in \mathbb{R}\}.$$

Para cada $\alpha \in \mathbb{R}$ podemos definir uma ação de $\mathbb{Z}$ em $\mathbb{S}^1$ por rotações da seguinte forma:

$$R_n^{(\alpha)} \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \begin{pmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{pmatrix} \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \begin{pmatrix} \cos(\theta + n\alpha) \\ \sin(\theta + n\alpha) \end{pmatrix}$$

Exercício 1.33 *Mostre que, se $\frac{\alpha}{2\pi} = \frac{p}{q} \in \mathbb{Q}$, a órbita de cada ponto de $\mathbb{S}^1$ é um polígono regular de q lados.*

Exercício 1.34 *Mostre que se $\frac{\alpha}{2\pi} \in \mathbb{R}\backslash\mathbb{Q}$ então a ação é livre.*

Este último caso, o das rotações por um ângulo incomensurável com 2π é um conhecido exemplo na teoria de sistemas dinâmicos e possui a propriedade que todo ponto possui uma órbita densa, isto é, em qualquer intervalo da circunferêancia, por menor que seja, existem infinitos pontos de qualquer órbita.

1.3 Ações de Grupos Finitos Sobre Conjuntos Finitos

No que se segue, vamos considerar ações de um grupo finito G sobre um conjunto, também finito, X. Como uma ação de grupo determina uma relação de equivalência em X (dois elementos de X são equivalentes, se, e somente se, estão na mesma órbita), e como as órbitas determinam uma partição no conjunto X, é fácil ver que o conjunto das órbitas coincide com o conjunto quociente determinado por esta relação de equivalência. Por isto, vamos denotar o conjunto das órbitas por X/G. Vamos denotar as cardinalidades de G, X e X/G, respectivamente por $|G|$, $|X|$ e $|X/G|$. Para cada $i = 1, \ldots, |X/G|$, escolhamos um representante x_i de cada órbita, vamos denotar o número de elementos na órbita de x_i por $|\mathcal{O}(x_i)|$. É fácil ver que, se $x \in X$ é um ponto fixo pela ação do grupo G então $|\mathcal{O}(x)| = 1$. Também é fácil de deduzir o seguinte resultado:

Proposição 1.4 *Considere uma ação do grupo finito G sobre o conjunto finito X. Considere também os elementos, $x_i \in X$, $i = 1, \ldots |X/G|$, que são os representantes de cada órbita. Então*

$$|X| = \sum_{i=1}^{|X/G|} |\mathcal{O}(x_i)|$$

Se denotarmos por X^G o sub-conjunto dos pontos fixos pela ação de G, podemos decompor a soma da proposição anterior em duas somas: A primeira referente a órbitas de pontos fixos (que possuem apenas um elemento) e a segunda composta de órbitas com mais de um elemento. Sendo assim, temos a denominada equação de classes:

$$|X| = |X^G| + \sum_{i=1}^{|X/G|-|X^G|} |\mathcal{O}(x_i)|. \tag{1.1}$$

Um resultado menos esperado é o que relaciona o número de elementos da órbita de um ponto com o estabilizador daquele elemento.

Teorema 1.2 *Seja uma ação α, do grupo finito G sobre um conjunto finito X. Considere um elemento $x \in X$, então*

$$|\mathcal{O}(x)| = \frac{|G|}{|Stab_x|}.$$

Demonstração: Vamos estabelecer uma bijeção entre o conjunto das classes laterais à esquerda em G determinadas por $Stab_x$ e a órbita de x, considere a aplicação;

$$\begin{array}{rccc} \phi: & G/Stab_x & \to & \mathcal{O}(x) \\ & g.Stab_x & \mapsto & \alpha_g(x). \end{array}$$

Facilmente, podemos ver que esta aplicação é sobrejetiva, pois todo elemento da órbita de x é da forma $\alpha_g(x)$ para algum $g \in G$, assim $\alpha_g(x) = \phi(g.Stab_x)$. Para verificarmos que esta aplicação é injetiva, considere $g, h \in G$ tais que

$$\phi(g.Stab_x) = \phi(h.Stab_x),$$

ou seja

$$\alpha_g(x) = \alpha_h(x).$$

Isto significa que

$$\alpha_{g^{-1}h}(x) = x,$$

ou ainda, que $g^{-1}h \in Stab_x$, o que implica que $g.Stab_x = h.Stab_x$.

Portanto, a função ϕ é bijetiva, o que nos leva à conclusão que a órbita de x e o conjunto quociente $G/Stab_x$ possuem o mesmo número de elementos. Pelo teorema de Lagrange, sabemos que

$$|G/Stab_x| = \frac{|G|}{|Stab_x|},$$

obtemos o resultado desejado. ■

Corolário 1.3 *Dada uma ação de um grupo finito G sobre um conjunto finito X, o número de elementos da órbita de $x \in X$ é um divisor de $|G|$.*

Juntando este corolário com a informação obtida pela equação de classes (1.1), podemos concluir que.

Corolário 1.4 *Dada uma ação de um grupo G sobre um conjunto finito X,com $|G| = p^n$, para p primo. Temos que*

$$|X| \equiv |X^G| (\mathrm{mod} p).$$

Demonstração: Como o número de elementos em qualquer órbita é um divisor de p^n, então deve ser igual a 1, ou um número da forma p^k com $k \leq n$. Da equação de classes, temos

$$|X| = |X^G| + \sum_{i=1}^{|X/G|-|X^G|} |\mathcal{O}(x_i)| = |X^G| + \sum_{i=1}^{|X/G|-|X^G|} p^{k_i}.$$

Assim, a diferença $|X| - |X^G|$ é divisível por p, como queríamos. ■

Como uma conseqüência deste resultado, podemos demonstrar de uma forma diferente o pequeno teorema de Fermat.

Teorema 1.3 *Seja $a \geq 1$ um número inteiro e p um número primo, então $a^p \equiv a(\mathrm{mod} p)$.*

Demonstração: Considere um conjunto $A = \{1, 2, \ldots, a\}$ e defina uma ação αdo grupo aditivo $\mathbb{Z}_p$ sobre $X = A^p$ por permutações cíclicas:

$$\begin{aligned}
\alpha_{[0]}(x_1, x_2, \ldots, x_p) &= (x_1, x_2, \ldots, x_p), \\
\alpha_{[1]}(x_1, x_2, \ldots, x_p) &= (x_2, x_3, \ldots, x_p, x_1), \\
\alpha_{[2]}(x_1, x_2, \ldots, x_p) &= (x_3, x_4, \ldots, x_1, x_2), \\
&\vdots \\
\alpha_{[n-1]}(x_1, x_2, \ldots, x_p) &= (x_p, x_1, \ldots, x_{p-2}, x_{p-1}),
\end{aligned}$$

Uma p-upla $(x_1, \ldots, x_p)$ será um ponto fixo por esta ação, se, e somente se $x_1 = x_2 = \cdots = x_p$. Isto significa que só podem existir a possíveis pontos fixos, ou seja $|X^G| = a$. Por outro lado, a cardinalidade do conjunto X é $|X| = a^p$. Do corolário da equação de classes temos que $|X| \equiv |X^G|(\mathrm{mod} p)$, ou seja $a^p \equiv a(\mathrm{mod} p)$. ■

Para finalizarmos este primeiro capítulo, vamos exibir um resultado importante na teoria de ações de grupos com conseqüências interessantes para a combinatória e para a teoria de números, o teorema de Burnside. Este resultado relaciona o número de órbitas em uma ação com o número de elementos em Fix_g para cada $g \in G$.

Lema 1.1 *Considere a ação de um grupo finito G sobre um conjunto finito X. Sejam $x, y \in X$ dois elementos na mesma órbita, então $|Stab_x| = |Stab_y|$.*

Demonstração: Se $y \in \mathcal{O}(x)$, então, existe $h \in G$ tal que $y = \alpha_h(x)$. Vamos mostrar que aplicação $Ad_h : G \to G$, quando restrita a $Stab_x$, produz uma bijeção entre $Stab_x$ e $Stab_y$:

Em primeiro lugar, note que, para qualquer $g \in Stab_x$, o elemento $Ad_h(g) \in Stab_y$. De fato,

$$\alpha_{hgh^{-1}}(y) = \alpha_{hgh^{-1}}\alpha_h(x) = \alpha_h\alpha_g(x) = \alpha_h(x) = y.$$

A aplicação Ad_h é injetiva quando definida em todo o grupo G, em particular, continua injetiva quando restrita a algum sub-grupo. A sobrejetividade vem do fato que, se $k \in Stab_y$, então $k = Ad_h(h^{-1}kh)$. Por um cálculo análogo ao feito anteriormente, é fácil ver que $h^{-1}kh \in Stab_x$. Portanto $Ad_h : Stab_x \to Stab_y$ é uma bijeção, garantindo, assim, o resultado. ■

Teorema 1.4 *Considere uma ação de um grupo finito G sobre um conjunto finito X. Então*

$$|X/G| \cdot |G| = \sum_{g \in G} |Fix_g|$$

Demonstração: A demonstração deste fato utiliza-se de uma técnica comum em combinatória, que é a contagem dupla. Denotemos $|X/G| = m$ e $|G| = n$, denote o número de elementos na k-ésima órbita por p_k, então $|X| = p_1 + p_2 + \cdots + p_m = p$. Os elementos do grupo serão denotados por $g_1, g_2, \ldots, g_n$ e os elementos do conjunto X por $x_1, x_2, \ldots, x_p$

Façamos uma matriz $F = (f(i,j))_{i,j}$ com n linhas e p colunas na qual $f(i,j) = 1$ se o elemento $x_j \in Fix_{g_i}$ e $f(i,j) = 0$ se $x_j \notin Fix_{g_i}$. Vamos avaliar a soma

$$\sum_{i=1}^{n}\sum_{j=1}^{p} f(i,j)$$

de duas maneiras diferentes. Primeiro, para um determinado índice i fixo, se somarmos para todo $1 \leq j \leq p$ teremos

$$\sum_{j=1}^{p} f(i,j) = |Fix_{g_i}|.$$

Por outro lado, se fixarmos uma coluna j e somarmos sobre o índice $1 \leq i \leq n$, teremos

$$\sum_{i=1}^{n} f(i,j) = |Stab_{x_j}|.$$

Pelo lema anterior, se dois elementos estão na mesma órbita, então seus sub-grupos estabilizadores possuem a mesma ordem, logo teremos

$$\sum_{j=1}^{p}\sum_{i=1}^{n} f(i,j) = \sum_{k=1}^{m} |\mathcal{O}(x_{p_1+\cdots+p_k})||Stab(x_{p_1+\cdots+p_k})|$$

considerando que

$$|\mathcal{O}(x_{p_1+\cdots+p_k})| = \frac{|G|}{|Stab(x_{p_1+\cdots+p_k})|},$$

teremos a igualdade

$$\sum_{i=1}^{n} |Fix_{g_i}| = \sum_{k=1}^{m} |G| = |G|.|X/G|.$$

Que é o resultado enunciado. ■

Como um exemplo de aplicação do teorema de Burnside, vamos solucionar um problema combinatórico simples: Considere um disco dividido em n setores circulares todos congruentes (como uma pizza, ou um guarda-chuva), suonha ainda que existam disponíveis q cores distintas para pintarmos os diversos setores circulares. De quantas maneiras não equivalentes podemos efeturar esta pintura?

