

O Teorema de Burnside e Aplicações

José Plínio O. Santos

e

Eduardo Bovo

Universidade Estadual de Campinas

1 - Permutações

Introduzimos, nesta seção, o conceito fundamental de permutação que servirá de base para todo nosso estudo.

Com a finalidade de sermos concisos, denotamos, para todo $n \in \mathbb{N}$, o conjunto finito $\{1, 2, \dots, n\}$ pelo símbolo $[n]$.

Definição 1.1 *Dado um conjunto não-vazio X , uma bijeção $\sigma : X \rightarrow X$ é denominada uma permutação do conjunto X .*

Exemplo 1.1 *Considere um baralho de 52 cartas em certa ordem $(b_1, b_2, \dots, b_{52})$. Qualquer embaralhamento de $X = (b_1, \dots, b_{52})$ é perfeitamente descrito por uma reindexação conveniente de seus índices $(b_{j_1}, \dots, b_{j_{52}})$, com $\{j_1, \dots, j_{52}\} = [52] = \{1, 2, 3, \dots, 52\}$. Qualquer embaralhamento das cartas possui uma ordem, geralmente diferente da anterior, se bem embaralhado, digamos $(b_{10}, b_{12}, b_1, b_6, \dots, b_{34})$ mas ainda é composto das mesmas cartas $\{b_1, \dots, b_{52}\}$.*

Assim podemos pensar no embaralhamento como uma permutação do conjunto $X = \{b_1, \dots, b_{52}\}$ das 52 cartas do baralho.

Denotamos o conjunto $S(X)$ como o conjunto de todas as permutações do conjunto X . Se X é finito com $\#X = n$, isto é, $X = \{x_1, \dots, x_n\}$, então para formar qualquer permutação destes n elementos, temos

$$\boxed{n \quad n-1 \quad \dots \quad 2 \quad 1}$$

n possibilidades de preenchimento para o primeiro quadrado da fila, $n-1$ possibilidades para o segundo, ..., 2 possibilidades para o $(n-1)$ -ésimo e 1 para o enésimo (último).

Assim, pelo princípio multiplicativo temos $n!$ permutações em $S(X)$, isto é, $\#S(X) = n!$.

Na maioria dos casos, estaremos mais interessados em estudar permutações de $X = [n]$ e denotamos $S_n = S([n])$.

Se $\sigma \in S_n$ e $j \in [n]$, a notação $\sigma(j)$ denota o valor da função bijetiva σ no ponto j . Desta forma podemos denotar a permutação σ pelo seguinte diagrama

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

exibindo visualmente o domínio e o contradomínio da bijeção σ considerada.

Exemplo 1.2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 2 & 4 & 6 & 3 & 8 & 7 \end{pmatrix} \in S_8$. *Observe que após aplicada esta permutação, os números 1 e 4 permanecem fixos.*

A segunda representação, muito importante para nós, é a representação por ciclos. Antes de introduzi-la,

é conveniente olharmos o exemplo acima por diagrama de setas

$$\begin{array}{l}
 1 \rightarrow 1 \\
 2 \rightarrow 5 \\
 3 \rightarrow 2 \\
 4 \rightarrow 4 \\
 5 \rightarrow 6 \\
 6 \rightarrow 3 \\
 7 \rightarrow 8 \\
 8 \rightarrow 7
 \end{array}
 \quad \text{que é equivalente a} \quad
 \begin{array}{c}
 1 \rightarrow 1 \\
 2 \rightarrow 5 \rightarrow 6 \rightarrow 3 \rightarrow 2 \\
 4 \rightarrow 4 \\
 7 \rightarrow 8 \rightarrow 7
 \end{array}
 \quad \text{e que iremos denotar por } (1)(2563)(4)(78)$$

De maneira geral, se $\sigma \in S_n$, para todo $j \in [n]$ temos que deve existir $l_j \in [n]$ tal que

$$\sigma^{l_j}(j) = \underbrace{(\sigma \circ (\sigma \circ (\dots \circ (\sigma(j)) \dots)))}_{l_j \text{ aplicações}} = j$$

Se não existisse tal l_j , ou $l_j \geq n + 1$, então após a n -ésima iteração teríamos o valor resultante fora do conjunto $[n]$, um absurdo pois σ é uma bijeção definida em $[n]$. Assim, temos um ciclo de σ determinado por $(j, \sigma(j), \sigma^2(j), \dots, \sigma^{l_j-1}(j))$ de comprimento l_j . Tomamos um outro elemento k não contido no ciclo $(j, \sigma(j), \sigma^2(j), \dots, \sigma^{l_j-1}(j))$ e temos que deve existir l_k tal que $(k, \sigma(k), \sigma^2(k), \dots, \sigma^{l_k-1}(k))$ seja um ciclo de comprimento l_k . Aplicamos este procedimento sucessivamente aos elementos que ainda não tenham aparecido nos ciclos anteriormente construídos até que todos os membros de $[n]$ sejam utilizados. Desta forma obtemos uma representação da permutação σ por meio de ciclos disjuntos. Denominamos um ciclo de comprimento k simplesmente de k -ciclo; se $k = 1$ dizemos que o ciclo é um *ponto fixo* e se $k = 2$ dizemos que o ciclo é uma *transposição*.

