Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas
Departamento de Matemática

Ações de Grupos e Contagem: Teorema de Burnside

Cinthia Marques Vieira Andretti
Orientador: Prof. Dr. Eliezer Batista

Florianópolis – SC
Fevereiro de 2011

Cinthia Marques Vieira Andretti

Ações de Grupos e Contagem: Teorema de Burnside

Monografia

Florianópolis – SC

Fevereiro de 2011

Agradecimentos

Agradeço ao meu orientador, Eliezer Batista, pelas palavras de incentivo que me motivaram a concluir este trabalho.

Aos meus amigos, Marcos Teixeira Alves e Monique Müller Lopes Rocha, meu muito obrigada. São pessoas que fizeram questão de acompanhar o meu trabalho mesmo de longe, me ajudando em formatações e no que mais fosse preciso. São amigos que crescem junto comigo e me fazem muito feliz.

A minha mãe, Margareth Marques Vieira, e ao meu esposo Rodrigo Klöppel, todo meu amor e minha gratidão. São meus maiores fãs e incentivadores, são capazes de acreditar em mim quando nem eu mesma acredito mais. Espero que a conclusão desta monografia possa de alguma forma suprir as expectativas e confiança que ambos tem em mim. Amo vocês!

Ações de Grupos e Contagem: Teorema de Burnside

por

Cinthia Marques Vieira Andretti

Esta monografia foi julgada adequada ...

Banca Examinadora:

Prof. Dr. Eliezer Batista
Orientador

Prof.

Prof.

Sumário

Introdução

Até o início do século XVI, não se sabia se todas as equações polinomiais de grau 3 eram solúveis por radicais, ou seja, se suas soluções poderiam ser dadas em termos de seus coeficientes usando apenas adições, subtrações, multiplicações, divisões e radiciações. Nesta época, os matemáticos italianos Scipione del Ferro (1456-1526) e Nicollo Fontana - Tartaglia (1499-1557) descobriram um procedimento para resolver a equação cúbica $x^3 + px = q$ $(p, q > 0)$.

Como já se sabia há muitos séculos que as equações de grau um e dois também eram solúveis por radicais, a solução de del Ferro propôs a seguinte questão: será que toda equação algébrica é solúvel por radicais? As pesquisas visando responder a essa questão se arrastaram por mais de dois séculos e meio, frustraram alguns dos grandes matemáticos desse período e contribuíram para a criação do conceito de grupo.

Em 1545, o também italiano Cardano divulgou o método de Ferrari para redução de uma equação polinomial de grau 4 para uma equação polinomial de grau 3. Usando as ideias de Tartaglia e del Ferro Ferrari, verificou que toda equação polinomial de grau 4 é solúvel por radicais.

Em 1824, o norueguês Niels H. Abel, mostrou que nem toda equação de grau 5 é solúvel por radicais. Claro que existem equações polinomiais de grau 5 que são solúveis por radicais, então a questão era: quais equações polinomiais de grau ≥ 5 são solúveis por radicais?

A resposta para esta pergunta foi dada por Évariste Galois (1811-1832), que in-

troduziu o conceito de grupo. Resumidamente, a ideia de Galois para responder a essa pergunta foi associar a cada equação um grupo formado por permutações de suas raízes e condicionar a resolubilidade por radicais a uma propriedade desse grupo. E, como para toda equação de grau ≤ 4 o grupo de permutações que lhe é associado goza dessa propriedade e para $n > 4$ sempre há equações cujo grupo não se sujeita a essa propriedade, a questão de resolubilidade por radicais estava esclarecida.

Com o tempo, verificou-se que a ideia de grupo era um instrumento da mais alta importância para a organização e o estudo de muitas partes da matemática. Uma de suas aplicações é a teoria das simetrias, muito importante para a cristalografia e química, por exemplo. Essencialmente, os grupos podem ser usados para retratar simetrias geométricas: a cada figura associa-se um grupo, grupo que caracteriza e retrata a simetria da figura. Na análise combinatória, a noção de grupo de permutação e o conceito de ação de um grupo são frequentemente utilizados para simplificar a contagem de um conjunto de objetos, e é o objetivo do presente trabalho.

Capítulo 1

Grupos e Exemplos

1.1 Grupos

Uma operação $*$ em um conjunto não vazio G é uma função

$$* : G \times G \longrightarrow G$$

$$(a, b) \longmapsto a * b.$$

Portanto, uma operação em G associa a cada par de elementos de G um único elemento de G.

Definição 1.1.1 Seja $*$ uma operação no conjunto não vazio G. Dizemos que $(G, *)$ é um **grupo** quando a operação $*$ satisfaz as seguintes propriedades:

(i) Associatividade: $a * (b * c) = (a * b) * c$, $\forall a, b, c \in G$.

(ii) Elemento neutro: existe $e \in G$ tal que $a * e = e * a = a$, $\forall a \in G$.

(iii) Elemento simétrico: dado $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$.

Observação 1.1.1 Quando o conjunto G é finito dizemos que o grupo $(G, *)$ é **grupo finito**. Caso contrário, $(G, *)$ é **grupo infinito.**

Definição 1.1.2 O grupo $(G, *)$ é **abeliano** ou **comutativo** quando:

(iv) $a * b = b * a, \forall a, b \in G$.

Observação 1.1.2 Quando a operação do grupo G é uma adição conhecida, dizemos que G é um **grupo aditivo** e usamos a notação $(G, +)$. Analogamente quando a operação do grupo G é uma multiplicação conhecida, dizemos que G é um **grupo multiplicativo** e usamos a notação $(G, \cdot)$.

Nossa primeira proposição mostrará a unicidade do elemento neutro e do elemento simétrico.

Proposição 1.1.1 Seja $(G, *)$ um grupo:

(a) Existe um único elemento neutro em G.

(b) Para cada $a \in G$ existe um único elemento simétrico em G.

Demonstração:

(a) Suponha que e e e' sejam elementos neutros para G.

Como e é elemento neutro de G, temos $e * e' = e'$.

Como e' é elemento neutro de G, temos $e * e' = e$.

Portanto, $e = e'$.

(b) Suponha que a' e a'' sejam simétricos para a.

Como a' é simétrico para a, temos $a' * a = e$.

Como a'' é simétrico para a, temos $a * a'' = e$.

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

■

Exemplo 1.1.1 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ são grupos abelianos infinitos.

Em cada um desses casos, a adição é uma operação sobre cada um dos conjuntos, associativa e comutativa. Existe um elemento neutro (o número 0), e todo elemento do conjunto tem um simétrico, também pertencente ao conjunto.

Exemplo 1.1.2 $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$ são grupos abelianos infinitos.

Em cada um desses casos, a multiplicação é uma operação sobre cada um dos conjuntos, associativa e comutativa. Existe um elemento neutro (o número 1), e todo elemento do conjunto tem um simétrico também pertencente ao conjunto.

Exemplo 1.1.3 $(\mathbb{N}, +)$, $(\mathbb{N}^*, \cdot)$, $(\mathbb{Z}^*, \cdot)$ não são grupos.

Em cada um desses casos, não é possível obter simétricos para todos os elementos. De fato, em $(\mathbb{N}, +)$ o elemento neutro é zero, mas para $1 \in \mathbb{N}$ não existe $a' \in \mathbb{N}$ tal que $1 + a' = 0$. Em $(\mathbb{N}^*, \cdot)$ e $(\mathbb{Z}^*, \cdot)$ o elemento neutro é 1, mas para $2 \in \mathbb{N}^* \subseteq \mathbb{Z}^*$ não existe $a' \in \mathbb{Z}^*$ tal que $2 \cdot a' = 1$, pois como $\mathbb{N}^* \subset \mathbb{Z}^*$ então também $a' \notin \mathbb{N}^*$.

Exemplo 1.1.4 O conjunto $U(1)$ dos números complexos de módulo um, ou seja, a circunferência unitária no plano complexo também denotado por $\mathbb{S}_1$, é grupo. Note que, se $z, w \in \mathbb{C}$ tais que $|z| = |w| = 1$, então $|z \cdot w| = |z| \cdot |w| = 1$.

As propriedades da multiplicação dos números complexos garantem-nos que $\mathbb{S}^1$ é grupo abeliano.

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:

$$z = e^{i\theta} = \cos\theta + i\text{sen}\theta, \text{ onde } 0 \leq \theta < 2\pi.$$

Um procedimento para produzir grupos a partir de anéis conhecidos, é tomar o conjunto dos elementos inversíveis de um anel com unidade, denotado por $U(A)$. Mostraremos isso na próxima proposição.

Proposição 1.1.2 Seja $(A, +, \cdot)$ um anel com unidade. Então $(U(A), \cdot)$ é grupo e será abeliano se $(A, +, \cdot)$ for comutativo.

Demonstração:

Inicialmente note que a multiplicação é de fato uma operação em $U(A)$, pois dados $a, b \in U(A)$, temos $a^{-1}, b^{-1} \in A$, então $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$. Analogamente $(b^{-1}a^{-1})ab = 1$, portanto $(ab)^{-1} = b^{-1}a^{-1}$.

Logo, $ab \in U(A)$ e a multiplicação é fechada em $U(A)$.

Como a multiplicação é associativa no anel A, também será associativa em $U(A)$.

É claro que $1 \in U(A)$ e que 1 é elemento neutro para $(U(A), \cdot)$.

Dado $a \in U(A)$ temos, por definição, que existe $a^{-1} \in U(A)$ tal que

$$aa^{-1} = a^{-1}a = 1 \in U(A).$$

Assim, $a^{-1} \in U(A)$.

Se $(A, +, \cdot)$ é anel comutativo, então a multiplicação em A é comutativa. Segue que a multiplicação em $U(A)$ é comutativa, e portanto $(U(A), \cdot)$ é grupo abeliano.

■

Exemplo 1.1.5 Seja K um corpo. Sabemos que $(M_n(K), +, \cdot)$ é anel com unidade, e então $(U(M_n(K)), \cdot)$ é um grupo, chamado de grupo linear sobre K e denotado por $GL_n(K)$.

Trataremos a partir de agora de três grupos de especial importância para aplicações: grupos de permutações, grupos de rotações e grupos diedrais. Os grupos de permutações são grupos formados por bijeções de um conjunto nele mesmo. Os grupos de rotações descrevem as rotações, no plano, de um polígono regular. Já os grupos diedrais descrevem os movimentos que preservam um polígono regular.

Grupos de Permutações

Seja E um conjunto não vazio, e denote por Bij(E) o conjunto de todas as bijeções de E em E, isto é:

$$\text{Bij(E)} = \{f : E \longrightarrow E; f \,\text{é bijetora}\}.$$

Proposição 1.1.3 A composta de bijeções é uma bijeção.

Demonstração:

Sejam $f, g \in \text{Bij}(E)$. Devemos provar que $f \circ g \in \text{Bij}(E)$.

• $f \circ g$ é injetiva.

Sejam $x, y \in E$, tais que $(f \circ g)(x) = (f \circ g)(y)$. Então $f(g(x)) = f(g(y))$.

Como f é injetiva temos que $g(x) = g(y)$.

Como g também é injetiva temos que $x = y$.

• $f \circ g$ é sobrejetiva.

Seja $z \in E$. Como f e g são sobrejetoras, existe $y \in E$ com $f(y) = z$, existe $x \in E$ com $g(x) = y$. Então, existe $x \in E$ tal que $f(g(x)) = z$ e portanto $f \circ g$ é sobrejetiva.

■

Desde que a composição de bijeções é uma bijeção, temos que a composição é uma operação em Bij(E). Denotaremos a operação composição pelo símbolo "$\circ$".

Proposição 1.1.4 Se E é um conjunto não vazio, então $(\text{Bij}(E), \circ)$ é um grupo.

Demonstração:

É claro que a função identidade é o elemento neutro de $(\text{Bij}(E), \circ)$, pois

$$f \circ \text{id} = \text{id} \circ f = f, \text{ para toda função } f \in \text{Bij}(E).$$

Seja $g \in \text{Bij}(E)$. Como g é bijetora, existe a função inversa $g^{-1} \in \text{Bij}(E)$ satisfazendo $g \circ g^{-1} = g^{-1} \circ g = \text{id}$. Logo, g^{-1} é o simétrico de g.

Para ver a associatividade, tomamos $f, g, h \in \text{Bij}(E)$ e $x \in E$.

$$\begin{aligned}(f \circ (g \circ h))(x) &= f((g \circ h)(x)) \\ &= f(g(h(x))) \\ &= (f \circ g)(h(x)) \\ &= ((f \circ g) \circ h)(x).\end{aligned}$$

■

Definição 1.1.3 O grupo $\text{Bij}(E)$ é chamado de **grupo de permutações** (ou **grupo simétrico**) do conjunto E.