Denotemos por r este número procurado. Note que neste problema, dada uma configuração de cores pintadas no disco, se o rotacionarmos por um ângulo múltiplo de $\frac{2\pi}{n}$ obteremos a mesma configuração de cores. Portanto, existe uma ação de um grupo cíclico $G = \langle a \rangle$ de ordem n sobre o disco, de forma que $\alpha_a(x) = R_{\frac{2\pi}{n}}(x)$ para todo ponto x no disco. Então cada órbita pela ação do grupo G pode ser considerada como a mesma configuração de cores. O problema é encontrar o número de órbitas existentes. É neste ponto que entra o teorema de Burnside, e ao invés de contarmos diretamente as órbitas, vamos contar os pontos fixos de cada elemento g do grupo. Para cada divisor d de n, existe um sub-grupo de ordem d. Este sub-grupo pode ser visto como o sub-grupo cíclico gerado pelo elemento $a^{\frac{n}{d}}$, que corresponde a uma rotação de ângulo $d \cdot \frac{2\pi}{n}$. Neste sub-grupo existem exatamente d elementos, a saber $a^{\frac{n}{d}}$, $a^{\frac{2n}{d}}$,..., $a^{\frac{dn}{d}} = e$. Destes, apenas $\varphi(d)$ elementos possuem ordem exatamente igual a d, isto é, $x^d = e$ e $x^k \neq e$ se $0 < k < d$ (**Verifique este fato**), e estes são todos os elementos de ordem d no

grupo (**Verifique isto também**). Para cada elemento de ordem d no grupo, existem $q^{\frac{n}{d}}$ configurações inequivalentes de cores. Assim, temos, pelo teorema de Burnside

$$r.|G| = \sum_{g \in G} |Fix_g|,$$

ou seja

$$r = \frac{1}{n} \sum_{d|n} \varphi(d) q^{\frac{n}{d}}. \tag{1.2}$$

Como um corolário deste resultado, se o número q, de cores for igual a 1, teremos apenas uma única cnfiguração possível ($r = 1$), logo, podemos deduzir uma propriedade importante da função φ de Euler:

Teorema 1.5 *Seja n um número natural não nulo, então*

$$\sum_{d|n} \varphi(d) = n$$

Demonstração: A verificação é imediata para $n = 1$ e $n = 2$, e para $n = 3$, podemos utilizar a fórmula (1.2) para $q = 1$. ■

Exercício 1.35 *De quantas maneiras podemos pintar uma bandeira listrada com n listras de igual largura e q cores?*

Exercício 1.36 *De quantas maneiras podemos pintar as arestas de um polígono regular de n lados com q cores?*

Capítulo 2

Representações de Grupos

Neste capítulo, vamos estudar um tipo específico de ações de grupos, as representações lineares, nas quais os elementos do grupo agem como transformações lineares bijetivas em um espaço vetorial dado. Veremos que para o caso de representações de grupos finitos sobre espaços vetoriais complexos, sempre podemos reduzir ao caso de representações unitárias, isto é, nos quais os elementos do grupos agem como transformações unitárias com relação a uma forma sequilinear. Também o problema de se classificar as representações pode ser totalmente resolvido para o caso de grupos finitos, pois as representações irredutíveis podem ser totalmente conhecidas. Finalmente, vamos nos dedicar Às representações irredutíveis de grupos abelianos finitos, veremos que o conjunto destas representações também forma um grupo abeliano com a mesma ordem do grupo original, que é denominado dual de Pontryagyn do grupo.

2.1 Definições Básicas e Exemplos

Durante todo o texto, $\mathbb{V}$ será um espaço vetorial de dimensão n sobre o corpo dos números complexos, $\mathbb{C}$. Denotemos $GL(n, \mathbb{C})$ o grupo das transformações lineares invertíveis neste espaço vetorial.

Definição 2.1 *Uma representação linear (à esquerda) de um grupo G sobre o espaço vetorial complexo $\mathbb{V}$ de dimensão n é um homomorfismo*[1] $\rho : G \to GL(n, \mathbb{C})$.

[1]Existem representações lineares à direita, que se constituem de anti-homomorfismos, isto é, $\rho(g)\rho(h) = \rho(hg)$.

Uma das conseqüências imediatas de termos uma representação linear de um grupo G é que podemos dispor de todos os mecanismos e técnicas próprios da álgebra linear para podermos estudar o grupo. Cada elemento do grupo é, agora, uma transformação linear, em última instância, uma matriz, que pode ser manipulada numericamente de maneira muito mais eficiente do que os elementos do grupo. Resultados de álgebra linear sobre fatoração matricial podem resultar em teoremas sobre fatoração dos elementos de um determinado grupo.

Exemplo 2.1: Considere o grupo aditivo $\mathbb{Z}_n$ e defina para cada $0 \leq k < n$ uma função

$$\begin{array}{rccc} \chi_k : & \mathbb{Z}_n & \to & \mathbb{C} \\ & [x] & \mapsto & e^{\frac{2\pi i k x}{n}}. \end{array}$$

É fácil ver que para cada k, a função χ_k é uma representação unidimensional de $\mathbb{Z}_n$:

$$\chi_k([x])\chi_k([y]) = e^{\frac{2\pi i k x}{n}} e^{\frac{2\pi i k y}{n}} = e^{\frac{2\pi i k (x+y)}{n}} = \chi_k([x]+[y]).$$

Exemplo 2.2: Seja $Aff(\mathbb{R})$ o grupo das transformações afins da reta na reta, isto é, um subgrupo do grupo das bijeções em $\mathbb{R}$ composto pelas transformações lineares não nulas (multiplicação por um número diferente de 0) e translações. Um elemento $g \in Aff(\mathbb{R})$ depende de dois números reais $a, b \in \mathbb{R}$, assim, podemos escrever $g = g_{a,b}$ que age da seguinte forma:

$$g_{a,b}(x) = ax + b.$$

A composta de dois elementos deste grupo resulta em

$$g_{a,b}(g_{c,d}(x)) = g_{a,b}(cx + d) = acx + ad + b = g_{ac,ad+b}(x)$$

Tome, agora a aplicação[2]

$$\begin{array}{rccc} \rho : & Aff(\mathbb{R}) & \to & GL(2,\mathbb{C}) \\ & g_{a,b} & \mapsto & \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}. \end{array}$$

Novamente, um cálculo elementar nos mostra que ρ, de fato, é uma representação do grupo $Aff(\mathbb{R})$.

[2]Note que podemos tomar a aplicação ρ com valores em $GL(n,\mathbb{R})$, ao invés de $GL(n,\mathbb{C})$.

Exercício 2.1 *Verifique que ρ definido acima é uma representação do grupo afim da reta.*

Exemplo 2.3: Seja o grupo de permutações S_n agindo em $\mathbb{C}^n$ da seguinta maneira: Se $\{e_1, e_2, \ldots, e_n\}$ é a base canônica de $\mathbb{C}^n$ então dado $\pi \in S_n$ definimos a transformação linear

$$\begin{array}{rccc} \rho(\pi) : \mathbb{C}^n & \to & \mathbb{C}^n \\ e_i & \mapsto & e_{\pi(i)} \end{array}$$

Exercício 2.2 *Verifique que a aplicação*

$$\begin{array}{rccc} \rho : & S_n & \to & GL(n, \mathbb{C}) \\ & \pi & \mapsto & \rho(\pi), \end{array}$$

onde as transformações $\rho(\pi)$ são as transformações lineares definidas acima, é uma representação do grupo S_n (esta representação é denominada representação definidora de S_n).

Exercício 2.3 *Escreva as matrizes da representação definidora de S_3.*

Antes de continuarmos com mais exemplos, vamos definir um espaço vetorial de extrema importância para a teoria de representações de grupos, a álgebra de grupo.

Definição 2.2 *Seja G um grupo finito. A álgebra de grupo $\mathbb{C}G$ é o espaço vetorial das funções de G a valores nos números complexos*[3]*. Neste espaço vetorial, é introduzido um produto entre as funções, denominado produto de convolução:*

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

Exercício 2.4 *Mostre que este produto é associativo, isto é, $(f * g) * h = f * (g * h)$, para quaisquer $f, g, h \in \mathbb{C}G$.*

Dentre as funções em $\mathbb{C}G$, tomemos as funções características $\delta_x : G \to \mathbb{C}$, definidas como $\delta_x(y) = \delta_{x,y}$, ou seja, $\delta_x(y) = 1$ se $x = y$ e $\delta_x(y) = 0$ se $x \neq y$.

[3] A estrutura de espaço vetorial neste espaço de funções é dada pela soma e multiplicação por escalar, ponto-a-ponto, isto é, $(f + g)(x) = f(x) + g(x)$ e $(\lambda f)(x) = \lambda f(x)$.

Exercício 2.5 *Mostre que o conjunto $\{\delta_x\}_{x\in G}$ forma uma base para o espaço vetorial $\mathbb{C}G$, sendo assim mboxdim$(\mathbb{C}G) = |G|$.*

Exercício 2.6 *Mostre que $\delta_x * \delta_y = \delta_{xy}$, para quaisquer $x, y \in G$.*

Exercício 2.7 *Mostre que a função δ_e é a unidade nesta álgebra, isto é, $\delta_e * f = f * \delta_e = f$ para todo $f \in \mathbb{C}G$.*

a partir destas definições, podemos dar outros dois exemplos de representações lineares de grupos:

Exemplo 2.4: Seja G um grupo finito, considere a aplicação $L : G \to GL(\mathbb{C}G)$ definida como, $L(x)\delta_y = \delta_{xy}$. É fácil ver que L define uma representação linear de G:

$$L(x)(L(y)\delta_z) = L(x)\delta_{yz} = \delta_{xyz} = L(xy)\delta_z.$$

Esta representação é denominada representação regular à esquerda.

Exemplo 2.5: Seja G um grupo finito, considere a aplicação $Ad : G \to GL(\mathbb{C}G)$ definida como $Ad_x\delta_y = \delta_{xyx^{-1}}$. Novamente, é facilmente verificável que Ad é uma representação linear do grupo G sobre $\mathbb{C}G$, esta representação é denominada representação adjunta.