Exemplo 1.3 A permutação $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix}$ pode ser representada na notação de ciclos disjuntos por $(12)(3)(465)$. O ciclo (12) é uma transposição e o ciclo (3) é um ponto fixo da permutação.

Observe que se permutarmos ciclicamente os elementos de um ciclo qualquer, ou se reordenarmos os ciclos isto não mudará a permutação representada. A menos destas possíveis variações, a representação por ciclos disjuntos é única.

É costume omitir da composição de permutações o símbolo \circ , e simplesmente justapor os operandos. Assim $\sigma_1 \circ \sigma_2$ é denotada por $\sigma_1\sigma_2$, onde entendemos que primeiro aplicamos σ_2 e depois σ_1 .

2 - Grupos de Permutações

A seguir demonstramos alguns lemas elementares que versam sobre $S(X)$, e provamos que se trata na verdade de um grupo com a operação de composição de funções.

2.1 $S(X)$ é um grupo de permutações

Consideramos nos resultados abaixo que X é um conjunto não-vazio qualquer, mas podemos tê-lo em mente como sendo o conjunto $[n]$.

Lema 2.1 O conjunto $S(X)$ é fechado por composição de permutações, isto é,

$$\sigma_1, \sigma_2 \in S(X) \Rightarrow \sigma_1\sigma_2 \in S(X)$$

Dem. Dadas $\sigma_1, \sigma_2 \in S(X)$, mostramos que $\sigma_1\sigma_2$ é também uma bijeção de X em X , e portanto pertence a $S(X)$.

$\sigma_1\sigma_2$ é injetiva. De fato, se tomarmos $x, y \in X, x \neq y$, como σ_2 é injetiva segue que $\sigma_2(x) \neq \sigma_2(y)$. Assim, como σ_1 é injetiva também, segue que $\sigma_1\sigma_2(x) \neq \sigma_1\sigma_2(y)$ e portanto $\sigma_1\sigma_2$ é também injetiva.

Mostramos agora que $\sigma_1\sigma_2$ é sobrejetiva e para isso seja $z \in X$. Como σ_1 e σ_2 são sobrejetivas, $\exists y \in X$ com $\sigma_1(y) = z, \exists x \in X$ com $\sigma_2(x) = y$. Isto é, existe $x \in X$ tal que $\sigma_1(\sigma_2(x)) = z$ e portanto $\sigma_1\sigma_2$ é sobrejetiva.

Assim concluímos que $\sigma_1\sigma_2 \in S(X)$, e o conjunto é fechado por composição de permutações. ■

Lema 2.2 A função $e : X \rightarrow X$ definida por $e(x) = x$ para todo $x \in X$ é uma bijeção e funciona como a identidade de $S(X)$, isto é

$$\forall \sigma \in S(X), \text{ temos } \sigma e = e\sigma = \sigma$$

Além disso, dada qualquer permutação $\sigma \in S(X)$, existe uma permutação inversa $\sigma^{-1} \in S(X)$ tal que

$$\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$$

Dem. É imediato verificar que a função $e(x)$ identidade é uma permutação e que funciona como elemento neutro de $S(X)$. Como toda função bijetiva possui inversa, e esta inversa também é bijetiva, segue a existência dos inversos em $S(X)$. ■

Sabemos que a composição de funções é associativa o que nos permite concluir diretamente, pela definição de operação que demos em $S(X)$, que

Lema 2.3 Dadas as permutações σ_1, σ_2 e σ_3 em $S(X)$, temos

$$\sigma_1(\sigma_2\sigma_3) = (\sigma_1\sigma_2)\sigma_3$$

Esses três lemas acima mostram que $S(X)$ é um grupo com a operação de composição de funções. Na próxima seção, relembremos as definições dos axiomas de grupo e demonstramos alguns resultados fundamentais.