Notação: Quando E é um conjunto finito com n elementos, indicamos $\text{Bij}(E)$ por S_n.

O corolário da próxima proposição assegura, que se E tem n elementos, então S_n tem $n!$ elementos.

Proposição 1.1.5 Sejam E e F conjuntos com n elementos. Então o número de bijeções de E em F é $n!$.

Demonstração:

Para demonstrar este fato vamos usar o Primeiro Princípio de Indução sobre n.

Para $n = 1$ é óbvio.

Suponha que o número de bijeções entre conjuntos com k elementos é $k!$ (hipótese de indução).

Sejam $E = \{a_1, a_2, \cdots, a_k, a_{k+1}\}$ e $F = \{b_1, b_2, \cdots, b_k, b_{k+1}\}$. Devemos mostrar que o número de bijeções de E em F é $(k+1)!$.

Para cada $i \in \{1, 2, \cdots, k+1\}$, considere a função

$$g_i : \{a_1\} \longrightarrow F$$

$$a_1 \longmapsto b_i.$$

Vamos estender g_i ao conjunto E para obter bijeções de E em F.

Note que $E - \{a_1\}$ e $F - \{b_i\}$ têm k elementos, então por hipótese de indução, temos $k!$ bijeções entre estes conjuntos. Se f é uma destas bijeções, então

$$g : E \longrightarrow F,\ g(x) = \begin{cases} f(x) & , \text{se} \quad x \neq a_1 \\ b_i & , \text{se} \quad x = a_1 \end{cases}$$

é uma bijeção que estende g_i.

Assim, para cada $i \in \{1, 2, \cdots, k+1\}$, temos $k!$ bijeções de E em F.

Como temos $k+1$ possibilidades para i, obtemos $(k+1)k! = (k+1)!$ bijeções de E em F.

Observe que estas são todas as bijeções de E em F. De fato, se $h : E \longrightarrow F$ é bijetora, então $h(a_1) = b_i$ para algum $i \in \{1, , 2, \cdots, k+1\}$.

Logo, h é uma bijeção que estende g_i e, portanto, h é uma das bijeções construídas anteriormente.

■

Corolário 1.1.1 Se E tem n elementos, então S_n tem $n!$ elementos.

Demonstração:

Imediata da proposição anterior.

■

Se $f \in S_n$, então $f : \{1, 2, \cdots, n\} \longrightarrow \{1, 2, \cdots, n\}$ é uma bijeção, e para cada $i \in \{1, 2, \cdots, n\}$, $f(i) = a_i \in \{1, 2, \cdots, n\}$, com $a_i \neq a_j$ quando $i \neq j$. Assim, temos

$f(1) = a_1, f(2) = a_2, \cdots, f(n) = a_n$.

Uma notação mais simples é $f = \begin{pmatrix} 1 & 2 & \cdots & \text{n} \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \in S_n$.

Note que é apenas uma notação mais concisa e não uma matriz de ordem $2 \times n$.

Por exemplo, a função $f \in S_4$ tal que $f(1) = 2, f(2) = 3, f(3) = 4$ e $f(4) = 1$ pode ser indicada por

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4.$$

Grupos de Rotações

Seja $\{1, 2, \cdots, n\}$, o conjunto dos vértices de um polígono regular com n lados.

Cada uma das rotações de ângulo, $0, \frac{2\pi}{n}, 2\frac{2\pi}{n}, \cdots, (n-1)\frac{2\pi}{n}$, no sentido anti-horário, mantém o polígono invariante (move apenas os vértices). Além disso, se olharmos para $S_n = \text{Bij}(E)$, $E = \{1, 2, \cdots, n\}$, vemos que estas rotações podem ser identificadas com elementos distintos de S_n.

Sejam e a rotação de 0 radianos e a a rotação de $\frac{2\pi}{n}$ radianos. Estes elementos correspondem às seguintes funções de S_n :

$$e = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix} \text{ e } a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}.$$

Usando a notação $a^j = a \circ a \circ \cdots \circ a, j$ vezes e a convenção $a^0 = \text{id} = e$, é fácil ver que as potências de a produzem todas as rotações. De fato,

a^2 é a rotação de ângulo $2\frac{2\pi}{n}$.

.

.

.

a^{n-1} é a rotação de ângulo $(n-1)\frac{2\pi}{n}$.

$a^n = a^0 = e$ é a rotação de ângulo 0.

Denotaremos por R_n o conjunto das rotações do polígono regular de n lados, isto é,

$$R_n = \{e = a^0, a, a^2, \cdots, a^{n-1}\} \subseteq S_n.$$

Note que, dados $a^i, a^j \in R_n$, vale $a^i \circ a^j = a^{i+j}$. Dividindo $i + j$ por n obtemos $q, r \in \mathbb{N}$ tais que $i + j = nq + r$, com $0 \leq r < n$. Assim,

$a^i \circ a^j = a^{i+j} = a^{nq+r} = (a^n)^q \circ a^r = e^q \circ a^r = e \circ a^r = a^r \in R_n$.

Portanto,

$$\begin{aligned} \circ : R_n \times R_n &\longrightarrow R_n \\ (a^i, a^j) &\longmapsto a^{i+j} \end{aligned}$$

é uma operação em R_n.

Proposição 1.1.6 $(R_n, \circ)$ é grupo abeliano com n elementos.

Demonstração:

Como os elementos de R_n são rotações de $\dfrac{2\pi}{n}k$ com $0 \leq k < n$, temos que R_n tem exatamente n elementos.

Vamos verificar que $(R_n, \circ)$ é grupo abeliano.

• Associatividade.

$a^i \circ (a^j \circ a^k) = a^i \circ a^{j+k} = a^{i+(j+k)} = a^{(i+j)+k} = a^{i+j} \circ a^k = (a^i \circ a^j) \circ a^k$.

• É claro que $a^0 = e$ é o elemento neutro de R_n.

• Todo elemento tem simétrico.

$a^i \circ a^{n-i} = a^n = a^0 = e, \forall i \in \{0, 1, \cdots, n-1\}$.

Logo, o simétrico de $a^i \in R_n$ é $a^{n-i} \in R_n$.

• Comutatividade.

$a^i \circ a^j = a^{i+j} = a^{j+i} = a^j \circ a^i$.

Portanto, $(R_n, \circ)$ é um grupo abeliano.

■

Definição 1.1.4 O grupo $(R_n, \circ)$ é chamado **grupo de rotações** de um polígono regular de n lados.

Exemplo 1.1.6 $R_3 = \{e, a, a^2\}$ é o grupo de rotações do triângulo equilátero de vértices 1,2 e 3.

O elemento neutro é $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, o elemento $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ é a rotação de $\frac{2\pi}{3}$, e o elemento $a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ é a rotação de $\frac{4\pi}{3}$.

Exemplo 1.1.7 $R_4 = \{e, a, a^2, a^3\}$ é o grupo de rotações do quadrado de vértices 1, 2, 3 e 4.

O elemento neutro é $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, o elemento $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ é a rotação de $\frac{\pi}{2}$, o elemento $a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ é a rotação de π e o elemento $a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ é a rotação de $\frac{3\pi}{2}$.

Existem outros grupos que correspondem a grupos de rotação de objetos tridimensionais. Em geral, estes grupos não são abelianos. Não vamos tratar destes grupos neste trabalho.

Grupos Diedrais

Considere novamente $\{1, 2, \cdots, n\}, n \geq 3$, como o conjunto dos vértices de um polígono regular de n lados. Seja $b \in S_n$ a reflexão em relação ao eixo horizontal, eixo

este que deve passar por dois vértices desse polígono regular de n lados.

Note que $b = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$ não é uma rotação, e que $b^2 = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

Lembre que o conjunto das rotações é $R_n = \{e, a, a^2, \cdots, a^{n-1}\}$, onde $a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$. Ao conjunto R_n vamos acrescentar b e também todos os $a^i b, i \in \{1, 2, \cdots, n-1\}$. Aqui estamos considerando a composição como sendo um produto, apenas para facilitar a escrita.

Desta forma, obteremos o conjunto

$$D_n = \{e, a, a^2, \cdots, a^{n-1}, b, ab, a^2b, \cdots, a^{n-1}b\} \subseteq S_n,$$

que tem $2n$ elementos. Cada um destes elementos representa uma simetria do polígono, isto é, um movimento que deixa o polígono invariante (move apenas os vértices).

Provaremos que D_n é um grupo com a operação de composição existente em S_n. Para isso, precisamos provar que

$$\begin{aligned} \circ : D_n \times D_n &\longrightarrow D_n \\ (a^i b^u, a^j b^v) &\longmapsto a^i b^u a^j b^v \end{aligned}$$

é de fato uma operação em D_n, ou seja, $a^i b^u a^j b^v \in D_n$.

Iniciamos com um lema que será útil para fazer contas em D_n.

Lema 1.1.1 Em D_n, vale a igualdade $ba^r = a^{n-r}b, \forall r \in \{1, 2, \cdots, n-1\}$.

Demonstração:

Para provar este fato vamos usar o Princípio de Indução sobre r.

Para $r = 1$, temos:

$$ba = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}. \ (i)$$

Para calcular $a^{n-1}b$ primeiro note que $a^{n-1} = a^n \circ a^{-1} = e \circ a^{-1} = a^{-1}$. Assim, $a^{n-1} = a^{-1}$ corresponde à rotação de $\dfrac{2\pi}{n}$ no sentido horário.

$$a^{-1}b = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & 1 & 2 & \cdots & n-2 & n-1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}. \ (ii)$$

De (i) e (ii) concluímos que $ba = a^{n-1}b$.

Suponha que $ba^k = a^{n-k}b$, para $k > 1$. (hipótese de indução)

Devemos mostrar que $ba^{k+1} = a^{n-(k+1)}b$.

$ba^{k+1} = ba^k a$

$= a^{n-k}ba$ (hipótese de indução)

$= a^{n-k}a^{n-1}b$ (caso $r = 1$)

$= a^n a^{n-(k+1)}b$ (associatividade)

$= ea^{n-(k+1)}b$

$= a^{n-(k+1)}b.$

■

Lema 1.1.2 A composição é uma operação em D_n.

Demonstração:

Devemos provar que se $a^ib^u, a^jb^v \in D_n$, então $a^ib^ua^jb^v \in D_n$, para $i, j \in \{0, 1, \cdots, n-1\}$ e $u, v \in \{0, 1\}$.

1^o caso: $u = 0$.

$a^ib^ua^jb^v = a^iea^jb^v = a^{i+j}b^v \in D_n$.

Lembrando que $a^{i+j} \in \{e, a, a^2, \cdots, a^{n-1}\}$ para quaisquer i e j.

2^o caso: $u = 1$.

$a^ib^ua^jb^v = a^iba^jb^v = a^ia^{n-j}bb^v = a^{n+i-j}b^{v+1} \in D_n$.

Lembrando que $b^2 = e$ e, portanto, qualquer potência de b pode ser reduzida a e ou b.

■

Proposição 1.1.7 $(D_n, \circ)$ é grupo não abeliano com $2n$ elementos.

Demonstração:

• Associatividade.

Como $D_n \subseteq S_n$, a associatividade em D_n é consequência da associatividade em S_n.

• e é o elemento neutro de D_n.

• Todo elemento tem simétrico.

Para provar que $a^ib^u \in D_n$ tem inverso em D_n, separamos em dois casos.

1^o caso: $u = 0$.

Neste caso, $a^ib^u = a^i$, e seu inverso é $a^{n-i} \in D_n$.

2^o caso: $u = 1$.

Neste caso, $a^ib^u = a^ib$ cujo inverso é o próprio $a^ib \in D_n$, pois

$a^iba^ib = a^ia^{n-i}bb = a^nb^2 = ee = e$.

• Não comutativo.

Basta notar que, pelo Lema 1.1.1, $ba = a^{n-1}b \neq ab$.

Portanto, $(D_n, \circ)$ é grupo não abeliano.

Falta verificar que D_n tem exatamente $2n$ elementos. Para isso vamos mostrar que os elementos do conjunto $\{e, a, a^2, \cdots, a^{n-1}, b, ab, a^2b, \cdots, a^{n-1}b\}$ são distintos dois a dois.

Sejam $i, j \in \{0, 1, 2, \cdots, n-1\}$ e $u, v \in \{0, 1\}$ tais que $a^ib^u = a^jb^v$. Devemos verificar que $i = j$ e $u = v$.