Exercício 2.8 *Mostre que, de fato, Ad é representação linear de G sobre $\mathbb{C}G$. mostre ainda que Ad_x é um morfismo de álgebra para cada $x \in G$, isto é, $Ad_x(f * g) = Ad_x f * Ad_x g$, para todos $f, g \in \mathbb{C}G$.*

Exercício 2.9 *Construa as matrizes das representações regular à esquerda e adjunta do grupo S_3.*

Vamos agora nos restringir a uma classe de representações que possuem um caráter geométrico, as representações unitárias. Primeiramente, precisamos definir uma forma sesquilinear, ou hermitiana, em um espaço vetorial complexo.

Definição 2.3 *Seja $\mathbb{V}$ um espaço vetorial sobre o corpo dos complexos. Uma forma sesquilinear em $\mathbb{V}$ é uma aplicação*

$$\begin{array}{rccc} \langle , \rangle : & \mathbb{V}\times\mathbb{V} & \to \mathbb{C} & \\ & (v,w) & \mapsto & \langle v, w\rangle, \end{array}$$

satisfazendo

1. *Para todos* $v, w_1, w_2 \in \mathbb{V}$ *e* $\lambda \in \mathbb{C}$*, temos* $\langle v, \lambda w_1 + w_2\rangle = \lambda\langle v, w_1\rangle + \langle v, w_2\rangle$.
2. *Para todos* $v, w \in \mathbb{V}$*, temos* $\langle w, v\rangle = \overline{\langle v, w\rangle}$.
3. *Para todo* $v \in \mathbb{V}$*, temos que* $\langle v, v\rangle \geq 0$ *e* $\langle v, v\rangle = 0$ *se, e somente se,* $v = 0$.

Um espaço vetorial munido de uma forma sesquilinear é chamado um espaço vetorial hermitiano.

A existência de uma forma hermitiana em um espaço vetorial introduz neste espaço uma noção de distância dada pela norma de um vetor:

$$\|v\| = \sqrt{\langle v, v\rangle}.$$

Podemos então nos concentrar nas representações de um dado grupo que sejam isometrias nestes espaços vetorias.

Definição 2.4 *Uma transformação unitária em um espaço vetorial hermitiano* $\mathbb{V}$ *é uma transformação linear* $U : \mathbb{V} \to \mathbb{V}$ *tal que*

$$\langle Uv, Uw\rangle = \langle v, w\rangle, \qquad \forall v, w \in \mathbb{V}.$$

Exercício 2.10 *Mostre que toda transformação unitária* U *é uma bijeção com a inversa dada pela hermitiana conjugada* U^**, definida como:*

$$\langle U^* v, w\rangle = \langle v, Uw\rangle.$$

Mostre, com isto, que o conjunto das transformações unitárias em um espaço hermitiano mathbbV é um sub-grupo de $GL(\mathbb{V})$*, denotado por* $U(\mathbb{V})$.

Exercício 2.11 *Verifique que se* $\mathbb{V} = \mathbb{C}^n$ *com a forma sesquilinear usual*

$$\langle v, w\rangle = \sum_{i=1}^{n} v_i w_i,$$

então o grupo das transformações unitárias é isomorfo ao grupo das matrizes unitárias $n \times n$*,* $U(n)$.

Definição 2.5 *Uma representação unitária de um grupo* G *é um homomorfismo entre o grupo* G *e o grupo* $U(\mathbb{V})$ *para algum espaço hermitiano* $\mathbb{V}$.

Exercício 2.12 *Mostre que em uma representação unitária $u : G \to U(\mathbb{V})$, temos que $u(g)^* = u(g^{-1})$.*

Exercício 2.13 *Mostre que, dada uma representação unitária $u : G \to U(\mathbb{V})$, os auto valores da transformação linear $u(g)$, para todo $g \in G$ são raízes da unidade, isto é, $\lambda \in \mathbb{C}$ tais que existe $n \in \mathbb{N}$ com $\lambda^n = 1$.*

O próximo resultado nos mostrará que para o caso de grupos finitos, podemos, sem perda de generalidade, considerar apenas as suas representações unitárias.

Teorema 2.1 *Seja $\rho : G \to GL(\mathbb{V})$ uma representação de um grupo finito G em um espaço hermitiano $\mathbb{V}$. Então existe uma forma sesquilinear em $\mathbb{V}$ que torna ρ uma representação unitária.*

Demonstração: Defina a aplicação

$$\begin{array}{rccc} \langle\langle , \rangle\rangle : & \mathbb{V} \times \mathbb{V} & \to & \mathbb{C} \\ (v, w) & \mapsto & \langle\langle v, w \rangle\rangle & \end{array}$$

como

$$\langle\langle v, w \rangle\rangle = \sum_{g \in G} \langle \rho(g)v, \rho(g)w \rangle.$$

Note que esta soma só é finita de o grupo G for finito. É fácil ver que a nova aplicação $\langle\langle , \rangle\rangle$ é uma forma sesquilinear (Verifique isto) e que para qualquer $h \in G$ temos

$$\begin{aligned} \langle\langle \rho(h)v, \rho(h)w \rangle\rangle &= \sum_{g \in G} \langle \rho(g)\rho(h)v, \rho(g)\rho(h)w \rangle = \\ &= \sum_{g \in G} \langle \rho(gh)v, \rho(gh)w \rangle = \\ &= \sum_{x \in G} \langle \rho(x)v, \rho(x)w \rangle = \\ &= \langle\langle v, w \rangle\rangle. \end{aligned}$$

Logo, a representação ρ é unitária com relação a esta nova forma sesquilinear. ■

Exemplo 2.6: Não apenas a prova deste teorema depende do fato de o grupo ser finito, mas o próprio resulltado depende deste fato também. Por exemplo, considere $G = \mathbb{Z}$ e $\rho(n) = a^n$ para algum $a \in \mathbb{C}^*$. Esta representação só é unitária se $|a| = 1$, com relação à única forma sesquilinear possível em $\mathbb{C}$: $\langle z, w\rangle = \bar{z}w$.

Definição 2.6 *Duas representações unitárias $u : G \to U(\mathbb{V})$ e $v : G \to U(\mathbb{W})$ são ditas unitariamente equivalentes se existe uma transformação unitária*[4] *$T : \mathbb{V} \to \mathbb{W}$ tal que $v(g) = Tu(g)T^*$ para todos os elementos $g \in G$.*

Vamos nos ocupar apenas com a classificação de classes de representações unitariamente equivalentes de um dado grupo G.

Finalmente chegamos a uma questão importante: Será que existem representações fundamentais de forma que todas as outras pudessem ser geradas a partir destas? Estamos a procura de "átomos de representações", que funcionem da mesma maneira que os números primos para os números inteiros. Estas representações recebem um nome importante e desempenham um papel central na teoria de representações, são as representações irredutíveis.

2.2 Representações Irredutíveis

Uma representação unitária u de um grupo G em um espaço $\mathbb{V}$ pode deixar sub-espaços invariantes, isto é, sub-espaços vetoriais $\mathbb{W} \subseteq \mathbb{V}$ tais que $u(g)w \in \mathbb{W}$ para todo $g \in G$ e todo $w \in \mathbb{W}$. A proposição a seguir nos mostra que se temos um sub-espaço invariante por uma representação unitária define outro sub-espaço invariante complementar a este.

Proposição 2.1 *Seja $u : G \to U(\mathbb{V})$ uma representação unitária e $\mathbb{W} \subseteq \mathbb{V}$ um sub-espaço invariante por esta representação. Então o complemento ortogonal*

$$\mathbb{W}^\perp = \{v \in \mathbb{V} | \langle v, w\rangle = 0, \forall w \in \mathbb{W}\}$$

é também um sub-espaço invariante por u.

Demonstração: Sejam $g \in G$, $v \in \mathbb{W}^\perp$ e $w \in \mathbb{W}$, então

$$\langle u(g)v, w\rangle = \langle v, u(g)^* w\rangle = \langle v, u(g^{-1})w\rangle = 0$$

[4]Portanto um isomorfismo.

pois $u(g^{-1}) \in \mathbb{W}$, assim $u(g)v \in \mathbb{W}^{\perp}$. ■

Portanto, dada uma representação unitária em um espaço vetorial, podemos decompor este espaço em somas diretas de sub-espaços invariantes e continuar esta decomposição até que não seja mais possível encontrar sub-espaços invariantes, assim teremos as representações irredutíveis.

Definição 2.7 *Uma representação $\rho : G \to GL(\mathbb{V})$ é dita ser irredutível se os únicos sub-espaços invariantes são $\{0\}$ e $\mathbb{V}$.*

Por outro lado, dadas duas representações unitárias $\rho : G \to U(\mathbb{V})$ e $\eta : G \to U(\mathbb{W})$, podemos definir uma nova representação no espaço vetorial soma direta $\mathbb{V} \oplus \mathbb{W}$ unitária com respeito à nova forma sesquilinear

$$\langle (v_1, w_1), (v_1, w_2) \rangle = \langle v_1, v_2 \rangle + \langle w_1, w_2 \rangle. \tag{2.1}$$

Esta nova representação, $\rho \oplus \eta : g \to U(\mathbb{V} \oplus \mathbb{W})$ é dada por

$$\rho \oplus \eta(g)(v, w) = (\rho(g)v, \eta(g)w). \tag{2.2}$$

Assim, conhecendo-se as representações irredutíveis, poderemos construir as demais representações através de somas diretas. Assim que demonstrarmos que todas as representações de dimensão finita de um grupo finito G podem ser obtidas desta maneira teremos mostrado que as representações irredutíveis (daqui para frente, chamadas simplesmente de irreps) são os constituintes básicos da teoria de representações. Vamos denotar por $\widehat{G}$ o conjunto das classes de equivalência das irreps unitárias do grupo G.

Exercício 2.14 *Mostre que a forma (2.1) é realmente uma forma sesquilinear no espaço soma direta e que a aplicação (2.2) é, de fato uma representação unitária com respeito a esta forma.*

Teorema 2.2 *Toda representação unitária de dimensão finita de um grupo finito pode ser decomposta como soma direta de irreps.*

Demonstração: Vamos demonstrar por indução sobre a dimensão de $\mathbb{V}$. Se $\dim\mathbb{V} = 1$, os únicos sub-espaços vetoriais possíveis são o sub-espaço nulo e o espaço inteiro. Logo, toda representação de G sobre $\mathbb{V}$ é irredutível. Suponha que toda representação de G sobre $\mathbb{V}$ seja decomposta como soma direta de irreps para $1 \leq \dim\mathbb{V} < n$ e considere $\mathbb{V}$ um espaço vetorial de

dimensão n. Ou esta representação é uma irrep, o que resulta na conclusão do teorema ou existe um sub-espaço invariante $\mathbb{W} \subseteq \mathbb{V}$ diferente do espaço nulo e do espaço todo. Assim, o sub-espaço $\mathbb{W}^{\perp}$ também é invariante e podemos escrever

$$\mathbb{V} = \mathbb{W} \oplus \mathbb{W}^{\perp}.$$

Por sua vez, estes dois espaços, $\mathbb{W}$ e $\mathbb{W}^{\perp}$ são espaços de dimensão menor que n, que por hipótese, ambos podem ser decompostos como somas diretas de irreps, o que nos leva à conclusão do teorema. ■

Os próximos dois resultados mostrarão relações que existem entre diferentes irreps.