2.2 Axiomas de Grupo

Uma operação binária $*$ em um conjunto G é entendida como uma função $* : G \times G \rightarrow G$ que associa a cada par de elementos de G , um elemento de G . Desta forma, se uma tal operação binária $*$ puder ser definida em G , teremos que obrigatoriamente G é fechado por ela. Assim o conceito de o conjunto G ser fechado pela operação $*$ está implícito no conceito de operação binária em G .

Definição 2.1 Um grupo é um par ordenado $(G, *)$, onde G é um conjunto e $*$ é uma operação binária em G satisfazendo:

(G1) *Identidade:* Existe $e \in G$ tal que $\forall x \in G \Rightarrow x * e = e * x = x$

O elemento e é chamado de identidade de G .

(G2) *Inversos:* $\forall x \in G$, existe $x^{-1} \in G$ tal que $x * x^{-1} = x^{-1} * x = e$

Dado x , o elemento x^{-1} é chamado de inverso de x .

(G3) *Associatividade:* $\forall x, y, z \in G$, temos $x * (y * z) = (x * y) * z$

A associatividade nos permite abandonar os parênteses na composição de operações entre elementos de G .

Temos então o seguinte teorema, que é consequência dos lemas da seção anterior:

Teorema 2.1 *Se X é um conjunto não-vazio, $(S(X), \circ)$ é um grupo chamado de grupo de permutações de X , e denotado simplesmente por $S(X)$.*

Exemplo 2.1 *Como exemplos básicos, temos que os seguintes pares são grupos:*

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

Exemplo 2.2 *Todos os conjuntos do exemplo acima são fechados por multiplicação, tendo 1 como identidade. No entanto, apenas os elementos não-nulos dos conjuntos \mathbb{Q} , \mathbb{R} e \mathbb{C} possuem inversos. Assim temos mais três exemplos de grupos,*

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

Exemplo 2.3 *Seja p um primo, $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ a classe dos resíduos módulo p . Então $(\mathbb{Z}_p, +_p)$ e $(\mathbb{Z}_p^*, \times_p)$ são grupos com as operações de soma e multiplicação módulo p , respectivamente.*

Exemplo 2.4 *O grupo simétrico S_n , formado pelas permutações dos símbolos $\{1, 2, \dots, n\}$.*

2.3 Subgrupos e o Teorema de Lagrange

A seguir apresentamos a definição de subgrupo de um grupo G . Essencialmente, entendemos por um subgrupo H de G , um subconjunto H de G tal que H se comporte como um grupo pela operação herdada da definida em G .

Como $H \subseteq G$, consideramos como operação binária $*$ em H a restrição de $*$ ao domínio $H \times H$. Pelo fato de a associatividade ser válida para todos os elementos de G , em particular é válida para todos os elementos de H , $H \subseteq G$.

Definição 2.2 *Dado um grupo G e $H \subseteq G$, H é um subgrupo de G se*

(SG1) *H é fechado sob a operação $*$, isto é, $\forall x, y \in H \Rightarrow x * y \in H$*

(SG2) *H contém o elemento identidade e de G .*

(SG3) *H contém inversos, isto é, $\forall x \in H$ temos $x^{-1} \in H$*

As condições da definição acima são equivalentes a uma mais concisa, que é dada na proposição abaixo

Proposição 2.1 *Se G é um grupo e $H \neq \emptyset$ é um subconjunto de G , então*

$$H \text{ é subgrupo de } G \iff \forall g, h \in H \text{ temos } g * h^{-1} \in H.$$

A partir de agora, omitimos, como de costume o símbolo $*$ da operação do grupo G e simplesmente justapomos os elementos sendo operados, como na notação multiplicativa, onde xy significa $x * y$.

Vamos definir alguns conceitos que nos serão úteis na demonstração do Teorema de Lagrange.

Definição 2.3 *Seja G um grupo e H um subgrupo de G . Para cada $g \in G$, a classe lateral gH é definida como sendo o conjunto*

$$gH = \{gh : h \in H\}$$

Lema 2.4 *Se H é um subgrupo de G , e $g_1, g_2 \in G$, então temos*

$$g_1H = g_2H \iff g_2^{-1}g_1 \in H$$

Dem. Supomos primeiramente que $g_1H = g_2H$. Como a identidade $e \in H$, temos

$$g_1e = g_1 \in (g_1H) \Rightarrow g_1 \in (g_2H)$$

Assim, existe $h \in H$ tal que $g_1 = g_2h$, o que equivale a $g_2^{-1}g_1 = h$, e portanto $g_2^{-1}g_1 \in H$.

Agora supomos que $g_2^{-1}g_1 \in H$. Disto tiramos que $g_2^{-1}g_1 = h \in H$, ou seja, que $g_1 = g_2h$.