Multiplicando à esquerda por $(a^j)^{-1}$ e à direita por $(b^u)^{-1}$ ficamos com

$a^ib^u = a^jb^v \Longrightarrow (a^j)^{-1}a^i = b^v(b^u)^{-1} = b^{-u+v} \in \{e, a, \ldots, a^{n-1}\}$, pois $(a^j)^{-1}a^i$ é uma rotação.

Se $u \neq v$ então $b^{-u+v} \notin \{e, a, \cdots, a^{n-1}\}$. Absurdo.

Logo, $u = v$ e a igualdade $a^ib^u = a^jb^v$ leva a $a^i = a^j$, e daí $i = j$.

Portanto, D_n tem $2n$ elementos.

■

Definição 1.1.5 O grupo $(D_n, \circ)$ é chamado **grupo diedral** de ordem $2n$, ou grupo das simetrias do polígono regular de n lados.

Exemplo 1.1.8 $D_3 = \{e, a, a^2, b, ab, a^2b\}$ é o grupo das simetrias do triângulo equilátero de vértices 1, 2 e 3, onde $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ é a rotação de ângulo $\frac{2\pi}{3}$ e $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ é a reflexão em relação ao eixo horizontal.

Exemplo 1.1.9 D_4 é o grupo das simetrias do quadrado. Um quadrado desenhado no plano possui 8 simetrias: a identidade, 3 rotações de ângulos $\frac{\pi}{2}, \pi, \frac{3\pi}{2}$, 2 reflexões através de suas mediatrizes e 2 reflexões através de suas diagonais.

1.2 Subgrupos

A partir de agora falaremos dos subgrupos, que são grupos dentro de grupos dados. Veremos que a noção de subgrupo é útil para produzir novos exemplos de grupos.

Definição 1.2.1 Seja $(G, *)$ um grupo. Dizemos que $H \subseteq G$, $H \neq \varnothing$, é um **subgrupo** de G quando:

(i) $a, b \in H \Longrightarrow a * b \in H$.

(ii) $(H, *)$ é grupo.

Notação. Para indicar que H é subgrupo de G, escrevemos $H \leq G$.

Se H é subgrupo de G, existem elementos neutros e_H e e_G em H e G respectivamente. Também, para cada $a \in H \subseteq G$, existem simétricos ${a_H}^{-1}$ e ${a_G}^{-1}$ em H e G respectivamente. Veremos na proposição abaixo que $e_H = e_G$ e ${a_H}^{-1} = {a_G}^{-1}$.

Proposição 1.2.1 Sejam $H \leq G$ e $a \in H$. Então:

(a) $e_H = e_G$.

(b) ${a_H}^{-1} = {a_G}^{-1}$.

Demonstração:

(a) e_H é elemento neutro de H e $e_H \in H$, então $e_H * e_H = e_H$.

e_G é elemento neutro de G e $e_H \in H \subseteq G$, então $e_G * e_H = e_H$.

Segue que, $e_H * e_H = e_G * e_H$.

Como $e_H \in G$ e G é grupo, temos que existe ${e_H}^{-1} \in G$ simétrico de e_H.

De onde vem que,

$$(e_H * e_H) * {e_H}^{-1} = (e_G * e_H) * {e_H}^{-1} \Longrightarrow e_H * (e_H * {e_H}^{-1}) = e_G * (e_H * {e_H}^{-1})$$
$$\Longrightarrow e_H * e_G = e_G * e_G$$
$$\Longrightarrow e_H = e_G.$$

(b) Por (a) podemos escrever $e_H = e_G = e$. Assim,

$$ {a_H}^{-1} * a = a * {a_H}^{-1} = e \text{ e } {a_G}^{-1} * a = a * {a_G}^{-1} = e,$$

ou seja, ${a_H}^{-1}$ e ${a_G}^{-1}$ são simétricos de a em G ($H \subseteq G$). Pela unicidade do simétrico, temos que ${a_H}^{-1} = {a_G}^{-1}$.

■

A proposição acima nos informa que, se o elemento neutro do grupo G não está em H, então H não é subgrupo de G.

Veremos agora uma forma mais breve de verificar se um subconjunto é um grupo.

Proposição 1.2.2 Seja H um subconjunto não vazio do grupo G. São equivalentes:

(a) $H \leq G$

(b) $a, b \in H \Longrightarrow a * b^{-1} \in H$, b^{-1} simétrico de b.

Demonstração:

$(a) \Longrightarrow (b)$ Como H é grupo e $b \in H$, existe $b^{-1} \in H$. De onde vem que, $a * b^{-1} \in H$ (operação fechada).

$(b) \Longrightarrow (a)$ Como H é um conjunto não vazio, existe $x \in H \subseteq G$. Por (b) vem que $e = x * x^{-1} \in H$, ou seja, o elemento neutro está em H.

Dado $b \in H$, temos $e, b \in H$ e por (b) vem que $b^{-1} = e * b^{-1} \in H$, ou seja, o elemento simétrico está em H.

Mostremos agora que H é fechado para a operação $*$. De fato, se $a, b \in H$, então levando em consideração a existência de simétrico já provada acima, temos que $a, b^{-1} \in H$. De onde vem, novamente pela hipótese que, $a * (b^{-1})^{-1} = a * b \in H$.

Falta mostrar a associatividade em H, mas isso é trivial, pois se $a, b, c \in H$, então $a, b, c \in G$ $(H \subseteq G)$ e, portanto, $(a * b) * c = a * (b * c)$ (vale a associatividade em G, pois G é grupo).

■

Observação 1.2.1 Note que quando o grupo é aditivo a condição (b) é dada por:

- $a, b \in H \Longrightarrow a + (-b) \in H$.

E se o grupo é multiplicativo a condição (b) é dada por:

- $a, b \in H \Longrightarrow a \cdot b^{-1} \in H$.

Exemplo 1.2.1 Usando a Proposição 1.2.2 vem que:

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$;

$(\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot)$.

Exemplo 1.2.2 Para cada $m \in \mathbb{Z}$ o conjunto $m\mathbb{Z} = \{mx; x \in \mathbb{Z}\}$ é subgrupo de $(\mathbb{Z}, +)$.

Sejam $a, b \in m\mathbb{Z}$, então existem $x, y \in \mathbb{Z}$ tais que $a = mx$ e $b = my$.

Assim, $a - b = mx - my = m(x - y) \in m\mathbb{Z}$.

Pela Proposição 1.2.2 vem que $m\mathbb{Z} \leq \mathbb{Z}$.

Exemplo 1.2.3 Existem alguns subgrupos dos grupos lineares $GL_n(K), K$ subcorpo de $\mathbb{C}$, que são importantes para aplicações. O conjunto $SL_n(K)$ composto de matrizes invertíveis $n \times n$ com entradas em um corpo K e cujo determinante é 1_K, é subgrupo de $GL_n(K)$, chamado grupo linear especial.

Sejam $A, B \in SL_n(K)$. Como B é invertível temos que existe B^{-1} e

$$\det(B \cdot B^{-1}) = \det(I) \Longrightarrow \det B \cdot \det B^{-1} = 1$$

$$\Longrightarrow \det B^{-1} = 1 \text{ (pois } \det B = 1_K)$$

$$\Longrightarrow B^{-1} \in SL_n(K).$$

Devemos provar que $A \cdot B^{-1} \in SL_n(K)$.

$\det(A \cdot B^{-1}) = \det(A) \cdot \det(B^{-1}) = 1 \cdot 1 = 1 \Longrightarrow A \cdot B^{-1} \in SL_n(K)$.

Existe uma maneira padrão para produzir subgrupos. Para isso tomamos um elemento x num grupo G e introduzimos a notação:

$\langle x \rangle = \{x^m; m \in \mathbb{Z}\}$.

Proposição 1.2.3 Sejam G um grupo e $x \in G$. Então $\langle x \rangle$ é subgrupo abeliano de G.

Demonstração:

Sejam $a, b \in \langle x \rangle$. Então existem $m, n \in \mathbb{Z}$ tais que $a = x^m$ e $b = x^n$.

Temos $a * b^{-1} = x^m * x^{-n} = x^{m-n} \in \langle x \rangle$.

Logo, $\langle x \rangle \leq G$.

Falta verificar que $\langle x \rangle$ é abeliano.

$x^m * x^n = x^{m+n} = x^{n+m} = x^n * x^m$.

■

Definição 1.2.2 Sejam G um grupo e $x \in G$. O subgrupo $\langle x \rangle$ é chamado de **subgrupo gerado** por x.

Definição 1.2.3 Dizemos que o grupo G é **cíclico** quando existe $x \in G$ tal que $G = \langle x \rangle$.

Note que pela definição acima, $\langle x \rangle$ é um subgrupo cíclico de G, para cada $x \in G$.

Exemplo 1.2.4 $(n\mathbb{Z}, +)$ é grupo cíclico pois $n\mathbb{Z} = \langle n \rangle = \{nm; m \in \mathbb{Z}\}$.

Definição 1.2.4 A **ordem** de um grupo G é o número de elementos do conjunto G.

Notação: A ordem do grupo G é indicada por $|G|$.

Definição 1.2.5 Sejam G um grupo e $x \in G$. A **ordem** de x é a ordem do subgrupo gerado por x, isto é, $|\langle x \rangle|$.

Notação: A ordem de x é indicada por $o(x)$.

Proposição 1.2.4 Seja $G = \langle a \rangle$ um grupo cíclico de ordem n.

(a) Se $H \leq G$, então H é cíclico. Além disso, se $H \neq \{e\}$, então $H = \langle a^m \rangle$ e $|H| = \dfrac{n}{m}$, onde m é o menor inteiro positivo tal que $a^m \in H$.

(b) Se $d \in \mathbb{N}^*$ e d divide n, então existe um único subgrupo H de G tal que $|H| = d$. Neste caso, $H = \langle a^{\frac{n}{d}} \rangle$.

Demonstração:

(a) É claro que $H = \{e\}$ é subgrupo cíclico de G. Assuma agora $H \neq \{e\}$.

Note que $G = \langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$, então todo elemento de H é da forma a^x, para $x \in \{0, 1, \cdots, n-1\}$.

Como $H \neq \{e\}$, existe um menor elemento $m \in \{1, 2, \cdots, n-1\}$ tal que $a^m \in H$.

Vamos mostrar que $H = \langle a^m \rangle$.

É óbvio que $\langle a^m \rangle \subseteq H$, pois $a^m \in H$.

Falta mostrar que $H \subseteq \langle a^m \rangle$.

Seja $h \in H$. Então $h = a^x, x \in \{0, 1, \cdots, n-1\}$. Aplicando o algoritmo de Euclides para x e m obtemos, $q, r \in \mathbb{N}$ tais que

$$x = mq + r, \text{ com } 0 \leq r < m.$$

Assim,

$$h = a^x = a^{mq+r} = (a^m)^q \cdot a^r.$$

Note que:

$a^m \in H \Longrightarrow (a^m)^q \in H \Longrightarrow (a^m)^{-q} \in H \Longrightarrow h(a^m)^{-q} \in H \Longrightarrow a^r \in H.$

Pela minimalidade de m vem que $r = 0$.

Logo, $x = mq$, ou seja, $h = a^x = a^{mq} = (a^m)^q \in \langle a^m \rangle$.

Portanto, $H = \langle a^m \rangle$.

Seja $d = |H| = o(a^m)$. Então d é o menor número natural não nulo tal que $(a^m)^d = e$.

Por outro lado, n é o menor natural não nulo tal que $a^n = e$.

Logo, $n = md$, de onde vem que, $d = \dfrac{n}{m} = |H|$.

(b) Como d divide n, existe $t \in \mathbb{N}^*$ tal que $n = dt$.

Tome $H = \langle a^t \rangle \leq G$ e seja $r = o(a^t) = |H|$.

Como $(a^t)^d = a^n = e$, vem que $r \leq d$.

Suponha que $r < d$. Então $rt < dt = n$. Mas isso é um absurdo, pois $a^{rt} = (a^t)^r = e$ e n é o menor natural não nulo tal que $a^n = e$.

Logo, $r = d$, portanto, $|H| = r = d$ e $H = \langle a^t \rangle = \langle a^{\frac{n}{d}} \rangle$.

Falta provar a unicidade.

Seja $K \leq G$ tal que $|K| = d$.

Se $d = 1$, então $K = \{e\}$ é o único subgrupo de ordem $d = 1$.

Se $d \neq 1$, pelo item (i) temos que $K = \langle a^m \rangle$ e $|K| = \dfrac{n}{m}$.

Logo, $d = \dfrac{n}{m}$, isto é, $m = \dfrac{n}{d}$. Portanto, $K = \langle a^{\frac{n}{d}} \rangle = H$.