Teorema 2.3 *(Lema de Schur, primeira formulação) Seja $\rho : G \to U(\mathbb{V})$ uma irrep e seja $A \in \mathcal{L}(\mathbb{V})$ tal que*

$$A.\rho(g) = \rho(g).A, \qquad \forall g \in G.$$

Então $A = \lambda I$, onde I é a transformação linear identidade em $\mathbb{V}$.

Demonstração: Podemos supor, sem perda de generalidade que $A^* = A$, ou seja que A é auto-adjunto. Isto se deve ao fato que todo operador linear em $\mathbb{V}$ pode ser decomposto da seguinte forma:

$$A = B + iC = \left(\frac{A + A^*}{2}\right) + i\left(\frac{A - A^*}{2i}\right),$$

sendo ambos, B e C, auto-adjuntos. Seja λ um auto-valor não nulo de A (se todos os auto-valores de A são iguais a 0, então já terémos provado o resultado, pois $A = 0.I$) e $v \in \mathbb{V}$ um auto-vetor associado a λ, então

$$(A - \lambda I)\rho(g)v = \rho(g)(A - \lambda I)v = 0.$$

Portanto $\rho(g)v$ é auto vetor de A com auto-valor λ para qualquer $g \in G$. Como $\lambda \neq 0$, temos que o sub-espaço dos auto-vetores com auto-valor λ é invariante pela representação. Como estamos supondo $A \neq 0$ temos que todo o espaço $\mathbb{V}$ é de auto-vetores de A com auto-valor λ. Assim $A = \lambda I$. ■

Teorema 2.4 *(Lema de Schur, segunda formulação) Sejam* $\rho : G \to U(\mathbb{V})$ *e* $\eta : G \to U(\mathbb{W})$ *duas irreps e* $T : \mathbb{V} \to \mathbb{W}$ *uma transformação linear tal que*

$$\eta(g).T = T.\rho(g), \qquad \forall g \in G.$$

Então $T \equiv 0$ *ou* T *é um isomorfismo.*

Demonstração: Considere o sub-espaço $\ker(T) \subseteq \mathbb{V}$, para qualquer $g \in G$, e qualquer $v \in \ker(T)$, temos

$$T.\rho(g)v = \eta(g).Tv = 0.$$

Portanto $\rho(g)v \in \ker(T)$, ou seja, este é um sub-espaço invariante pela irrep ρ, portanto $\ker(T) = \mathbb{V}$, que implica $T \equiv 0$, ou $\ker(T) = \{0\}$, o que implica que T é injetiva. Considere agora o sub-espaço $\mathrm{Im}(T) \subseteq \mathbb{W}$, este é um sub-espaço invariante por η:

$$\eta(g).Tv = T.\rho(g)v \in \mathrm{Im}(T)$$

Se $T \equiv 0$, então $\mathrm{Im}(T) = \{0\}$, se T é injetiva, então a única possibilidade é que $\mathrm{Im}(T) = \mathbb{W}$ e portanto também é sobrejetiva, o que implica que T é um isomorfismo. ■

Corolário 2.1 *Todas as irreps de um grupo abeliano são unidimensionais.*

Demonstração: Seja $\rho : G \to U(\mathbb{V})$ uma ireep unitária, com G sendo um grupo abeliano. Para todo elemento $h \in G$ temos

$$\rho(h)\rho(g) = \rho(g)\rho(h), \qquad \forall g \in G.$$

Assim, de acordo com a primeira forma do lema de Schur, cada $\rho(g)$ é um múltiplo da identidade, assim todo sub-espaço unidimensional de $\mathbb{V}$ é invariante. Sendo assim, a representação ρ somente será irredutível se $\dim(\mathbb{V}) = 1$. ■.

2.3 Caracteres e Grupo Dual

No que se segue, estudaremos com mais detalhes apenas as representações unitárias irredutíveis dos grupos abelianos finitos. Vimos como conseqüência

do Lema de Schur que as irreps de um grupo abeliano são unidimensionais, assim, uma irrep de um grupo abeliano G é um homomorfismo de grupos

$$\chi : G \to GL(1, \mathbb{C}),$$

ou ainda, é uma função

$$\chi : G \to \mathbb{C}^{\times},$$

onde $\mathbb{C}^{\times}$ é o conjunto dos elementos invertíveis de $\mathbb{C}$ (que são os números complexos não nulos, pois $\mathbb{C}$ é um corpo), satisfazendo

$$\chi(g)\chi(h) = \chi(gh).$$

Restringindo um pouco mais, a condição de a irrep ser unitária nos garante que a função toma valores na circunferência unitária,

$$\mathbb{S}^1 = \{z \in \mathbb{C} | \quad |z| = 1\},$$

ou seja, $|\chi(g)| = 1$ para todo elemento $g \in G$.

Definição 2.8 *Uma representação unitária unidimensional de um grupo é denominada um caracter do grupo.*

Proposição 2.2 *Qualquer caracter de um grupo finito G, abeliano ou não abeliano, associa a cada elemento $g \in G$ uma raiz n-ésima da unidade, onde $n = |G|$.*

Demonstração: Como foi mostrado no capítulo primeiro, todo elemento g de um grupo finito G, com exatamente n elementos satisfaz $g^n = e$. Seja $\chi : G \to \mathbb{S}^1$ um caracter do grupo G, então

$$1 = \chi(e) = \chi(g^n) = (\chi(g))^n,$$

o que prova nossa afirmação. ■

Como para um grupo abeliano todas as irreps são caracteres, então o conjunto $\widehat{G}$ é igual ao conjunto dos seus caracteres. O próximo resultado nos mostrará que o conjunto dos caracteres é também um grupo abeliano. Para a sua demonstração utilizaremos um outro teorema estrutural sobre grupo abelianos finitos, o qual faremos menção, mas não o demosntraremos, por envolver ainda alguns outros conteúdos que não serão menciionados aqui:

Teorema 2.5 *Todo grupo abeliano finito é isomorfo ao produto direto de grupos cíclicos.*

Teorema 2.6 *Seja G um grupo abeliano finito, então $\widehat{G}$ também é um grupo abeliano de mesma ordem.*

Demonstração: Sejam $\chi, \xi \in \widehat{G}$, vamos mostrar que a função produto $\chi\xi$ também é um caracter. De fato,

$$\begin{aligned}(\chi\xi)(gh) &= \chi(gh)\xi(gh) = \chi(g)\chi(h)\xi(g)\xi(h) = \\ &= \chi(g)\xi(g)\chi(h)\xi(h) = (\chi\xi)(g)(\chi\xi)(h).\end{aligned}$$

A associatividade do produto decorre facilmente da associatividade do produto em $\mathbb{C}$. O elemento neutro deste grupo é o caracter identicamente igual a 1, isto é, $\mathbf{1}(g) = 1$ para todo elemento $g \in G$. Finalmente, dado um caracter $\chi \in \widehat{G}$, o seu inverso será o caracter χ^{-1} que opera como

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

A verificação de que realmente este é o inverso é direta:

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

Com isto, temos que $\widehat{G}$ é um grupo. O produto ponto a ponto entre funções nos garante que este grupo é abeliano.

Para verificarmos a ordem do grupo $\widehat{G}$, consideremos primeiramente o caso em que G é um grupo cíclico:

$$G = \{a, a^2, a^3, \ldots, a^{n-1}a^n = e\}.$$

Neste caso, conhecendo-se o valor do caracter aplicado ao elemento a, podemos conhecer o valor deste caracter aplicado a qualquer outro elemento do grupo, em outras palavras, o caracter está unicamente determinado pelo seu valor no elemento a. Como um caracter somente pode mandar este elemento em uma raiz n-ésima da unidade, conforme demonstrado anteriormente, então temos n possibilidades distintas para caracteres de G, o que implica que $|\widehat{G}| = |G| = n$.

Se G não é cíclico, podemos utilizar o resultado que G é isomorfo a um produto direto de grupos cíclicos, isto é equivalente a dizer que existem

elementos a_1, a_2, ..., a_r e números inteiros positivos n_1, n_2, ..., n_r, todos maiores que 1 tais que

$$a_1^{n_1} = a_2^{n_2} = \cdots = a_r^{n_r} = e$$

e de forma que todo elemento de G pode ser escrito como

$$g = a_1^{k_1} \cdot a_2^{k_2} \cdots a_r^{k_r},$$

com $0 \leq k_i < n_i$ e $i = 1, \ldots, r$ (Verifique que $n = n_1.n_2.\ldots.n_r$). Um caracter do grupo G vai poder associar a cada gerador a_i uma n_i-ésima raiz da unidade. Portanto, teremos $n_1.n_2.\ldots.n_r = n$ possibilidades de caracteres distintos, o que nos leva a concluir que $|\widehat{G}| = |G| = n$. ■

Exercício 2.15 *Dado um grupo abeliano finito G e um elemento $g \neq e$, verifique que existe um caracter $\chi \in \widehat{G}$ tal que $\chi(g) \neq 1$.*

Definição 2.9 *Dado G um grupo abeliano finito, o grupo $\widehat{G}$, dos caracteres de G, é denominado grupo dual de Pontryagyn de G.*

Os últimos resultados deste capítulo são concernentes a relações aritméticas obedecidas pelos caracteres de um grupo finito

Teorema 2.7 *Seja G um grupo finito e $\widehat{G}$ seu grupo dual. Então*

$$\textit{(i)} \quad \sum_{g\in G} \chi(g) = \begin{cases} |G|, & se \quad \chi = \mathbf{1}, \\ 0, & se \quad \chi \neq \mathbf{1} \end{cases}$$

$$\textit{(ii)} \quad \sum_{\chi\in \widehat{G}} \chi(g) = \begin{cases} |G|, & se \quad g = e, \\ 0, & se \quad g \neq e \end{cases}$$

Demonstração: (i) É fácil ver que se $\chi = \mathbf{1}$ então $\sum_{g\in G} \chi(g) = |G|$, pois $\mathbf{1}(g) = 1$ para todo $g \in G$. Agora, seja $\chi \neq \mathbf{1}$, então existe $h \in G$ tal que $\chi(h) \neq 1$, assim

$$\chi(h) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(h)\chi(g) = \sum_{g\in G} \chi(g).$$

Como $\chi(h) \neq 1$, temos que ter $\sum_{g\in G} \chi(g) = 0$.