■

1.3 Subgrupo Normal e Grupo Quociente

Sejam G um grupo e $H \leq G$. Destacaremos duas relações de equivalência em G obtidas a partir de H. As classes de equivalência de uma destas relações serão chamadas classes laterais à esquerda de H em G, e as classes da outra serão chamadas classes laterais à direita de H em G. Quando G for finito, provaremos que a ordem de H divide a ordem de G. Este resultado é conhecido como Teorema de Lagrange.

Quando a classe lateral à esquerda de cada elemento de G coincide com a classe lateral à direita, dizemos que H é subgrupo normal de G, definiremos formalmente isto mais adiante. Neste caso, é possível construir o grupo quociente $\frac{G}{H}$.

Proposição 1.3.1 Sejam G um grupo, $H \leq G$ e $x, y \in G$. As relações

$$y \sim_L x \iff x^{-1} * y \in H \text{ e } y \sim_R x \iff y * x^{-1} \in H$$

são relações de equivalência em G.

Demonstração:

- Reflexiva: $x \sim_L x$, $\forall x \in G$, pois $e = x^{-1} * x \in H$.
- Simétrica:

$y \sim_L x \implies x^{-1} * y \in H$

$\implies y^{-1} * x = (x^{-1} * y)^{-1} \in H$

$\implies x \sim_L y; \forall x, y \in G.$

- Transitiva:

$y \sim_L x$ e $x \sim_L z \implies x^{-1} * y \in H$ e $z^{-1} * x \in H$

$\implies (z^{-1} * x) * (x^{-1} * y) = z^{-1} * y \in H$

$\implies y \sim_L z.$

Demonstração análoga para $\sim_R$.

■

Observação 1.3.1 Note que:

$$y \sim_L x \iff x^{-1} * y \in H$$

$$\iff \exists h \in H; x^{-1} * y = h$$

$$\iff y = xh, \text{ para algum } h \in H$$

$$\iff y \in xH = \{xh; h \in H\}.$$

Logo, a classe de equivalência de $x \in G$, definida pela relação $\sim$, é

$$\{y \in G; y \sim_L x\} = xH.$$

Definição 1.3.1 A classe de equivalência $xH = \{xh; h \in H\}$ é chamada **classe lateral** de x **à esquerda** de H em G. Analogamente para a relação $\sim_R$, $Hx = \{hx; h \in H\}$ é chamada **classe lateral** de x **à direita** de H em G.

Antes de enunciar o próximo teorema vamos fixar a seguinte notação.

Notação. Seja X um conjunto qualquer. A cardinalidade de X, ou seja, a quantidade de elementos do conjunto X, será denotado por $|X|$.

Teorema 1.3.1 Sejam G um grupo, $H \leq G$ e $x, y \in G$. Então:

(a) Duas classes laterais à esquerda (ou à direita) são iguais ou disjuntas.

(b) A união das classes laterais à esquerda (ou à direita) disjuntas é G.

(c) Toda classe lateral de H em G tem $|H|$ elementos.

(d) A quantidade de classes laterais à esquerda e à direita é a mesma.

Demonstração:

(a) Vamos demonstrar este fato para classes laterais à esquerda. O outro caso é análogo.

Sejam xH e yH classes laterais à esquerda.

Suponha que $xH \bigcap yH \neq \emptyset$. Então existe $z \in G$ tal que $z \in xH \bigcap yH$.

Seja $u \in yH$ então $u \sim_L y$, mas $z \in yH$ então $z \sim_L y$. Logo, $y \sim_L z$ e por transitividade $u \sim_L z$.

Por outro lado $z \in xH$ então $z \sim_L x$ e portanto $u \sim_L x$, o que significa que $u \in xH$. Portanto $yH \subseteq xH$.

Com raciocínio análogo, também podemos provar que $xH \subseteq yH$. Logo $xH = yH$.

Portanto, $xH \bigcap yH = \emptyset$ ou $xH = yH$.

(b) Seja $\{x_iH\}_{i \in r}$ o conjunto das classes laterais à esquerda que são disjuntas. Devemos provar que $G = \bigcup x_iH$.

Como $x_iH \subseteq G$, então $\bigcup x_iH \subseteq G$.

Seja agora $z \in G$, considere a sua classe lateral à esquerda, ela deve ser igual a algum x_iH, ou seja, $zH \in \{x_iH\}_{i \in r}$. Logo $z \in zH \subseteq \bigcup x_iH$, e então $G \subseteq \bigcup x_iH$.

O caso para classes laterais à direita é análogo.

(c) Dado $x \in G$ devemos mostrar que $|xH| = |Hx| = |H|$.

Defina: $\varphi_1 : H \longrightarrow xH$ e $\varphi_2 : H \longrightarrow Hx$

$$h \longmapsto xh \qquad\qquad h \longmapsto hx.$$

Basta verificar que φ_1 e φ_2 são bijeções.

Note que φ_1 é sobrejetora, pois para todo $z \in xH$, temos $z = xh$, para algum $h \in H$. Logo, $z = \varphi_1(h)$.

Devemos provar que φ_1 é injetiva.

Sejam $a, b \in H$.

$\varphi_1(a) = \varphi_1(b) \Longrightarrow xa = xb \Longrightarrow x^{-1}xa = x^{-1}xb \Longrightarrow a = b.$

Analogamente provamos que φ_2 é bijeção.

(d) Vamos provar que

$$\varphi : \{xH; x \in G\} \longrightarrow \{Hx; x \in G\}$$

$$xH \longmapsto Hx^{-1}$$

está bem definida e é bijetora.

• φ está bem definida e é injetiva:

$$xH = yH \iff y \in xH$$

$$\iff y = xh, h \in H$$

$$\iff x = yh^{-1}, h \in H$$

$$\iff e = x^{-1}yh^{-1}, h \in H$$

$$\iff h = x^{-1}y, h \in H$$

$$\iff hy^{-1} = x^{-1}, h \in H$$

$$\iff x^{-1} \in Hy^{-1}, h \in H$$

$$\iff Hx^{-1} = Hy^{-1} \, (*)$$

$$\iff \varphi(xH) = \varphi(yH)$$

Vamos provar $(*)$.

$x^{-1} \in Hy^{-1} \Longrightarrow x^{-1} = hy^{-1}, h \in H.$

$(\subseteq)$ $u \in Hx^{-1} \Longrightarrow u = h_1x^{-1}, h_1 \in H$

$$\Longrightarrow u = h_1(hy^{-1})$$

$$\Longrightarrow u = (h_1h)y^{-1}$$

$$\Longrightarrow u \in Hy^{-1}.$$

$(\supseteq)$ É análogo.

Logo, $Hx^{-1} = Hy^{-1}$.

• Claro que φ é sobrejetiva, basta considerar $Hy \in \{Hx; x \in G\}$ e então tome $y^{-1}H \in \{xH; x \in G\}$. Então $\varphi(y^{-1}H) = Hy$.

Portanto φ é bijetora e assim os dois conjuntos tem o mesmo número de elementos.

■

Definição 1.3.2 Seja $H \leq G$. O **índice** de H em G é a cardinalidade do conjunto de classes laterais à esquerda de H em G.

Notação: Indicamos o índice de H em G por $(G : H)$.

Teorema 1.3.2 Teorema de Lagrange.

Sejam G um grupo finito e $H \leq G$. Então:

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

Demonstração: Como G é finito, temos que $(G : H) = n$, para algum $n \in \mathbb{N}$.

Seja $\{x_1H, x_2H, \cdots, x_nH\}$ o conjunto das classes laterais à esquerda (distintas) de H em G. Pelo Teorema 1.3.1 (a) e (b), temos:

$G = x_1H \bigcup x_2H \bigcup \cdots \bigcup x_nH$ e $x_iH \bigcap x_jH = \emptyset$ se $i \neq j$.

Novamente pelo Teorema 1.3.1 (c), vem que $|x_iH| = |H|$, $\forall i \in \{1, 2, \cdots, n\}$.

Logo,

$$|G| = \underbrace{|H| + |H| + \cdots + |H|}_{n \text{ vezes}} = |H| \cdot n = |H|(G : H).$$

■

Se G é um grupo e H é subgrupo normal de G, mostraremos que o conjunto $\frac{G}{H}$, formado pelas classes laterais de H em G, possui uma operação bem definida que torna $\frac{G}{H}$ um grupo.

Iniciamos tomando um grupo G, $H \leq G$ e estabelecendo a notação

$$\frac{G}{H} = \{xH; x \in G\},$$

para indicar o conjunto das classes laterais à esquerda de H em G.

Queremos descobrir sob que condições, impostas a H, a operação entre classes

$$\begin{aligned} \cdot : \frac{G}{H} \times \frac{G}{H} &\longrightarrow \frac{G}{H} \\ (xH, yH) &\longmapsto xyH \end{aligned}$$

está bem definida.

Proposição 1.3.2 Seja H um subgrupo de G. São equivalentes:

(a) A operação entre classes laterais à esquerda de H em G está bem definida.

(b) $gHg^{-1} \subseteq H, \forall g \in G$.

(c) $gHg^{-1} = H, \forall g \in G$.

(d) $gH = Hg, \forall g \in G$.

Demonstração:

$(a) \Longrightarrow (b)$ Sejam $xH = x_1H \in \dfrac{G}{H}$ e $yH = y_1H \in \dfrac{G}{H}$.

$xH = x_1H \Longrightarrow x_1 \in xH \Longrightarrow x_1 = xh$, para algum $h \in H$.

$yH = y_1H \Longrightarrow y_1 \in yH \Longrightarrow y_1 = yk$, para algum $k \in H$.

Por hipótese, a operação está bem definida. Logo:

$$\begin{aligned} xHyH = x_1Hy_1H &\Longleftrightarrow xyH = x_1y_1H \\ &\Longleftrightarrow x_1y_1 \in xyH \\ &\Longleftrightarrow xhyk \in xyH \\ &\Longleftrightarrow hyk \in yH \\ &\Longleftrightarrow \exists h_1 \in H \text{ tal que } hyk = yh_1 \\ &\Longleftrightarrow y^{-1}hy = h_1k^{-1}, h_1 \in H \end{aligned}$$

$$\iff y^{-1}hy \in H.$$

Note que x, y, x_1, y_1 são elementos quaisquer de G.

Seja $g \in G$. Basta então fazer $y = g^{-1}$, obtendo $ghg^{-1} \in H$, para todo $h \in H$.

Logo, $gHg^{-1} \subseteq H$.

$(b) \implies (c)$ Precisamos mostrar apenas que $H \subseteq gHg^{-1}, \forall g \in G$.

Sejam $g \in G$ e $h \in H$. Note que por hipótese $g^{-1}Hg \subseteq H$. Assim:

$g^{-1}hg \in g^{-1}Hg \subseteq H \implies g^{-1}hg = k$, para algum $k \in H$

$$\implies h = gkg^{-1} \in gHg^{-1}.$$

Logo, $H \subseteq gHg^{-1}$.

$(c) \implies (d)$ Dado $g \in G$, temos por hipótese que $gHg^{-1} = H$.

Seja $gh \in gH$. Claro que $ghg^{-1} \in gHg^{-1} = H$. Logo $ghg^{-1} = k$ para algum $k \in H$. Segue que $gh = kg \in Hg$.

Portanto, $gH \subseteq Hg$ e, analogamente, prova-se que $Hg \subseteq gH$.

$(d) \implies (a)$ Sejam $xH = x_1H$ e $yH = y_1H$. Temos que mostrar que $x_1y_1H = xyH$.

$(\subseteq)$ Seja $a \in x_1y_1H$. Então existe $h \in H$ tal que $a = x_1y_1h$.

Como $y_1H = Hy_1$ então existe $k \in H$ tal que $y_1h = ky_1$.

Também temos que $x_1H = xH$ então existe $l \in H$ tal que $x_1k = xl$.

Novamente $Hy_1 = y_1H$, então existe $m \in H$ tal que $ly_1 = y_1m$.

Finalmente, como $y_1H = yH$ temos que existe $n \in H$ tal que $y_1m = yn$.

Portanto,

$a = x_1y_1h = x_1ky_1 = xly_1 = xy_1m = xyn \in xyH \implies x_1y_1H \subseteq xyH$.

Com raciocínio análogo podemos provar que $xyH \subseteq x_1y_1H$.

■

Definição 1.3.3 Seja H um subgrupo de G. Dizemos que H é **subgrupo normal** de G quando valem as condições equivalentes da proposição anterior.

Notação: $H \lhd G$ indica que H é subgrupo normal de G.

Exemplo 1.3.1 $(\mathbb{Z}, +) \lhd (\mathbb{Q}, +) \lhd (\mathbb{R}, +) \lhd (\mathbb{C}, +)$

$(\mathbb{Q}^*, \cdot) \lhd (\mathbb{R}^*, \cdot) \lhd (\mathbb{C}^*, \cdot)$

$(m\mathbb{Z}, +) \lhd (\mathbb{Z}, +), \forall m \in \mathbb{Z}$

Exemplo 1.3.2 Lembre que $GL_n(\mathbb{R})$ é o grupo multiplicativo das matrizes reais de ordem n inversíveis, isto é, que têm determinante não nulo e $SL_n(\mathbb{R})$ é o grupo multiplicativo das matrizes reais de ordem n com determinante unitário. Então $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Pelo Exemplo 1.2.3, $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Falta mostrar que $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Sejam $X \in GL_n(\mathbb{R})$ e $Y \in SL_n(\mathbb{R})$. Dessa forma, $\det X \neq 0$ e $\det Y = 1$.

Note que $\det X^{-1} \neq 0$, pois

$$1 = \det(XX^{-1}) = \det X \det X^{-1} \Longrightarrow \det X^{-1} \neq 0.$$

Então vamos provar o que nos interessa.

$$\begin{aligned} \det(XYX^{-1}) &= \det X \cdot \det Y \cdot \det X^{-1} \\ &= \det X \cdot 1 \cdot \det X^{-1} \\ &= 1. \end{aligned}$$

Logo, $XYX^{-1} \in SL_n(\mathbb{R})$.

Portanto, pela Proposição 1.3.2 item (b), $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Como último assunto desta seção, vamos utilizar subgrupos normais para produzir grupos quocientes.

Teorema 1.3.3 Se H é subgrupo normal de G, então $\left(\frac{G}{H}, \cdot\right)$ é grupo.

Demonstração:

Devemos provar os três axiomas de grupo.

• Associatividade: Sejam $xH, yH, zH \in \frac{G}{H}$. Então $x, y, z \in G$ e $(xy)z = x(yz)$.

Logo, $(xH\, yH)zH = xyH\, zH = (xy)zH = x(yz)H = xH(yHzH)$.

• Elemento neutro: O elemento $eH = H \in \frac{G}{H}$ e dado $xH \in \frac{G}{H}$, temos:

$eH\, xH = exH = xH$ e $xH\, eH = xeH = xH$.

Logo, eH é o elemento neutro de $\frac{G}{H}$.

• Simétrico: Dado $xH \in \frac{G}{H}$, temos $x^{-1}H \in \frac{G}{H}$. Além disso,

$xH\, x^{-1}H = xx^{-1}H = eH$ e $x^{-1}H\, xH = x^{-1}xH = eH$.

Portanto, o simétrico de xH é $x^{-1}H$.

■

Definição 1.3.4 O grupo $\frac{G}{H}$ é chamado **grupo quociente** de G por H.

1.4 Homomorfismos e Isomorfismos

O objetivo principal desta seção são as funções entre grupos, que preservam as operações destes grupos. A estas funções chamamos de homomorfismo de grupos.

Definição 1.4.1 Sejam $(G, \cdot)$ e $(H, *)$ grupos. Um **homomorfismo** de G em H é uma função $f : G \longrightarrow H$ que satisfaz

$$f(a \cdot b) = f(a) * f(b),\ \forall a, b \in G.$$

Definição 1.4.2 Um homomorfismo injetor é chamado **monomorfismo**.

Um homomorfismo sobrejetor é chamado **epimorfismo**.

Um homomorfismo bijetor é chamado **isomorfismo**.

Um homomorfismo $f : G \longrightarrow G$ é chamado **endomorfismo**.

Um isomorfimo $f : G \longrightarrow G$ é chamado **automorfismo**.

Notações. $End(G) = \{f : G \longrightarrow G; f \text{ é homomorfismo}\}$.

$Aut(G) = \{f : G \longrightarrow G; f \text{ é isomorfismo}\}$.

$G \simeq H$ indica que G e H são isomorfos, isto é, existe um isomorfismo $f : G \longrightarrow H$.

Exemplo 1.4.1 Para cada $n \in \mathbb{Z}$, a função $f_n : \mathbb{Z} \longrightarrow \mathbb{Z}$, $f_n(x) = nx, \forall x \in \mathbb{Z}$ é endomorfismo do grupo $(\mathbb{Z}, +)$.

Sejam $a, b \in \mathbb{Z}$, temos:

$f_n(a + b) = n \cdot (a + b) = na + nb = f_n(a) + f_n(b)$.

O exemplo acima apresenta uma infinidade de endomorfismos do grupo $(\mathbb{Z}, +)$, um para cada $n \in \mathbb{Z}$.

Vamos agora definir núcleo e imagem para um homomorfismo de grupos.

Definição 1.4.3 Seja $f : G \longrightarrow H$ um homomorfismo de grupos.

O **núcleo** (ou **kernel**) de f é o conjunto dos elementos de G cuja imagem é o elemento neutro de H, isto é,

$$N(f) = \{x \in G; f(x) = e_H\}.$$

A **imagem** do homomorfismo de grupos é a imagem da função f, isto é,

$$Im(f) = \{f(x); x \in G\}.$$

Exemplo 1.4.2 Para cada $n \in \mathbb{Z}$, considere o homomorfismo $f_n : \mathbb{Z} \longrightarrow \mathbb{Z}, f_n(x) = nx$. Então:

- Para $n = 0$ temos que f_n é o homomorfismo nulo e, portanto

$$N(f_0) = \mathbb{Z} \text{ e } Im(f_0) = \{0\}.$$

- Para $n \neq 0$ temos:

$$N(f_n) = \{x \in \mathbb{Z}; f_n(x) = 0\} = \{x \in \mathbb{Z}; nx = 0\} = \{0\}$$

$$Im(f_n) = \{f_n(x); x \in \mathbb{Z}\} = \{nx; x \in \mathbb{Z}\} = n\mathbb{Z}.$$

A seguir apresentaremos uma proposição com alguns resultados importantes sobre homomorfismo e núcleo.

Proposição 1.4.1 Sejam $(G, \cdot)$, $(H, *)$ grupos; $f : G \longrightarrow H$ homomorfismo de grupos, e_G o elemento neutro de G e e_H o elemento neutro de H.

(a) $f(e_G) = e_H$.

(b) $f(g^{-1}) = (f(g))^{-1}, \forall g \in G$.

(c) $N(f) \lhd G$.

(d) f é monomorfismo $\Longleftrightarrow N(f) = \{e_G\}$.

Demonstração:

(a) Como f é homomorfismo de grupos temos que:

$f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$

Multiplicando a igualdade acima por $(f(e_G))^{-1}$ ficamos com:

$f(e_G) * (f(e_G))^{-1} = f(e_G) * f(e_G) * (f(e_G))^{-1} \Longrightarrow e_H = f(e_G) * e_H = f(e_G)$.

(b) Como $g \cdot g^{-1} = e_G, \forall g \in G$ temos que $f(g \cdot g^{-1}) = f(e_G)$.

Por (a), $f(g \cdot g^{-1}) = f(e_G) = e_H \Longrightarrow f(g) * f(g^{-1}) = f(e_G) = e_H$.

Analogamente provamos que $f(g^{-1}) * f(g) = f(e_G) = e_H$.

Isso mostra que o simétrico de $f(g)$ é $f(g^{-1})$, ou seja, $(f(g))^{-1} = f(g^{-1})$.

(c) Primeiro devemos provar que $N(f) \leq G$.

Sejam $a, b \in N(f)$. Então $f(a) = f(b) = e_H$.

Por (b) temos

$f(a \cdot b^{-1}) = f(a) * f(b^{-1}) = f(a) * (f(b))^{-1} = e_H * (e_H)^{-1} = e_H$.

Logo, $a \cdot b^{-1} \in N(f)$ e, portanto $N(f) \leq G$.

Para verificar que $N(f) \lhd G$, tome $g \in G$ e $a \in N(f)$. Devemos mostrar que $g \cdot a \cdot g^{-1} \in N(f)$.

$f(g \cdot a \cdot g^{-1}) = f(g) * f(a) * f(g^{-1}) = f(g) * e_H * (f(g))^{-1} = e_H$.

Portanto, $N(f) \lhd G$.

(d) $(\Longrightarrow)$ Seja $x \in G$. Como f é injetiva temos que:

$x \in N(f) \Longleftrightarrow f(x) = e_H = f(e_G) \Longleftrightarrow x = e_G$.

Logo, $N(f) = \{e_G\}$.

$(\Longleftarrow)$ Sejam $x, y \in G$. Então:

$f(x) = f(y) \Longleftrightarrow f(x) * (f(y))^{-1} = e_H$

$\Longleftrightarrow f(x) * f(y^{-1}) = e_H$

$\Longleftrightarrow f(x \cdot y^{-1}) = e_H$

$\Longleftrightarrow x \cdot y^{-1} \in N(f) = \{e_G\}$

$\Longleftrightarrow x \cdot y^{-1} = e_G$

$\Longleftrightarrow x = y.$

Portanto, f é injetora.

■

Como $f : G \longrightarrow H$ é homomorfismo de grupos e $N(f) \lhd G$, então sempre existe o grupo quociente $\dfrac{G}{N(f)}$.

A seguir apresentaremos a principal ferramenta para produzir isomorfismo entre grupos, o Teorema do Isomorfismo.

Teorema 1.4.1 Teorema do Isomorfismo.

Seja $f : G \longrightarrow H$ um homomorfismo de grupos. Então:

$$\begin{aligned} \overline{f} : \frac{G}{N(f)} &\longrightarrow Im(f) \\ gN(f) &\longmapsto f(g) \end{aligned}$$

é isomorfismo.

Demonstração: Como os elementos de $\dfrac{G}{N(f)}$ são classes de equivalência, devemos mostrar que $\overline{f}$ não depende da escolha dos representantes da classe lateral. Isto é, devemos mostrar que, se $g_1N(f) = g_2N(f)$ em $\dfrac{G}{N(f)}$, então $\overline{f}(g_1N(f)) = \overline{f}(g_2N(f))$.

$$\begin{aligned} g_1N(f) = g_2N(f) &\Longrightarrow g_1 \in g_2N(f) \\ &\Longrightarrow g_1 = g_2x, \text{ para algum } x \in N(f) \\ &\Longrightarrow f(g_1) = f(g_2x) = f(g_2)f(x) = f(g_2)e = f(g_2) \\ &\Longrightarrow \overline{f}(g_1N(f)) = f(g_1) = f(g_2) = \overline{f}(g_2N(f)). \end{aligned}$$

Logo, $\overline{f}$ está bem definida.

Para ver que $\overline{f}$ é homomorfismo, tome $g_1N(f)$ e $g_2N(f) \in \dfrac{G}{N(f)}$.

$$\begin{aligned} \overline{f}(g_1N(f)g_2N(f)) &= \overline{f}(g_1g_2N(f)) \\ &= f(g_1g_2) \end{aligned}$$

$$= f(g_1)f(g_2)$$

$$= \overline{f}(g_1N(f))\overline{f}(g_2N(f)).$$

Claro que $\overline{f}$ é sobrejetora, pois dado $y \in Im(f)$, temos que $y = f(x)$, para algum $x \in G$. Tomando $xN(f) \in \dfrac{G}{N(f)}$, vem que $\overline{f}(x(N(f))) = f(x) = y$.

Falta verificar que $\overline{f}$ é injetora.

Seja $gN(f) \in \dfrac{G}{N(f)}$, então:

$gN(f) \in N(\overline{f}) \Longleftrightarrow \overline{f}(gN(f)) = e$

$$\Longleftrightarrow f(g) = e$$

$$\Longleftrightarrow g \in N(f)$$

$$\Longleftrightarrow gN(f) = \{N(f)\}.$$

Portanto, $N(\overline{f}) = \{N(f)\}$, ou seja, $N(f)$ é o elemento neutro do grupo quociente $\dfrac{G}{N(f)}$ e $\overline{f}$ é isomorfismo.

■

Apresentaremos agora O Teorema de Cayley que permite concluir que, se conhecermos os grupos de permutações e seus subgrupos, conheceremos a menos de isomorfismo, todos os grupos.

Teorema 1.4.2 Teorema de Cayley.

Todo grupo é isomorfo a um subgrupo de um grupo de permutações.

Demonstração:

Seja G um grupo e considere o grupo de permutações $Bij(G)$. Defina

$T : G \longrightarrow Bij(G)$ $\qquad$ $T_g : G \longrightarrow G$

$g \longmapsto T_g$, onde $x \longmapsto gx$.

Primeiramente devemos verificar se T está bem definida.