(ii) Novamente, é fácil ver que se $g = e$, teremos $\sum_{\chi\in\widehat{G}} \chi(g) = |G|$, pois $\chi(e) = 1$ para todo caracter $\chi \in \widehat{G}$. Agora, assuma que $g \neq e$, então existe um caracter $\xi \in \widehat{G}$ tal que $\xi(g) \neq 1$, assim

$$\xi(g)\sum_{\chi\in\widehat{G}} \chi(g) = \sum_{\chi\in\widehat{G}} \xi(g)\chi(g) = \sum_{\chi\in\widehat{G}} (\xi\chi)(g) = \sum_{\chi\in\widehat{G}} \chi(g).$$

E novamente, como $\xi(e) \neq 1$, temos que $\sum_{\chi\in\widehat{G}} \chi(g) = 0$. ■

Exercício 2.16 *Mostre as seguintes identidades envolvendo os caracteres de um grupo abeliano finito G:*

$$\textit{(i)} \quad \sum_{g\in G} \xi(g)\chi(g) = \begin{cases} |G|, & se \quad \chi = \xi, \\ 0, & se \quad \chi \neq \xi \end{cases}$$

$$\textit{(ii)} \quad \sum_{\chi\in\widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |G|, & se \quad g = h, \\ 0, & se \quad g \neq h \end{cases}$$

Agora estamos com as informações suficientes sobre representações de grupo para que possamos demonstrar o teorema de Dirichlet, o que faremos no capítulo seguinte.

Capítulo 3

O Teorema de Dirichlet

Neste capítulo, demonstraremos o famoso teorema de Dirichlet que pode ser enunciado da seguinte maneira:

Teorema 3.1 *(Dirichlet) Se* $mdc(a, r) = 1$*, então a progressão aritmética* $a + nr$ *contém uma quantidade infinita de números primos.*

De fato, pode-se demonstrar além e medirmos o comportamento assintótico da função distribuição dos números primos na progressão aritmética.

Teorema 3.2 *(Siegel-Walfisz-Paige) O número* $\pi(x; a, r)$ *de primos* $p \leq x$ *na seqüência aritmética* $a+nr$*, para cada um dos* $\varphi(r)$ *números a menores ou iguais a* r *primos com* r *é assintoticamente independente de* a*, e* $\pi(x; a, r) \sim x/(\varphi(r) \ln x)$.

Vamos iniciar mostrando alguns casos particulares deste resultado para podermos depois nos dedicar às técnicas necessárias para a demonstração do primeiro teorema. Este resultado e muitos outros relacionados, como o teorema dos números primos, de Haddamard e De La Valée Pousin, fazem parte de um ramo da matemática conhecido como teoria analítica dos números, que utiliza técnicas de análise matemática como séries de potências e funções analíticas complexas para a resolução de problemas de teoria de números.

3.1 Alguns Pesultados Particulares

Nesta seção vamos demonstrar dois resultados sobre primos em progressões aritméticas, a saber, que existem infinitos primos da forma $4k + 3$ e infinitos primos da forma $4k + 1$.

Teorema 3.3 *Existem infinitos primos da forma* $4k+3$.

Demonstração: Suponha que os números 3, 7, ..., p_n seja a lista completa dos números primos da forma $4k+1$ e crie o número

$$N = 4.3.7.\ldots p_n - 1.$$

Este número é da forma $4k+1$ e é maior que qualquer um dos primos da lista, logo N não é primo. Então, N é o produto de primos ímpares

$$N = q_1.q_2.\ldots q_l,$$

dos quais, algum deles tem que ser da forma $4k+3$, pois se fossem todos primos da forma $4k+1$, então N também o seria. Seja q_i um desses primos da forma $4k+3$ que são divisores de N, então q_i não pode ser divisor de $N+1$, mas todos os primos da forma $4k+3$ são divisores de $N+1$, pois

$$N+1 = 4.3.7.\ldots.p_n.$$

Desta contradição, podemos concluir o resultado. ■

O próximo resultado possui uma demonstraçõa um pouco mais elaborada.

Teorema 3.4 *Existem infinitos números da forma* $4k+1$.

Demonstração: Suponha que os números 5, 13, 17, ... , p_n seja a lista completa de primos da forma $4k+1$. Defina N como sendo o número

$$N = 5.13.17.\ldots p_n,$$

e considere o número N^2+1. Esta número não é primo, pois é par, e nenhum número primo da lista dos primos da forma $4k+1$ dividem N^2+1 pois são divisores de N^2. Assim, somente restam primos da forma $4k+3$ para serem divisores do número N^2+1, mas isto significa que

$$N^2 \equiv -1(\mathrm{mod}p).$$

Isto contraria um resultado importante em teoria de números que diz que a equação

$$x^2 \equiv -1(\mathrm{mod}p),$$

para p primo tem soução se, e somente se $p \equiv 1(\mathrm{mod}4)$. Assim temos o resultado. ■

Para generalizarmos o resultado da infinitude de primos da forma $a+nr$ para $\mathrm{mdc}(a,r) = 1$ temos que introduzir novas técnicas oriundas da análise matemática, é o que faremos na próxima seção.

3.2 Séries de Dirichlet

Dada uma função aritmética $f : \mathbb{Z}_+^* \to \mathbb{C}$ (veja o apêndice A para mais detalhes sobre funções aritméticas) podemos associar a esta função uma série infinita,

$$L(f,s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad s \in \mathbb{C}.$$

Esta série é denominada série de Dirichlet de f.

Proposição 3.1 *Se f é uma função aritmética limitada, então $L(f,s)$ converge absolutamente para $\Re(s) > 1$, onde $\Re(s)$ é a parte real do número complexo s.*

Demonstração: Escreva $s = x + iy$, e seja $M > 0$ tal que $|f(n)| \leq M$ para todo então

$$\begin{aligned} \sum_{n=1}^{\infty} \left| \frac{f(n)}{n^s} \right| &\leq \sum_{n=1}^{\infty} \frac{M}{|n^{x+iy}|} \leq \\ &\leq M. \sum_{n=1}^{\infty} \frac{1}{|n^x||e^{i(\ln n)y}|} = \\ &= M. \sum_{n=1}^{\infty} \frac{1}{n^x}. \end{aligned}$$

Sabemos que a série da última linha somente converge somente para $x > 1$, ou seja, para $\Re(s) > 1$, portanto, temos a convergência absoluta da série $L(f,s)$ para $\Re(s) > 1$. ■

Então, para os valores de $s \in \mathbb{C}$ para os quais a série $L(f,s)$ convergem, podemos definir uma nova função $L(f) : D \to \mathbb{C}$, onde

$$D = \{s \in \mathbb{C} | \Re(s) > 1\},$$

associando a cada $s \in D$ o valor da série $L(f,s)$, esta é a função L de Dirichlet. Esta função é contínua pois pode ser pensada como o limite de uma seqüência de funções que corresponde às somas parciais da série. Como a convergência é absoluta ponto a ponto na série, então, pelo teste M, de Weierstrass, podemos garantir que a convergência das funções é uniforme

no domínio, portanto, a função $L(f)$ é contínua. Note que para a função aritmética $N_0(n) = n^0 = 1$, a função L de Dirichlet, resulta em

$$L(N_0, s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s),$$

que é a função zeta de Riemann.

Uma propriedade interessante das funções L de Dirichlet é que o produto de duas funções L, associadas a duas funções aritméticas é igual à função L do produto de convolução entre as funções (veja no apêndice A a definição de produto de convolução de duas funções aritméticas).

Proposição 3.2 *Sejam $f, g : \mathbb{Z}_+^* \to \mathbb{C}$ duas funções aritméticas e $L(f)$ e $L(g)$ suas respectivas funções L de Dirichlet, então*

$$L(f, s)L(g, s) = L(f * g, s).$$

Demonstração: Esta verificação pode ser feita por cálculo direto.

$$\begin{aligned} L(f,s)L(g,s) &= \left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{g(m)}{m^s}\right) = \\ &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s} = \\ &= \sum_{n=1}^{\infty} \frac{\sum_{d|n} f(d)g\left(\frac{n}{d}\right)}{n^s} = \\ &= \sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s} = \\ &= L(f*g,s). \qquad \blacksquare \end{aligned}$$

Para a demonstração do teorema da infinitude de números primos na progresssão aritmética $a + nr$ com $\text{mdc}(a, r) = 1$, Dirichlet construiu funções L associadas a novas funções aritméticas definidas a partir de caracteres de grupos abelianos[1]. Mais precisamente, considere o grupo multiplicativo

[1]É claro que o próprio Dirichlet não possuia esta nomenclatura, que foi inventada a partir do seu trabalho. Estamos nestas notas tentando explicitar a relação deste teorema com representações de grupo e não tentando reconstruir a sua trajetória histórica.

dos elementos invertíveis em $\mathbb{Z}_r$, já sabemos que este grupo é formado pelas classes dos números que são primos com r, e portanto é um grupo abelianno que possui $\varphi(r)$ elementos, no capítulo 1 denotamos este grupo por $\mathbb{Z}_r^\times$. Do capítulo 2, sabemos que o grupo abeliano dual, $\widehat{\mathbb{Z}_r^\times}$, consistindo dos caracteres do grupo $\mathbb{Z}_r^\times$, possui a mesma ordem que o grupo, portanto, existem $\varphi(r)$ diferentes caracteres existentes. Para cada caracter $\chi \in \widehat{\mathbb{Z}_r^\times}$, defina a função aritmética $\chi : \mathbb{Z}_+^* \to \mathbb{C}$ como

$$\chi(n) = \begin{cases} \chi([n]), & \text{se} \quad \text{mdc}(n,r) = 1 \\ 0, & \text{se} \quad \text{mdc}(n,r) > 1. \end{cases}$$

Exercício 3.1 *Verifique que a função aritmética χ, definida acima é totalmente multiplicativa, isto é, $\chi(mn) = \chi(m)\chi(n)$ para quaisquer inteiros positivos m e n.*

Como esta função aritmética é limitada, portanto a função L de Dirichlet, $L(\chi, s)$ é uma função bem definida para todo $s \in \mathbb{C}$ tal que $\Re(s) > 1$. O fato das funções χ serem totalmente multiplicativas nos garante o seguinte resultado, extremamente importante para o seu uso em teoria de números.

Teorema 3.5 *Para $\Re(s) > 1$, a função L de Dirichlet de χ satisfaz à seguinte igualdade:*

$$L(\chi, s) = \prod_{p\, primo} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

Demonstração: Antes de verificarmos explicitamente os cálculos, note que, como χ é totalmente multiplicativa, então $\chi(p^n) =^(\chi(p))^n$, para qualquer primo p. Considere agora um número primo P, vamos calcular o produto para todos os primos $p \leq P$

$$\begin{aligned} \prod_{p\leq P} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} &= \prod_{p\leq P} \left(1 + \frac{\chi(p)}{p^s} + \frac{(\chi(p))^2}{p^{2s}} + \cdots\right) = \\ &= \prod_{p\leq P} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right) = \\ &= \sum_{n\in S} \frac{\chi(n)}{n^s}, \end{aligned}$$

onde S é o conjunto dos números inteiros positivos que não possuem fatores primos maiores que P. Conseqüentemente,

$$L(\chi, s) - \prod_{p \leq P} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n \in T} \frac{\chi(n)}{n^s},$$

onde T é o complementar de S nos números inteiros positivos, ou seja, é o conjunto dos números inteiros positivos cujos fatores primos são estritamente maiores que P, em particular, isto implica que a soma se inicia em um número $n > P$. Finalmente, denotando $s = x + iy$, com $x > 1$

$$\left|\sum_{n \in T} \frac{\chi(n)}{n^s}\right| \leq \sum_{n \in T} \frac{|\chi(n)|}{|n^s|} = \sum_{n \in T} \frac{|\chi(n)|}{n^x} = \sum_{n \in T} \frac{1}{n^x} \leq \sum_{n > P} \frac{1}{n^x}.$$

Como sabemos que a série

$$\sum_{n=1}^{\infty} \frac{1}{n^x}$$

converge para $x > 1$,então temos que

$$\lim_{P \to \infty} \sum_{n > P} \frac{1}{n^x} = 0.$$

O que resulta em

$$L(\chi, s) = \lim_{P \to \infty} \prod_{p \leq P} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

que equivale ao resultado. ■

Teorema 3.6 *Seja $\chi_0 = \mathbf{1}_{\mathbb{Z}_r^\times}$ o caracter que associa a todo elemento de $\mathbb{Z}_r^\times$ o número 1. Então, para $\Re(s) > 1$ temos*

$$L(\chi_0, s) = \prod_{p | r} \left(1 - \frac{1}{p^s}\right) \cdot \zeta(s),$$

onde o produto é tomado sobre os fatores primos de r, e

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

é a função zeta de Riemann.

Demonstração: Pelo teorema anterior demonstramos que

$$L(\chi_0, s) = \prod_{p\,\text{primo}} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1}.$$

No entanto, $\chi_0(p) = 1$, exceto quando $p|r$, neste caso $\chi_0(p) = 0$, então

$$\begin{aligned}
\zeta(s) &= \prod_{p\,\text{primo}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p|r} \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{p\nmid r} \left(1 - \frac{1}{p^s}\right)^{-1} = \\
&= \prod_{p|r} \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{p\nmid r} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \\
&= \prod_{p|r} \left(1 - \frac{1}{p^s}\right)^{-1} \cdot L(\chi_0, s).
\end{aligned}$$

Como o produtório do lado direito da igualdade é de um número finito de fatores (pois r possui apenas uma quantidade finita de fatores primos), então pode ser invertida. Com isto, obtemos o resultado. ■

Para os próximos teoremas, vamos necessitar de alguns resultados analíticos a respeito da função zeta, cuja demonstração fugiria ao escopo destas notas, para mais detalhes consulte as referências [5][6].

Teorema 3.7 *Para $\Re(s) > 0$ a função zeta é analítica, exceto no polo de primeira ordem $s = 1$ com resíduo $a_{-1} = 1$, e possui representação*

$$\zeta(s) = \frac{1}{s-1} + 1 - s\int_1^\infty \frac{x - \lfloor x \rfloor}{x^{s+1}} dx,$$

onde $\lfloor x \rfloor$ é o valor da função maior inteiro de x. □

Corolário 3.1 $\lim_{s\to 1}(s-1)\zeta(s) = 1.$ □

Como conseqüências do teorema 3.6 e do corolário 3.1, podemos obter o seguinte resultado para $L(\chi_0, s)$:

Corolário 3.2 $\lim_{s\to 1}(s-1)L(\chi_0, s) = \frac{\varphi(r)}{r}.$

Demonstração: Utilizando o teorema 3.6 e o corolário 3.1, temos

$$\begin{aligned}\lim_{s\to 1}(s-1)L(\chi_0,s) &= \lim_{s\to 1}(s-1)\zeta(s)\prod_{p|r}\left(1-\frac{1}{p^s}\right) = \\ &= \prod_{p|r}\left(1-\frac{1}{p}\right) = \frac{\varphi(r)}{r}.\end{aligned}$$

Na última igualdade, utilizamos a expressão para a função totiente de Euler obtida no exemplo A.3 do apêndice A. ■

Corolário 3.3 *A função $L(\chi_0, s)$ admite extensão para todo plano complexo como uma função meromorfa com polo simples em $s = 1$ cujo resíduo é $\frac{\varphi(r)}{r}$.*

Demonstração: Esta é uma combinação dos resultados do corolário 3.2 e do teorema 3.7. ■

Vale a pena ressaltar que o corolário acima nos diz que a função $L(\chi_0, s)$ pode ser escrita da seguinte forma:

$$L(\chi_0,s) = \frac{\varphi(r)}{r}\frac{1}{s-1} + \sum_{i=0}^{\infty} c_i(s-1)^i, \tag{3.1}$$

onde a série infinita é convergente para todo $s \in \mathbb{C}$.

Vamos analisar, agora, a convergência das funções $L(\chi, s)$ para $\chi \neq \chi_0$. Neste caso, veremos que a representação da função $L(\chi, s)$ como série é válida para todos os pontos s, do plano complexo tais que $\Re(s) > 0$.

Lema 3.1 *Para $\chi \neq \chi_0$ temos a seguinte desigualdade*

$$\left|\sum_{n=l+1}^{m}\chi(n)\right| \leq \varphi(r),$$

para $l \leq m$ números inteiros positivos.

Demonstração: Lembremo-nos da relação de ortogonalidade demonstrada no teorema 2.7,

$$\sum_{g\in G}\chi(g) = \begin{cases} |G|, & \text{se} \quad \chi = \chi_0 \\ 0, & \text{se} \quad \chi \neq \chi_0. \end{cases}$$

assim, se $\chi \in \widehat{\mathbb{Z}_r^\times}$ é um caracter tal que $\chi \neq \chi_0$, então

$$\sum_{n=1}^{n+r} \chi(n) = \sum_{[n]\in\mathbb{Z}_r^\times} \chi([n]) = 0.$$

Agora, se $m = l + qr + k$, com $0 \leq k < r$, teremos

$$\sum_{n=l+1}^{m} \chi(n) = \sum_{n=l+1}^{l+qr} \chi(n) + \sum_{n=l+qr+1}^{m} \chi(n) = \sum_{n=l+qr+1}^{m} \chi(n),$$

e portanto

$$\left|\sum_{n=l+1}^{m} \chi(n)\right| \leq \sum_{n=l+1}^{m} |\chi(n)| \leq \sum_{[n]\in\mathbb{Z}_r^\times} |\chi([n])| = \varphi(r). \qquad \blacksquare$$

Teorema 3.8 *Se $\chi \neq \chi_0$, então a série $\sum_{n=1} \infty^{\frac{\chi(n)}{n^s}}$ converge para $\Re(s) > 0$.*

Demonstração: Vamos mostrar que a seqüência das somas parciais

$$\left(\sum_{n=1}^{N} \frac{\chi(n)}{n^s}\right)_{N\in\mathbb{Z}_+^*},$$

é de Cauchy. Sejam $1 \leq u \leq v$, com $u, v \in \mathbb{Z}_+^*$ e defina

$$S(x) = \sum_{1\leq n\leq x} \chi(n).$$

Assim

$$\begin{aligned}
\sum_{u\leq n\leq v} \frac{\chi(n)}{n^s} &= \sum_{u\leq n\leq v} \frac{S(n) - S(n-1)}{n^s} = \\
&= \sum_{n=u}^{v-1} S(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + \frac{S(v)}{v^s} - \frac{S(u-1)}{u^s} = \\
&= \sum_{n=u}^{v-1} S(n)s\int_n^{n+1} \frac{dx}{x^{s+1}} + \frac{S(v)}{v^s} - \frac{S(u-1)}{u^s} = \\
&= \sum_{n=u}^{v-1} s\int_n^{n+1} \frac{S(x)dx}{x^{s+1}} + \frac{S(v)}{v^s} - \frac{S(u-1)}{u^s} = \\
&= s\int_u^v \frac{S(x)dx}{x^{s+1}} + \frac{S(v)}{v^s} - \frac{S(u-1)}{u^s}.
\end{aligned}$$

Do lema anterior, sabemos que $|S(u)| \leq \varphi(r)$, para qualquer $u \in \mathbb{Z}_+^*$. É fácil ver que o módulo da integral

$$\int_u^v \frac{sS(x)dx}{x^{s+1}},$$

satisfaz à desigualdade

$$\begin{aligned}\left|\int_u^v \frac{sS(x)dx}{x^{s+1}}\right| &\leq |s|\varphi(r)\int_u^v \frac{dx}{x^{\Re(s)+1}} \leq \\ &\leq \frac{|s|\varphi(r)}{\Re(s)}\left(\frac{1}{u^{\Re(s)}} - \frac{1}{v^{\Re(s)}}\right) \leq \\ &\leq \frac{|s|\varphi(r)}{\Re(s)}\frac{1}{u^{\Re(s)}}.\end{aligned}$$

Assim, podemos ver que

$$\begin{aligned}\left|\sum_{n=1}^{v}\frac{\chi(n)}{n^s} - \sum_{n=1}^{u}\frac{\chi(n)}{n^s}\right| &= \left|\sum_{u\leq n\leq v}\frac{\chi(n)}{n^s}\right| \leq \\ &\leq \frac{|s|\varphi(r)}{\Re(s)}\frac{1}{u^{\Re(s)}} + \left|\frac{S(v)}{v^s}\right| + \left|\frac{S(u-1)}{u^s}\right| \leq \\ &\leq \frac{|s|\varphi(r)}{\Re(s)}\frac{1}{u^{\Re(s)}} + \frac{2\varphi(r)}{u^{\Re(s)}} = \\ &= \frac{\varphi(r)}{u^{\Re(s)}}\left(\frac{|s|}{\Re(s)} + 2\right).\end{aligned} \tag{3.2}$$