• Claro que se $g = h$, então $T_g = T_h$, pois $T_g(x) = gx = hx = T_h(x), \forall x \in G$.

• T_g é injetora para todo $g \in G$ pois, para todo $x, y \in G$ temos,

$T_g(x) = T_g(y) \Longrightarrow gx = gy \Longrightarrow x = y$.

• T_g é sobrejetora, pois dado $x \in G$, escrevemos $x = g \cdot g^{-1} \cdot x$ e dessa maneira, $T_g(g^{-1}x) = x$.

Logo, T está bem definida.

• Afirmamos que T é homomorfismo de grupos.

De fato, dados $g_1, g_2 \in G$, temos:

$T_{g_1g_2}(x) = g_1g_2x = g_1(g_2x) = T_{g_1}(T_{g_2}(x)) = (T_{g_1} \circ T_{g_2})(x), \forall x \in G$.

Isso mostra que $T_{g_1g_2} = T_{g_1} \circ T_{g_2}$, então $T(g_1g_2) = T(g_1) \circ T(g_2)$.

Portanto, T é homomorfismo de grupos.

• T é sobrejetora sobre a imagem $T(G)$.

• Para mostrar que T é injetora vamos usar a Proposição 1.4.1 item (d).

Seja $g \in G$, então:

$g \in N(T) \Longleftrightarrow T(g) = Id$

$\Longleftrightarrow T_g = Id$

$\Longleftrightarrow T_g(x) = Id(x), \forall x \in G$

$\Longleftrightarrow gx = x, \forall x \in G$

$\Longleftrightarrow g = e$.

Segue que $G \simeq T(G) \leq \text{Bij}(G)$.

Portanto, G é isomorfo a um subgrupo do grupo de permutações $\text{Bij}(G)$.

■

Observação 1.4.1 O Teorema de Cayley diz que cada grupo G é isomorfo ao subgrupo

$$T(G) = \{T_g \in Bij(G); g \in G \,\mathrm{e}\, T_g(x) = gx, \forall x \in G\} \leq Bij(G).$$

Este grupo $T(G)$ é conhecido como **grupo de translações** à esquerda.

Capítulo 2

Ações de Grupos

2.1 Ações de Grupos

No capítulo passado vimos o Teorema de Cayley, que afirma que todo grupo é isomorfo a um subgrupo de um grupo de bijeções. 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 2.1.1 Uma **ação** de um grupo G em um conjunto X é um homomorfismo de G no grupo das bijeções em X.

Essa definição nos diz que os grupos agem em certos conjuntos, mudando os seus elementos de lugar.

Notação. Vamos denotar uma ação α por:

$$\alpha : G \longrightarrow Bij(X) \qquad\qquad \alpha_g : X \longrightarrow X$$

$$g \longmapsto \alpha_g \quad , \text{ onde } \quad x \longmapsto \alpha_g(x).$$

Portanto α_g é uma bijeção no conjunto X , que associa a cada elemento $x \in X$ o elemento $\alpha_g(x)$.

Observação 2.1.1 Como α é um homomorfismo, temos:

- $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$, para todos elementos $g, h \in G$ e $x \in X$.
- $\alpha_e = Id_X$, ou seja, $\alpha_e(x) = x$ para todo $x \in X$.
- $(\alpha_g)^{-1} = \alpha_{g^{-1}}$, para todo $g \in G$.

Exemplo 2.1.1 Considere o grupo $G = (\mathbb{Z}, +)$ e o conjunto $X = \mathbb{R}$.

$$\alpha : G \longrightarrow Bij(X) \qquad \alpha_n : X \longrightarrow X$$

$$n \longmapsto \alpha_n \quad , \text{ onde } \quad x \longmapsto \alpha_n(x) = x + n.$$

α é uma ação do grupo G no conjunto X.

Primeiramente note que α está bem definida.

- Claro que se $n = m$, então $\alpha_n = \alpha_m$, pois $\alpha_n(x) = x+n = x+m = \alpha_m(x), \forall x \in X$.
- α_n é injetora para todo $n \in G$ pois, para todo $x, y \in X$ temos,

$\alpha_n(x) = \alpha_n(y) \Longrightarrow x + n = y + n \Longrightarrow x = y$.

- α_n é sobrejetora, pois dado $x \in X$, basta tomar $y = x - n \in X$ e dessa maneira, $\alpha_n(y) = x$.

Agora devemos mostrar que α é homomorfismo.

De fato,

$$\begin{aligned}\alpha_n(\alpha_m(x)) &= \alpha_n(x + m) \\ &= (x + m) + n \\ &= x + (m + n) \\ &= \alpha_{m+n}(x).\end{aligned}$$

Logo α é uma ação do grupo G no conjunto X.

Exemplo 2.1.2 Considere o grupo $G = (\mathbb{R}^*, \cdot)$ e o conjunto $X = \mathbb{R}^2$.

$$\alpha : G \longrightarrow Bij(X) \qquad \alpha_\lambda : X \longrightarrow X$$

$$\lambda \longmapsto \alpha_\lambda \quad , \text{ onde } \quad z \longmapsto \alpha_\lambda(z) = \lambda z.$$

α é uma ação do grupo G no conjunto X.

Primeiramente note que α está bem definida.

• Claro que se $\lambda = \mu$, então $\alpha_\lambda = \alpha_\mu$, pois $\alpha_\lambda(z) = \lambda z = \mu z = \alpha_\mu(z), \forall z \in X$.

• α_λ é injetora para todo $\lambda \in G$ pois, para todo $y, z \in X$ temos,

$\alpha_\lambda(y) = \alpha_\lambda(z) \Longrightarrow \lambda y = \lambda z \Longrightarrow y = z$, pois $\lambda \in \mathbb{R}^*$.

• α_λ é sobrejetora, pois dado $z \in X$, basta tomar $y = \dfrac{1}{\lambda} z \in X$ e dessa maneira, $\alpha_\lambda(y) = z$.

Agora devemos mostrar que α é homomorfismo.

De fato,

$$\begin{aligned} \alpha_\lambda(\alpha_\mu(x, y)) &= \alpha_\lambda(\mu x, \mu y) \\ &= (\lambda\mu x, \lambda\mu y) \\ &= \lambda\mu(x, y) \\ &= \alpha_{\lambda\mu}(x, y). \end{aligned}$$

Logo α é uma ação do grupo G no conjunto X.

Exemplo 2.1.3 Considere o grupo $G = (\mathbb{Z}, +)$ e $X = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 = 1\} = \mathbb{S}^1$.

$$\alpha : G \longrightarrow Bij(X) \qquad \alpha_n : X \longrightarrow X$$

$$n \longmapsto \alpha_n \quad , \text{ onde } \quad z \longmapsto \alpha_n(z) = R_{n\theta}(z).$$

$\alpha_n = R_{n\theta} =$ rotação de um ângulo $n\theta, \theta$ um ângulo fixado.

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow^{R\psi} \begin{pmatrix} \cos\psi & -\text{sen}\,\psi \\ \text{sen}\,\psi & \cos\psi \end{pmatrix}_{2\times 2} \cdot \begin{pmatrix} x \\ y \end{pmatrix}_{2\times 1} = \begin{pmatrix} x\cos\psi - y\text{sen}\,\psi \\ x\text{sen}\,\psi + y\cos\psi \end{pmatrix}_{2\times 1}$$

Primeiro note que α_n de fato é bijeção em X.

Sejam $z \in X, z = (x, y), \psi = n\theta$ e $\varphi = m\theta$.

$$\begin{aligned}
\alpha_n \circ \alpha_m(z) &= R_{n\theta} \circ R_{m\theta}(z) \\
&= R_{\psi} \circ R_{\varphi}(z) \\
&= R_{\psi}(R_{\varphi}(z)) \\
&= R_{\psi} \begin{pmatrix} x\cos\varphi - y\text{sen}\,\varphi \\ x\text{sen}\,\varphi + y\cos\varphi \end{pmatrix}_{2\times 1} \\
&= \begin{pmatrix} \cos\psi & -\text{sen}\,\psi \\ \text{sen}\,\psi & \cos\psi \end{pmatrix}_{2\times 2} \cdot \begin{pmatrix} x\cos\varphi - y\text{sen}\,\varphi \\ x\text{sen}\,\varphi + y\cos\varphi \end{pmatrix}_{2\times 1} \\
&= \begin{pmatrix} \cos\psi \cdot (x\cos\varphi - y\text{sen}\,\varphi) - \text{sen}\,\psi \cdot (x\text{sen}\,\varphi + y\cos\varphi) \\ \text{sen}\,\psi \cdot (x\cos\varphi - y\text{sen}\,\varphi) + \cos\psi \cdot (x\text{sen}\,\varphi + y\cos\varphi) \end{pmatrix}_{2\times 1} \\
&= \begin{pmatrix} x(\cos\psi\cos\varphi - \text{sen}\,\psi\,\text{sen}\,\varphi) - y(\cos\psi\,\text{sen}\,\varphi + \text{sen}\,\psi\cos\varphi) \\ x(\text{sen}\,\psi\cos\varphi + \cos\psi\,\text{sen}\,\varphi) + y(-\text{sen}\,\psi\,\text{sen}\,\varphi + \cos\psi\cos\varphi) \end{pmatrix}_{2\times 1} \\
&= \begin{pmatrix} \cos(\psi+\varphi) & -\text{sen}\,(\psi+\varphi) \\ \text{sen}\,(\psi+\varphi) & \cos(\psi+\varphi) \end{pmatrix}_{2\times 2} \cdot \begin{pmatrix} x \\ y \end{pmatrix}_{2\times 1} \\
&= R_{\psi+\varphi}(z) \\
&= R_{n\theta+m\theta}(z). \\
&= R_{(n+m)\theta}(z). \\
&= \alpha_{n+m}(z).
\end{aligned}$$

Logo α é uma ação do grupo G no conjunto X.

Observação 2.1.2 No exemplo anterior como θ é uma ângulo fixado temos uma família de exemplos, um para cada θ.

Definição 2.1.2 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

$$O_x = \{\alpha_g(x); g \in G\}.$$

Exemplo 2.1.4 Considere o grupo $G = (\mathbb{Z}, +)$ e o conjunto $X = \mathbb{R}$.

$\alpha : G \longrightarrow Bij(X)$ $\qquad$ $\alpha_n : X \longrightarrow X$

$n \longmapsto \alpha_n$, onde $x \longmapsto \alpha_n(x) = x + n.$

$O_x = \{x + n; n \in \mathbb{Z}\}$.

Exemplo 2.1.5 Seja o grupo $G = (\mathbb{R}^*, \cdot)$ e o conjunto $X = \mathbb{R}^2 - \{(0, 0)\}$.

$\alpha : G \longrightarrow Bij(X)$ $\qquad$ $\alpha_\lambda : X \longrightarrow X$

$\lambda \longmapsto \alpha_\lambda$, onde $z \longmapsto \alpha_\lambda(z) = \lambda z.$

$O_z = \{\lambda z; \lambda \in \mathbb{R}^*\}$.

Definição 2.1.3 Seja α uma ação de um grupo G sobre um conjunto X e considere um elemento $x \in X$. Dizemos que a **órbita** desse elemento x é **periódica** quando:

$$\exists n \in G \text{ tal que } \alpha_n(x) = x.$$

Exemplo 2.1.6 Seja o grupo $G = (\mathbb{Z}, +)$ e $X = \{(x, y) \in \mathbb{R}^2; x^2 + y^2 = 1\} = \mathbb{S}^1$.

$\alpha : G \longrightarrow Bij(X)$ $\qquad$ $\alpha_n : X \longrightarrow X$

$n \longmapsto \alpha_n$, onde $z \longmapsto \alpha_n(z) = R_{n\theta}(z).$

• Caso 1: $\dfrac{\theta}{2\pi} = \dfrac{p}{q} \in \mathbb{Q} \Longrightarrow q\theta = p2\pi$ com $p, q \in \mathbb{Z}, q \neq 0$ e θ um ângulo fixado.

$\alpha_q = R_{q\theta} = R_{p2\pi} = Id = \alpha_0$.

Temos as seguintes ações: Id $= \alpha_0$, α_1, $\alpha_2, \cdots, \alpha_{q-1}$

$\therefore \forall x \in X; |O_x| = q.$

• Caso 2: $\dfrac{\theta}{2\pi} \in \mathbb{R} - \mathbb{Q}$. Neste caso nenhum elemento do conjunto tem órbita periódica.

Suponha $z = (x, y) \in \mathbb{S}^1$ tal que existe $n \in \mathbb{Z}$ tal que $\alpha_n(z) = z$.

$$R_{n\theta}(z) = z = R_{m2\pi}(z) \Longrightarrow R_{n\theta} = R_{m2\pi}$$
$$\Longrightarrow \frac{\theta}{2\pi} = \frac{m}{n} \in \mathbb{Q}, \text{ contradição pois } \frac{\theta}{2\pi} \in \mathbb{R} - \mathbb{Q}.$$

Proposição 2.1.1 Seja G um grupo e X um conjunto. Uma ação α de G em X define a seguinte relação de equivalência em X :

$$x \sim y \Longleftrightarrow \exists g \in G \text{ tal que } \alpha_g(x) = y.$$

Demonstração:

- Reflexiva: $\forall x \in X, \alpha_e(x) = x \Longrightarrow x \sim x.$
- Simétrica:

$x \sim y \Longrightarrow \exists g \in G, \alpha_g(x) = y$

$\Longrightarrow \alpha_{g^{-1}}(\alpha_g(x)) = \alpha_{g^{-1}}(y)$

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

$\Longrightarrow \alpha_e(x) = \alpha_{g^{-1}}(y)$

$\Longrightarrow x = \alpha_{g^{-1}}(y)$

$\Longrightarrow y \sim x.$

- Transitiva:

$x \sim y \Longrightarrow \exists g \in G, \alpha_g(x) = y \ (i)$

$y \sim z \Longrightarrow \exists h \in G, \alpha_h(y) = z \ (ii)$

De (i) e (ii) concluímos que:

$z = \alpha_h(y) = \alpha_h(\alpha_g(x)) = \alpha_{hg}(x) \Longrightarrow x \sim z.$

■

Da proposição acima concluímos que:

$[x] = \{y \in X; x \sim y\} = \{y \in X; \exists g \in G; \alpha_g(x) = y\} = \{\alpha_g(x) = y; g \in G\} = O_x.$

Proposição 2.1.2 Duas órbitas pela ação de um grupo ou são disjuntas ou são coincidentes.

Demonstração:

Suponha que $O_x \bigcap O_y \neq \emptyset$.

Então, existe $a \in O_x \bigcap O_y$.

$a \in O_x \Longrightarrow \exists g \in G$ tal que $\alpha_g(x) = a \Longrightarrow x \sim a.(i)$

$a \in O_y \Longrightarrow \exists g' \in G$ tal que $\alpha_{g'}(y) = a \Longrightarrow y \sim a.(ii)$

De (i) e (ii) concluímos que $x \sim y$.

Claro que $y \in O_y$ e como $x \sim y$, então $y \in O_x$. Logo, $O_y \subseteq O_x$.

De maneira análoga, provamos que $O_x \subseteq O_y$.

Portanto, $O_x = O_y$.

■

O resultado da proposição anterior nos leva à conclusão que a ação de um grupo sobre um conjunto provoca uma partição neste conjunto, composta pelas órbitas.

Definição 2.1.4 Um subconjunto T de X que corta cada órbita da ação de G em X em um único ponto é chamado um **conjunto de representantes de órbitas** ou de um **conjunto transversal**. (Tal conjunto sempre existe pelo Axioma da escolha.)

Definição 2.1.5 Considere uma ação α de um grupo G sobre um conjunto X. O **estabilizador** de um elemento $x \in X$ é definido como

$$\text{Stab}_x = \{g \in G; \alpha_g(x) = x\} \subseteq G.$$

Assim, dado $x \in X$, chamamos de estabilizador de x, o conjunto dos elementos de G que na ação de grupo fixam x.

Proposição 2.1.3 Stab_x é subgrupo de G.

Demonstração:

Sejam $g, h \in \text{Stab}_x$. Então $\alpha_g(x) = x$ e $\alpha_h(x) = x$.

Gostaríamos de provar que $\alpha_{gh^{-1}} \in \text{Stab}_x$.

Note que:

$\alpha_h(\alpha_{h^{-1}}(x)) = \alpha_e(x) = x = \alpha_h(x) \Longrightarrow \alpha_{h^{-1}}(x) = x$.

Vamos agora verificar o que realmente nos interessa.

$\alpha_{gh^{-1}}(x) = \alpha_g(\alpha_{h^{-1}}(x)) = \alpha_g(x) = x \Longrightarrow gh^{-1} \in \text{Stab}_x \Longrightarrow \text{Stab}_x \leq G$.

■

De forma semelhante, podemos falar do subgrupo estabilizador de um subconjunto $Y \subseteq X$.

Definição 2.1.6 Considere uma ação α de um grupo G sobre um conjunto X e $Y \subseteq X$. O subgrupo **estabilizador** de Y é definido como

$$\text{Stab}_Y = \{g \in G; \alpha_g(Y) \subseteq Y\}.$$

Definição 2.1.7 O subconjunto dos **pontos fixos** de um elemento $g \in G$ é o conjunto

$$\text{Fix}_g = \{x \in X; \alpha_g(x) = x\} \subseteq X.$$

Se $H \subseteq G$ é subgrupo de G, o conjunto dos pontos fixos pela ação de H é definido por

$$\text{Fix}_H = \{x \in X, \alpha_g(x) = x, \forall g \in H.\}$$

Definição 2.1.8 Uma ação α de G em X é dita ser

1. **Fiel**, quando: se $Fix_g = X$, então $g = e$.

$$\alpha_g(x) = x, \forall x \in X \Longrightarrow g = e.$$

2. **Livre**, quando: se $Fix_g \neq \emptyset$, então $g = e$.

$$\exists x \in X \text{ tal que } \alpha_g(x) = x \Longrightarrow g = e. \ (g \neq e \Longrightarrow \alpha_g(x) \neq x, \forall x \in X.)$$

3. **Transitiva**, quando: $O_x = X$, para todo $x \in X$.

$$\forall x, y \in X, \exists g \in G \text{ tal que } y = \alpha_g(x).$$

Exemplo 2.1.7 Seja $G = (\mathbb{Z}, +)$ e $X = (\mathbb{Z}_p, +)$.

Considere a ação $\alpha_n(\bar{k}) = \overline{k+n}$.

• α não é fiel e não é livre.

Seja $n = p \cdot x \neq 0, x \in \mathbb{Z}^*$.

$\alpha_n(\bar{k}) = \overline{k+n}$

$= \overline{k + p \cdot x}$

$= \bar{k}$.

Isso nos diz que $\text{Fix}_n = X$, para $n = p \cdot x \neq 0$. Portanto, α não é fiel.

Logo $\text{Fix}_n \neq \emptyset$ porém $n \neq 0$. Portanto, α não é livre.

• α é transitiva.

Seja $\bar{k} \in \mathbb{Z}_p$. Vamos mostrar que existem $\bar{l} \in \mathbb{Z}_p$ e $n \in \mathbb{Z}$ tal que $\alpha_n(\bar{l}) = \bar{k}$.

Considere $n = k - l \in \mathbb{Z}$.

$\alpha_n(\bar{l}) = \overline{l+n}$

$= \overline{l + k - l}$

$= \bar{k}$.

Exemplo 2.1.8 Seja $G = (\mathbb{R}, +)$ e $X = \mathbb{R}^2$.

Considere a ação $\alpha_\lambda(v) = v + \lambda \cdot v_0, v_0 \neq 0 \in \mathbb{R}^2$ fixo.

• α é livre.

Seja v ponto fixo por α_λ.

$\alpha_\lambda(v) = v \Longrightarrow v + \lambda \cdot v_0 = v$

$\Longrightarrow \lambda \cdot v_0 = 0$

$\Longrightarrow \lambda = 0.$ (pois $v_0 \neq 0$)

• α não é transitiva, pois as órbitas são retas paralelas.

Exemplo 2.1.9 Seja $G = \{z \in \mathbb{C}; |z| = 1\}$ multiplicativo e $X = \mathbb{C}$.

Primeiro note que G é grupo.

Sejam $z, w \in G$. Então $|z| = 1 = |w|$.

$|z \cdot w^{-1}| = |z| \cdot |w^{-1}|$

$= |z| \cdot |w|^{-1}$

$= 1 \cdot 1^{-1}$

$= 1.$

Considere a ação α por multiplicação.

$$\alpha_z : \mathbb{C} \longrightarrow \mathbb{C}$$

$$w \longmapsto zw$$

• α não é livre.

Sejam $w \in \mathbb{C}$ e $z \in G$.

$\alpha_z(w) = z \cdot w$.

$w = 0$ é ponto fixo, ou seja, $0 \in \text{Fix}_z, \forall z \in G$ mas $z \neq 1$.

• α é fiel.

Suponhamos $z \cdot w = w, \forall w \in \mathbb{C}$.

Em particular, para $w = 1$ temos:

$z \cdot 1 = 1 \Longrightarrow z = 1.$

Exemplo 2.1.10 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 $g, h \in G$.

Vamos mostrar que $Ad_g \in \mathrm{Aut}(G), \forall g \in G$.

• Ad_g é homomorfismo.

$$\begin{aligned} Ad_g(hk) &= ghkg^{-1} \\ &= ghg^{-1}gkg^{-1} \\ &= Ad_g(h)Ad_g(k). \end{aligned}$$

• Ad_g é injetiva.

$$\begin{aligned} Ad_g(h) = Ad_g(k) &\Longrightarrow ghg^{-1} = gkg^{-1} \\ &\Longrightarrow g^{-1}(ghg^{-1})g = g^{-1}(gkg^{-1})g \\ &\Longrightarrow h = k. \end{aligned}$$

• Ad_g é sobrejetiva.

$\forall h \in G, h = gg^{-1}hgg^{-1} = Ad_g(g^{-1}hg)$.

2.2 Ações de Grupos Finitos sobre Conjuntos Finitos

Nesta seção vamos considerar ações de um grupo finito G sobre um conjunto também finito X. Como uma ação de um grupo determina uma relação de equivalência em X, e como as órbitas determinam uma partição no conjunto X, é fácil ver que o conjunto das órbitas é igual ao conjunto quociente determinado por esta relação de equivalência. Por este motivo, vamos denotar o conjunto das órbitas por $\dfrac{X}{G}$. As cardinalidades de G, X

e $\frac{X}{G}$ serão denotadas, respectivamente, por $|G|, |X|$ e $\left|\frac{X}{G}\right|$. Para cara $i = 1, \cdots, \left|\frac{X}{G}\right|$, escolhemos um representante x_i de cada órbita, vamos denotar o número de elementos na órbita de x_i por $|O(x_i)|$. Note que, se $x \in X$ é um ponto fixo pela ação do grupo G, então $O_x = \{x\}$, ou seja, $|O(x)| = 1$.

Proposição 2.2.1 Considere uma ação do grupo finito G sobre o conjunto finito X. Considere também os elementos $x_i \in X$, $i = 1, \cdots, \left|\frac{X}{G}\right|$, que são os representantes de cada órbita. Então

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

Demonstração:

Pela Proposição 2.1.2 temos que as órbitas formam uma partição de X. Assim a contagem do segundo membro da igualdade está correta visto que nenhum elemento é contado duas vezes.

■

Observação 2.2.1 Se denotarmos por X^G o subconjunto dos pontos fixos pela ação de G, podemos decompor a soma da proposição anterior como:

$$|X| = \sum_{j=1}^{|X^G|} |O(x_j)| + \sum_{i=1}^{|\frac{X}{G}|-|X^G|} |O(x_i)| = |X^G| + \sum_{i=1}^{|\frac{X}{G}|-|X^G|} |O(x_i)|.$$

Análogo a equação das classses de conjugação.

Teorema 2.2.1 Seja uma ação α, do grupo finito G sobre um conjunto finito X. Considere um elemento $x \in X$, então

$$|O(x)| = \frac{|G|}{|\mathrm{Stab}_x|}.$$

Demonstração:

Seja $\dfrac{G}{\text{Stab}_x}$ o conjunto das laterais à esquerda de Stab_x em G.

Considere a seguinte função:

$$\begin{aligned}\phi : \frac{G}{\text{Stab}_x} &\longrightarrow O_x \\ g \cdot \text{Stab}_x &\longmapsto \alpha_g(x).\end{aligned}$$

• ϕ está bem definida.

$g \cdot \text{Stab}_x = h \cdot \text{Stab}_x \Longrightarrow g^{-1} \cdot h \in \text{Stab}_x$ (Proposição 1.3.1)

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

$$\Longrightarrow \alpha_{g^{-1}}(\alpha_h(x)) = x$$

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

$$\Longrightarrow \phi(g \cdot \text{Stab}_x) = \phi(h \cdot \text{Stab}_x).$$

• ϕ é sobrejetora.

$\forall y \in O_x, \exists g \in G$ tal que $y = \alpha_g(x) = \phi(g \cdot \text{Stab}_x)$.