Então, para s fixo com $\Re(s) > 0$ e dado qualquer $\epsilon > 0$ é possível encontrar $N_0 \in \mathbb{Z}_+^*$ tal que para quaisquer $N_0 \leq u \leq v$ tenhamos

$$\left|\sum_{n=1}^{v}\frac{\chi(n)}{n^s} - \sum_{n=1}^{u}\frac{\chi(n)}{n^s}\right| < \epsilon.$$

Portanto, a seqüência de somas parciais é de Cauchy, o que garante a convergência da série. ■

Isto nos permite concluir que a função $L(\chi, s)$ converge uniformemente em cada domínio compacto no semi-plano complexo $\Re(s) > 0$, em particular,

esta função é contínua em todo este semi-plano[2], em particular, temos o resultado que iremos precisar mais tarde na demonstração do Teorema 3.1:

$$\lim_{s\to 1} L(\chi, s) = L(\chi, 1).$$

Vamos, finalmente, passar à demonstração do teorema de Dirichlet:

Demonstração do Teorema 3.1: Seja $\chi \in \widehat{\mathbb{Z}_r^\times}$ e considere, para $\Re(s) > 1$ a função

$$\mathrm{Ln}\left(L(\chi, s)\right) = -\sum_{p\text{primo}} \mathrm{Ln}\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{p\text{primo}} \sum_{m=1}^{\infty} \frac{\chi(p^m)}{mp^{ms}},$$

onde, na última igualdade já utilizamos o fato de que a função χ é totalmente multiplicativa. A convergência absoluta dastas somas está garantida para $\Re(s) > 1$, assim, podemos ainda inverter a ordem das somas e escrever

$$\mathrm{Ln}\left(L(\chi, s)\right) = \sum_{m=1}^{\infty} \sum_{p\text{primo}} \frac{\chi(p^m)}{mp^{ms}} = \sum_{p\text{primo}} \frac{\chi(p)}{p^s} + R(\chi, s).$$

Pode-se verificar facilmente que esta última função,

$$R(\chi, s) = \sum_{m=2}^{\infty} \sum_{p\text{primo}} \frac{\chi(p^m)}{mp^{ms}},$$

é limitada para $\Re(s) > 1$: Considere $s = x + iy$ com $x > 1$, então

$$\begin{aligned}
|R(\chi, s)| &= \left|\sum_{m=2}^{\infty} \sum_{p\text{primo}} \frac{\chi(p^m)}{mp^{ms}}\right| \leq \sum_{p\text{primo}} \sum_{m=2}^{\infty} \frac{|\chi(p^m)|}{mp^{mx}} \leq \\
&\leq \sum_{p\text{primo}} \sum_{m=2}^{\infty} \frac{1}{mp^{mx}} \leq \frac{1}{2} \sum_{p\text{primo}} \sum_{m=2}^{\infty} \frac{1}{p^{mx}} = \\
&= \frac{1}{2} \sum_{p\text{primo}} \frac{1}{p^{2x}\left(1 - \frac{1}{p^x}\right)} \leq \frac{1}{2} \sum_{p\text{primo}} \frac{1}{p^{2x}\left(1 - \frac{1}{2^x}\right)} \leq \\
&\leq \frac{1}{2} \sum_{p\text{primo}} \frac{1}{p^{2x}\left(1 - \frac{1}{2}\right)} = \sum_{p\text{primo}} \frac{1}{p^{2x}} \leq \\
&\leq \sum_{p\text{primo}} \frac{1}{p^2} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 < 1.
\end{aligned}$$

[2]De fato, esta função é analítica em todo o plano complexo.

Lembrando que queremos analisar a quantidade de primos na progressão aritmética $a + nr$ com $\text{mdc}(a, r) = 1$, vamos considerar a soma

$$X(s) = \sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} \overline{\chi(a)} \text{Ln}\left(L(\chi, s)\right),$$

para então estudarmos o limite $\lim_{s\to 1^+} X(s)$.

Esta soma pode ser vista de dois modos diferentes: De um lado, temos que

$$X(s) = \text{Ln}\left(L(\chi_0, s)\right) + \sum_{\chi \neq \chi_0} \overline{\chi(a)} \text{Ln}\left(L(\chi, s)\right),$$

Utilizando a expressão escrita em (3.1), podemos dizer que o primeiro termo desta soma é essencialmente igual a

$$\text{Ln}\left(\frac{1}{s-1}\right) = -\text{Ln}(s-1)$$

mais um termo limitado em um compacto ao redor de $s = 1$. O segundo termo da expressão de $X(s)$ é uma função contínua em s e que tem como limite

$$\lim_{s\to 1^+} \sum_{\chi \neq \chi_0} \overline{\chi(a)} \text{Ln}\left(L(\chi, s)\right) = \sum_{\chi \neq \chi_0} \overline{\chi(a)} \text{Ln}\left(L(\chi, 1)\right)$$

Assim,

$$\lim_{s\to 1^+} X(s) = -\lim_{x\to 1^+} \ln(x-1) = +\infty. \tag{3.3}$$

Por outro lado, temos que

$$\begin{aligned} X(s) &= \sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} \overline{\chi(a)} \text{Ln}\left(L(\chi, s)\right) = \\ &= \sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} \overline{\chi(a)} \left(\sum_{p\text{primo}} \frac{\chi(p)}{p^s} + R(\chi, s) \right) = \\ &= \sum_{p\text{primo}} \frac{1}{p^s} \left(\sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} \overline{\chi(a)} \chi(p) \right) + f(\chi, s). \end{aligned}$$

Na expressão acima, podemos verificar que o termo $f(\chi, s)$ é limitado para $\Re(s) > 1$, pois

$$|f(\chi,s)| = \left| \sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} \overline{\chi(a)} R(\chi,s) \right| \leq \sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} |\chi(a)| \leq \varphi(r).$$

Devido à relação de ortogonalidade entre os caracteres irredutíveis de um grupo,

$$\sum_{\chi \in \widehat{G}} \overline{\chi(g)}\chi(h) = \begin{cases} |G|, & \text{se} \quad g = h \\ 0 & \text{se} \quad g \neq h \end{cases},$$

podemos deduzir que

$$\sum_{\chi \in \widehat{\mathbb{Z}_r^\times}} \overline{\chi(a)}\chi(p) = \begin{cases} \varphi(r), & \text{se} \quad p \equiv a (\text{mod} r) \\ 0 & \text{se} \quad p \not\equiv a (\text{mod} r) \end{cases}.$$

Assim, teremos

$$X(s) = \sum_{p \equiv a (\text{mod} r)} \frac{1}{p^s} + f(\chi, s), \tag{3.4}$$

e no limite $s \to 1^+$, teremos a soma dos inversos dos primos $p \equiv a(\text{mod}r)$ mais um termo limitado. Se houvesse apenas uma quantidade finita de números primos nesta seqüência aritmética, isto levaria a uma contradição, pois de um lado obteríamos um limite infinito (3.3), por outro lado, obteríamos um limite finito da expressão (3.4). Isto prova que existem infinitos primos na progressão aritmética $a + nr$. ■

Note que o resultado importante da teoria de representações que foi útil na demonstração deste teorema foi a relação de ortogonalidade entre os caracteres, que permitiu selecionarmos na série dos inversos das potências dos primos apenas os primos que pertenciam à progressão aritmética dada, este passo foi crucial para a demonstração do teorema. a teoria de representações de grupos possui uma diversa gama de aplicações em diversas áreas da matemática. Introduzimos a teoria de representações com uma aplicação à teoria analítica de números deviso ao apelo intuitivo do problema, à fácil compreensão do seu enunciado e à beleza envolvida em sua demonstração, devido à mistura de técnicas oriundas de diversas áreas. Esperamos que esta motivação inicial tenha sido de grande valia para que você continue a se interessar por esta fascinante área da matemática.

Apêndice A

Anel das Funções Aritméticas

Neste pequeno apêndice, vamos apresentar algumas propriedades do anel das funções aritméticas.

Definição A.1 *Uma função aritmética é uma função* $f : \mathbb{Z}_+^* \to \mathbb{C}$.

Teorema A.1 *O conjunto de todas as funções aritméticas pode ser munido com a estrutura de anel comutativo com unidade, com a soma de funções ponto a ponto e o produto de convolução dado por*

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Demonstração: As propriedades comutativa e associativa da soma são facilmente verificadas. O elemento nulo no anel é a função identicamente nula e o inverso aditivo de f é a função $-f$, definida como $(-f)(n) = -f(n)$. Verifique a distributividade do produto em relação à soma.

A comutatividade da multiplicação também pode ser facilmente obtida:

$$\begin{aligned}(f * g)(n) &= \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \\ &= \sum_{e|n} f\left(\frac{n}{e}\right) g(e) = \\ &= \sum_{d|n} g(e) f\left(\frac{n}{e}\right) = (g * f)(n)\end{aligned}$$

A unidade deste anel é dada pela função δ_1 que satisfaz à relação $\delta_1(n) = \delta_{1,n}$:

$$(\delta_1 * f)(n) = \sum_{d|n} \delta_1(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \delta_{1,d} f\left(\frac{n}{d}\right) = f\left(\frac{n}{1}\right) = f(n).$$

Para verificarmos a associatividade do produto, precisamos escrevê-lo de um outro modo mais apropriado:

$$(f * g)(n) = \sum_{k\in\mathbb{Z}_+^*} \sum_{l\in\mathbb{Z}_+^*} \delta_{kl,n} f(k) g(l).$$

Escrevendo desta maneira, podemos ver que

$$\begin{aligned}
((f * g) * h)(n) &= \sum_{k\in\mathbb{Z}_+^*} \sum_{l\in\mathbb{Z}_+^*} \delta_{kl,n} (f * g)(k) h(l) = \\
&= \sum_{k\in\mathbb{Z}_+^*} \sum_{l\in\mathbb{Z}_+^*} \delta_{kl,n} \left(\sum_{p\in\mathbb{Z}_+^*} \sum_{q\in\mathbb{Z}_+^*} \delta_{pq,k} f(p) g(q) \right) h(l) = \\
&= \sum_{p\in\mathbb{Z}_+^*} \sum_{q\in\mathbb{Z}_+^*} \sum_{l\in\mathbb{Z}_+^*} \delta_{pql,n} f(p) g(q) h(l).
\end{aligned}$$

Por outro lado

$$\begin{aligned}
(f * (g * h))(n) &= \sum_{p\in\mathbb{Z}_+^*} \sum_{k\in\mathbb{Z}_+^*} \delta_{pk,n} f(p) (g * h)(k) = \\
&= \sum_{p\in\mathbb{Z}_+^*} \sum_{k\in\mathbb{Z}_+^*} \delta_{pk,n} f(p) \left(\sum_{q\in\mathbb{Z}_+^*} \sum_{l\in\mathbb{Z}_+^*} \delta_{ql,k} g(q) h(l) \right) = \\
&= \sum_{p\in\mathbb{Z}_+^*} \sum_{q\in\mathbb{Z}_+^*} \sum_{l\in\mathbb{Z}_+^*} \delta_{pql,n} f(p) g(q) h(l).
\end{aligned}$$