• ϕ é injetora.

Sejam $g, h \in G$ tais que

$\phi(g \cdot \text{Stab}_x) = \phi(h \cdot \text{Stab}_x) \Longrightarrow \alpha_g(x) = \alpha_h(x)$

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

$$\Longrightarrow g^{-1}h \in \text{Stab}_x$$

$$\Longrightarrow g \cdot \text{Stab}_x = h \cdot \text{Stab}_x.$$

Portanto, a função ϕ é bijetiva, o que nos leva à conclusão que a órbita de x e o conjunto quociente $\dfrac{G}{\text{Stab}_x}$ possuem o mesmo número de elementos.

Então, pelo Teorema de Lagrange,

$$\left|\frac{G}{\text{Stab}_x}\right| = \frac{|G|}{|\text{Stab}_x|}.$$

■

Corolário 2.2.1 Dada uma ação de um grupo finito G sobre um conjunto finito X, o número de elementos da órbita $x \in X$ é um divisor de $|G|$.

Demonstração:

Este resultado vem direto do teorema anterior.

■

Corolário 2.2.2 Considere a ação de um grupo finito G sobre um conjunto finito X. Sejam $x, y \in X$ dois elementos na mesma órbita, então $|\text{Stab}_x| = |\text{Stab}_y|$.

Demonstração:

Note que como $x, y \in X$ estão na mesma órbita, temos pela Proposição 2.1.2, que $O_x = O_y$.

Então, pelo Teorema 2.2.1 temos que:

$|G| = |O_x| \cdot |\text{Stab}_x| = |O_y| \cdot |\text{Stab}_y| = |O_x| \cdot |\text{Stab}_y| \Longrightarrow |\text{Stab}_x| = |\text{Stab}_y|$.

■

Corolário 2.2.3 Dada uma ação de um grupo G sobre um conjunto finito X, com $|G| = p^n$, para p primo. Temos que

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

Demonstração:

Note que:

$|O(x_i)| \neq 1$ e $|O(x_i)| \mid |G| \Longrightarrow |O(x_i)| \mid p^n$

$$\Longrightarrow |O(x_i)| = p^k, 1 \leq k \leq n.$$

Dessa forma, pela Proposição 2.2.1,

$$|X| = |X^G| + \sum_{i=1}^{|\frac{X}{G}|-|X^G|} |O(x_i)| = |X^G| + \sum_i p^{k_i} \Longrightarrow p \mid |X| - |X^G|.$$

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

■

Como consequência deste resultado, podemos demonstrar de uma forma diferente o Pequeno Teorema de Fermat.

Teorema 2.2.2 Seja $a \geq 1$ um número inteiro e p um número primo, então

$$a^p \equiv a \,(\mathrm{mod} p).$$

Demonstração:

Considere o conjunto $A = \{1, 2, \cdots, a\}$ e defina uma ação α do grupo aditivo $\mathbb{Z}_p$ sobre $X = A^p = \{(x_1, \cdots, x_p); x_i \in A\}$ por permutações cíclicas:

$$\alpha_{\bar{0}}(x_1, \cdots, x_p) = (x_1, \cdots, x_p)$$

$$\alpha_{\bar{1}}(x_1, \cdots, x_p) = (x_p, x_1, \cdots, x_{p-1})$$

$$\alpha_{\bar{2}}(x_1, \cdots, x_p) = (x_{p-1}, x_p, x_1, \cdots, x_{p-2})$$

$$\vdots$$

$$\alpha_{\overline{p-1}}(x_1, \cdots, x_p) = (x_2, x_3, \cdots, x_p, x_1).$$

Uma p-upla $(x_1, \cdots, x_p)$ 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 $|X| = a^p$.

Pelo Corolário 2.2.3 temos que $|X| \equiv |X^G| \,(\mathrm{mod} p)$, ou seja, $a^p \equiv a (\mathrm{mod} p)$. ■

Capítulo 3

O Teorema de Burnside e Aplicações

3.1 O Teorema de Burnside

Neste capítulo vamos enunciar um resultado importante na teoria de ações de grupos com consequências interessantes para a combinatória, o Teorema de Burnside. Este resultado relaciona o número de órbitas em uma ação com o número de elementos de Fix_g, para cada $g \in G$.

Apesar do teorema a seguir ser associado ao nome de William Burnside, ele foi primeiramente provado por Georg Frobenius em 1887. Burnside publicou um livro muito influente em teoria dos grupos e sua primeira edição foi o primeiro texto em inglês deste assunto. Nesta primeira edição, Burnside coloca o teorema e o atribui a Frobenius, mas essa atribuição não passou para a segunda edição, de muito maior penetração. É provável que isso tenha originado toda essa confusão histórica.

Teorema 3.1.1 Considere uma ação de um grupo finito G sobre um conjunto finito X. Então

$$\left|\frac{X}{G}\right| \cdot |G| = \sum_{g \in G} |\mathrm{Fix}_g|.$$

Demonstração: A demonstração deste fato utiliza-se de uma técnica comum em combinatória, que é a contagem dupla. Para isto vamos fixar algumas notações:

- $\left|\frac{X}{G}\right| = m$;
- $|G| = n$;
- vamos denotar o número de elementos na k-ésima órbita por p_k (de onde vem que, $|X| = p_1 + p_2 + \cdots + p_m = p$;)
- $g_1, g_2, \cdots, g_n$: os elementos do grupo;
- $x_1, x_2, \cdots, x_p$: os elementos do conjunto X.

Façamos uma matriz $F = (f(i,j))_{i,j}$ com n linhas e p colunas na qual

$$f(i,j) = \begin{cases} 1 & \text{, se} \quad x_j \in \text{Fix}_{g_i}, \text{ ou seja, } \alpha_{g_i}(x_j) = x_j \\ 0 & \text{, se} \quad x_j \notin \text{Fix}_{g_i}, \text{ ou seja, } \alpha_{g_i}(x_j) \neq x_j \end{cases}$$

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

$$\sum_{i=1}^{n}\sum_{j=1}^{p} f(i,j) = \sum_{i=1}^{n} |\text{Fix}_{g_i}|.$$

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

$$\sum_{i=1}^{n}\sum_{j=1}^{p} f(i,j) = \sum_{j=1}^{p} |\text{Stab}_{x_j}|$$

$$\sum_{j=1}^{p} |\text{Stab}_{x_j}| = \sum_{j=1}^{p} \frac{|G|}{|O_{x_j}|}$$

Para avaliarmos a soma anterior vamos ordenar os elementos de X de acordo com as órbitas geradas, na forma:

$$X = \{x_1, x_2, \cdots, x_{p_1}, x_{p_1+1}, \cdots, x_{p_1+p_2}, x_{p_1+p_2+1}, \cdots, x_{p_1+p_2+p_3}, \cdots, x_{p_1+\cdots+p_{m-1}+1}, \cdots, x_{p_1+\cdots+p_m}\},$$

onde $O_{x_1} = \cdots = O_{x_{p_1}}, O_{x_{p_1+1}} = \cdots = O_{x_{p_1+p_2}}$, e assim por diante.

Assim, a soma anterior pode ser escrita como

$$\sum_{j=1}^{p} \frac{|G|}{|O_{x_j}|} = \sum_{j=1}^{p_1} \frac{|G|}{|O_{x_j}|} + \sum_{j=1}^{p_2} \frac{|G|}{|O_{x_{p_1+j}}|} + \cdots + \sum_{j=1}^{p_m} \frac{|G|}{|O_{x_{p_1+\cdots+p_m+j}}|}.$$

Cada um dos denominadores em suas respectivas somas possui o mesmo valor, assim

$$|O_{x_1}| = |O_{x_2}| = \cdots = |O_{x_{p_1}}| = p_1$$

$$|O_{x_{p_1+1}}| = \cdots = |O_{x_{p_1+p_2}}| = p_2$$

.

.

.

$$|O_{x_{p_1+\cdots+p_{m-1}+1}}| = \cdots = |O_{x_{p_1+\cdots+p_m}}| = p_m$$

Portanto, podemos reescrever a soma anterior como

$$\sum_{j=1}^{p} \frac{|G|}{|O_{x_j}|} = \sum_{j=1}^{p_1} \frac{|G|}{p_1} + \sum_{j=1}^{p_2} \frac{|G|}{p_2} + \cdots + \sum_{j=1}^{p_m} \frac{|G|}{p_m}$$

$$= \sum_{k=1}^{m} \left(\sum_{j=1}^{p_k} \frac{|G|}{p_k} \right)$$

$$= \sum_{k=1}^{m} p_k \cdot \frac{|G|}{p_k}$$

$$= \sum_{k=1}^{m} |G|$$

$$= m \cdot |G|$$

$$= \left|\frac{X}{G}\right| \cdot |G|.$$

Portanto,

$$\left|\frac{X}{G}\right| \cdot |G| = \sum_{g \in G} |\mathrm{Fix}_g|.$$

■

Exemplo 3.1.1 Obter o número de permutações circulares de n elementos; isto é, determinar o número de maneiras de arranjarmos n objetos distintos em torno de um círculo.

Neste problema, o conjunto X é formado pelas $n!$ permutações dos n objetos distintos. Para definirmos o grupo G de simetrias, basta notar que uma disposição em círculo é considerada a mesma que outra, se uma puder ser obtida da outra por alguma rotação. Portanto o grupo G é composto pela identidade e por $(n-1)$ rotações. Portanto G é o grupo cíclico $\langle a \rangle$, $a = R_{\frac{2\pi}{n}}$. A identidade e fixa todos os $n!$ elementos de X, mas para qualquer outro elemento $g \in G$ é tal que $\mathrm{Fix}(g) = 0$. Isto porque os n elementos são todos distintos e qualquer rotação não-trivial leva uma configuração de X em alguma outra diferente. Pelo Teorema de Burnside temos então que o número de permutações circulares de n elementos é dado por

$$\frac{1}{n}\left(n! + \overbrace{0 + \cdots + 0}^{n-1 \text{ zeros}}\right) = (n-1)!$$

Exemplo 3.1.2 Considere um disco dividido em n setores circulares todos congruentes (como uma pizza, ou um guarda-chuva), suponha ainda que existam disponíveis q cores distintas para pintarmos os diversos setores circulares. De quantas maneiras não equivalentes podemos efetuar essa pintura?

Seja r o número que estamos procurando.

Note que nesse 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 do 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 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. Como já vimos na Proposição 1.2.4 para cada divisor d de n, existe um subgrupo H de ordem d gerado pelo elemento $a^{\frac{n}{d}}$, que corresponde neste caso a uma rotação de ângulo $d \cdot \frac{2\pi}{n}$. Então, neste subgrupo existem exatamente d elementos, a saber $a^{\frac{n}{d}}, a^{\frac{2n}{d}}, \cdots, a^{\frac{dn}{n}} = e$. Destes, apenas $\varphi(d)$ elementos possuem ordem exatamente igual a d, isto é, $x^d = e$ e $x^k \neq e$ se $0 < k < d$, e estes são todos os elementos de ordem d no grupo. Para cada elemento de ordem d no grupo, existem $q^{\frac{n}{d}}$ configurações inequivalentes de cores. Assim, pelo teorema de Burnside, temos

$$\left|\frac{X}{G}\right| \cdot |G| = \sum_{g \in G} |\mathrm{Fix}_g| \Longrightarrow r \cdot |G| = \sum_{d|n} \varphi(d) q^{\frac{n}{d}}$$

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

No caso especial de $q = 1$, isto é, uma única cor, r também é igual a 1. Assim temos a fórmula

$$r = \frac{1}{n} \sum_{d|n} \varphi(d) q^{\frac{n}{d}} \Longrightarrow 1 = \frac{1}{n} \sum_{d|n} \varphi(d) \cdot 1$$

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

Referências Bibliográficas

[1] BATISTA, Eliezer - *Ações e Representações de Grupos e Teoria de Números*. IV Bienal da Sociedade Brasileira de Matemática. Maringá - setembro de 2008.

[2] DOMINGUES, Hygino H. e Iezzi, Gelson – *Álgebra Moderna*. São Paulo, Atual, 2003.

[3] GONÇALVES, Adilson – *Introdução à Álgebra*. Rio de Janeiro, IMPA, 2008.

[4] JANESCH, Oscar Ricardo - *Álgebra II*. Florianópolis: UFSC/EAD/CED/CFM, 2008.

[5] SANTOS, José Plínio O. e Eduardo Bovo - *O Teorema de Burnside e Aplicações*. II Bienal da Sociedade Brasileira de Matemática. Universidade Federal da Bahia - Instituto de Matemática - 25 a 29 de outubro de 2004.