Da igualdade entre estas duas expessões, temos a associatividade do produto de convolução. ■

O subconjunto das funções aritméticas que satisfazem $f(1) \neq 0$ forma um grupo abeliano com respeito ao produto de convolução. Já demonstramos que o produto de convolução é associativo e a unidade no anel de funções

aritméticas δ_1 é uma função que não se anula em $n = 1$. Então, somente nos resta mostrar que dada uma função aritmética f tal que $f(1) \neq 0$ possui inverso multiplicativo. Se g for a função inversa multiplicativa de f, então

$$(g * f)(n) = \delta_1(n) = \delta_{1,n}.$$

Assim

$$(g * f)(1) = g(1)f(1) = 1 \qquad \Rightarrow \qquad g(1) = \frac{1}{f(1)}.$$

Supondo, por indução, que conheçamos todos os valores de $g(k)$ para $1 \leq k < n$, podemos calcular

$$(g * f)(n) = \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = g(n)f(1) + \sum_{1<d|n} g(d) f\left(\frac{n}{d}\right) = 0.$$

Portanto,

$$g(n) = -\frac{1}{f(1)} \left(\sum_{1<d|n} g(d) f\left(\frac{n}{d}\right) \right).$$

Com isto, demonstramos que é possível calcular os valores da função inverso multiplicativo de f para todos os números inteiros positivos.

Uma outra classe importante de funções aritméticas são as funções multiplicativas.

Definição A.2 *Uma função aritmética f é dita ser multiplicativa se, para todo par de números inteiros positivos m e n tais que $mdc(m, n) = 1$, tivermos que $f(mn) = f(m)f(n)$. Uma função é dita ser completamente multiplicativa se, para quaisquer números inteiros positivos m e n, tivermos que $f(mn) = f(m)f(n)$.*

Proposição A.1 *O produto de convolução de duas funções multiplicativas é uma função multiplicativa.*

Demonstração: Sejam f e g duas funções multiplicativas e m e n dois inteiros positivos primos entre si. Se $\text{mdc}(m, n) = 1$ e $d|m$ e $e|n$, então

$\mathrm{mdc}(d,e)=1$ (Verifique isto). Portanto

$$\begin{aligned}(f*g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = \\ &= \sum_{k|m,\, l|n} f(kl)g\left(\frac{m}{k}\frac{n}{l}\right) = \\ &= \sum_{k|m,\, l|n} f(k)f(l)g\left(\frac{m}{k}\right)g\left(\frac{n}{l}\right) = \\ &= \left(\sum_{k|m} f(k)g\left(\frac{m}{k}\right)\right)\left(\sum_{l|n} f(l)g\left(\frac{n}{l}\right)\right) = \\ &= (f*g)(m)(f*g)(n).\end{aligned}$$

O que nos mostra o resultado desejado. ■

Vamos dar alguns exemplos de funções aritméticas importantes para a teoria de números.

Exemplo A.1: A função número de divisores de um número inteiro positivo, $\tau(n)$. É fácil ver que esta função é multiplicativa, pois se $\mathrm{mdc}(m,n)=1$, para cada divisor $d|m$, se fizermos o produto de d por cada divisor de n, teremos um divisor de mn, assim o número de divisores de mn é igual ao produto do número de divisores de m pelo número de divisores de n, ou seja $\tau(mn)=\tau(m)\tau(n)$.

Para calcularmos explicitamente o valor $\tau(n)$, é preciso primeiramente considerarmos os valores desta função em potências de primos, posi qualquer número inteiro positivo pode ser decomposto de forma única em fatoras primos,

$$n = p_1^{k_1}.p_2^{k_2}.\ldots.p_r^{k_r}.$$

Como $\mathrm{mdc}(p_i^{k_i}, p_j^{k_j})=1$ para qualquer par $i\neq j$, temos que

$$\tau(n) = \tau(p_1^{k_1})\tau(p_2^{k_2})\ldots\tau(p_r^{k_r}).$$

Para calcularmos $\tau(p_i^{k_i})$, temos que verificar quais são os divisores de $p_i^{k_i}$, que são: 1, p_1, p_1^2, ..., $p_i^{k_i}$, logo, temos (k_i+1) divisores distintos. Portanto,

$$\tau(n) = (k_1+1)(k_2+1)\ldots(k_r+1).$$

Exemplo A.2: A função soma dos divisores de um número inteiro positivo, $\sigma(n)$. Também podemos facilmente ver que esta função é mutltiplicativa: Se $\text{mdc}(m,n)=1$, para cada divisor $d|m$, se multiplicarmos d por cada divisor de n, temos um divisor de mn, como so divisores de m e de n não possuem divisores em comum, não haverá dois destes produtos que sejam iguais. Assim, a soma dos divisores de mn será a soma de todos os produtos arbitrários de divisores de m por divisores de n

$$\sigma(mn)=\sum_{d|m}\sum_{e|n}d.e=\sum_{d|m}d\left(\sum_{e|n}e\right)=\sigma(m)\sigma(n).$$

Novamente, para calcularmos os valores $\sigma(n)$, precisamos saber somente os valores $\sigma(p^k)$, para p primo, que são facilmente calculados como

$$\sigma(p^k)=1+p+p^2+\cdots+p^k=\frac{(p^{k+1}-1)}{(p-1)}.$$

Portanto, para $n=p-1^{k_1}.p_2^{k_2}.\ldots.p_r^{k_r}$, teremos

$$\sigma(n)=\sigma(p_1^{k_1})\sigma(p_2^{k_2})\ldots\sigma(p_r^{k_r})=\left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right)\ldots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right).$$

Exemplo A.3: A função totiente de Euler, $\varphi(n)$, que mede o número de números inteiros positivos k, menores ou iguais a n que são primos com n, oou seja que $\text{mdc}(k,n)=1$. Se p é um número primo, todos os inteiros positivos menores que p são primos com p, assim $\varphi(p)=p-1$. Se $n=p^k$, então os únicos números inteiros positivos menores ou iguais a p^k que não são primos com p^k são os múltiplos de p, que corresponde a p^{k-1} múltiplos de p dos p^k números existentes (Verifique isto), assim

$$\varphi(p^k)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right).$$

A verificação de que a função φ é multiplicativa não é tão imediata quanto as anteriores, e será feita na próxima proposição. Por hora, vamos utilizar este resultado para calcularmos os valores $\varphi(n)$. Seja $n=p_1^{k_1}.\ldots.p_r^{k_r}$, então

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1})\ldots\varphi(p_r^{k_r})= \\ &= p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right)= \\ &= n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

Proposição A.2 *A função totiente de Euler é uma função multiplicativa.*

Demonstração: Considere dois inteiros positivos m e n primos entre si. Vamos organizar os números de 1 a mn de acordo com a seguinte tabela:

$$\begin{array}{cccc} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & mn \end{array}$$

Primeiramente, verifiquemos que em uma determinada coluna, todos os elementos possuem o mesmo máximo divisor comum com n: Sejam a e b dois números na i-ésima coluna e suponha que $\text{mdc}(a,n) = d$ e $\text{mdc}(b,n) = e$. Por estarem na i-ésima coluna, existem números inteiros positivos k e l (suponha, sem perda de generalidade que $k > l$) tais que

$$a = kn + i, \qquad b = ln + i,$$

resultando em

$$a - b = (k - l)n.$$

Como $d|a$ e $d|n$, então, da expressão acima, podemos concluir que $d|b$, o que implica que $d|e$, pois $e = \text{mdc}(b,n)$. Por outro $e|b$ e $e|n$, logo, da mesma expressão, temos que $e|a$, o que implica que $e|d$, pois $d = \text{mdc}(a,n)$. Logo, $d = e$, como queríamos provar. Portanto, apenas $\varphi(n)$ colunas contém elementos primos com n (condição necessária para ser primo com mn).

Agora, analisando cada uma destas $\varphi(n)$ colunas, vamos mostrar que estas colunas formam um sistema completo de restos módulo m. Suponha que dois elementos na mesma coluna sejam congruentes módulo m, então, por um lado $a - b = pm$ por outro lado $a - b = (k - l)n$, assim teríamos que, por um lado $pm = (k - l)n$, como $m \nmid m$ temos que $m|(k - l)$. Por outro lado k e l são inteiros menores que m, assim $(k - l) < m$. Temos, então uma contradição, portanto dois elementos diferentes em cada coluna são incongruentes módulo m, como temos exatamente m elementos em cada coluna, temos que cada coluna forma um sistema completo de restos módulo m.

Com um raciocínio totalmente análogo ao realizado para n, podemos mostrar que dois números côngruos módulo m possuem o mesmo máximo

divisor comum com m (Verifique os detalhes), assim em cada coluna temos exatamente $\varphi(m)$ números primos com m. Portanto o número de números menores ou iguais a mn que são primos com mn são os $\varphi(m)$ elementos de cada uma das $varphi(n)$ colunas obtidas no passo anterior, o que resulta em $\varphi(m)\varphi(n)$ números, ou seja

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Isto significa que a função φ é multiplicativa. ■

Bibliografia

[1] A. Ash and R. Gross: "Fearless Symmetry, Exposing the Hidden Patterns of Numbers", Princeton University Press (2006).

[2] W.A. Coppel: "Number Theory, An Introduction to Mathematics", Part B, Springer-Verlag (2006).

[3] P.G.L. Dirichlet: "Lectures on Number Theory", History of Mathematics Sources, Vol. 16, American Mathematical Society (1999).

[4] H.H. Domingues: "Fundamentos de Aritmética", Atual Ed. (1991).

[5] E. Grosswald: "Topics from the Theory of Numbers", Birkhäuser (1984).

[6] G.H. Hardy and E.M. Wright: "An Introduction to the Theory of Numbers", Oxford University Press (1960).

[7] B.V. Holt and T.J. Evans: "Group Actions in Number Theory", arXix:math.HO/0508396 (2005).

[8] N. Jacobson: "Basic Algebra", Vols 1 and 2, W.H. Freeman and Co. (1989).

[9] J.J. Rotman: "A First Course in Abstract Algebra", 2nd. Ed., Prentice Hall (2000).

[10] J.J. Rotman: "Advanced Modern Algebra", Prentice Hall (2002).

[11] J.P.O. Santos: "Introdução à Teoria dos Números", Coleção Matemática Universitária, IMPA (2003).