Vamos mostrar que $g_1H \subseteq g_2H$. Seja $x \in g_1H$, isto é, $x = g_1h_1$ para algum $h_1 \in H$. Temos

$$x = g_1h_1 = (g_2h)h_1 = g_2(hh_1) = g_2h_2 \text{ com } h_2 \in H, \text{ pois } H \text{ é subgrupo de } G$$

Desta forma temos que $x \in g_2H$ e portanto $g_1H \subseteq g_2H$.

Reescrevemos a equação $g_1 = g_2h$ utilizando o inverso de h em H , obtendo $g_2 = g_1h^{-1}$ (lembre-se que H é subgrupo de G , e portanto $h^{-1} \in H$). Assim podemos aplicar o raciocínio anterior para mostrar que $g_2H \subseteq g_1H$. Portanto temos a igualdade $g_1H = g_2H$. ■

Lema 2.5 *Se H é um subgrupo de G então quaisquer classes laterais de H ou são idênticas, ou são disjuntas. Em símbolos:*

$$\forall g_1, g_2 \in H, \text{ temos exclusivamente que } g_1H = g_2H \text{ ou } g_1H \cap g_2H = \emptyset.$$

Dem. Suponha que $g_1H \cap g_2H \neq \emptyset$ e seja $x \in g_1H \cap g_2H$. Então existem $h_1, h_2 \in H$ tais que $x = g_1h_1 = g_2h_2$, o que significa que $g_2^{-1}g_1 = h_2h_1^{-1}$. Mas $h_2h_1^{-1} \in H$, pois H é subgrupo de G , o que implica que $g_2^{-1}g_1 \in H$ e assim pelo lema 2.4 temos $g_1H = g_2H$. ■

Definição 2.4 *Em vista do lema anterior, definimos como índice de H em G o número de diferentes classes laterais de H em G , e denotamos por $|G : H|$. Em símbolos,*

$$|G : H| = \#\{gH : g \in G\}$$

Agora temos as ferramentas necessárias para a demonstração do importante Teorema de Lagrange, acerca da ordem de subgrupos de G .

Teorema 2.2 *Se H é um subgrupo de um grupo finito G , então*

$$|G : H| \times |H| = |G|$$

Dem. Como H é subgrupo de G , a identidade e está em H . Portanto, para cada $g \in G$, $g = ge \in gH$, e assim cada elemento de G está em alguma classe lateral de H em G .

Mostramos agora que cada classe lateral de H em G possui ordem igual à ordem de H . Como $H \subseteq G$ e H é subgrupo, temos que $|H| < \infty$. Seja $H = \{h_1, \dots, h_m\}$ com os h_j todos distintos (isto é, $|H| = m$). Afirmamos que para todo $g \in G$, gh_j são todos distintos com j percorrendo os valores $1, \dots, m$. De fato, se tivéssemos $gh_j = gh_k$ com $j \neq k$, poderíamos cancelar g à esquerda e obter $h_j = h_k$, um absurdo. Assim concluímos que para qualquer classe lateral gH , $|gH| = |H|$.

Portanto, utilizando o lema 2.5 temos que as diferentes classes laterais de H em G particionam G em $|G : H|$ conjuntos de cardinalidade $|H|$ e concluímos nossa demonstração. ■

Assim obtemos o importante

Teorema 2.3 (Teorema de Lagrange) *Se H é subgrupo de um grupo finito G , então a ordem de H divide a ordem de G .*

Dem. Como G e H são grupos finitos, os números $|G : H|$, $|H|$ e $|G|$ são inteiros positivos. Portanto, pela definição de divisibilidade e pela equação do teorema anterior, temos que $|G|$ é divisível por $|H|$. ■

3 - Grupos de Simetria

A seguir definimos o que se entenderá por simetria de figuras planas ou espaciais.

Definição 3.1 *Entendemos por uma figura um conjunto F de pontos de \mathbb{R}^2 ou \mathbb{R}^3 .*

Definição 3.2 *Dada uma figura F , uma simetria de F é uma aplicação $f : F \rightarrow F$ com as seguintes propriedades*

- (i) f é uma isometria
- (ii) f é sobrejetiva

Pela definição dada, uma simetria é uma aplicação que leva a figura nela mesma e que preserva distâncias.

Exemplo 3.1 *Um triângulo equilátero possui 6 simetrias: 1 delas é a identidade, 2 são rotações horárias centradas em seu centro de gravidade de ângulos $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$ e 3 delas são reflexões através de suas medianas.*

Exemplo 3.2 *Um quadrado desenhado no plano possui 8 simetrias: 1 delas é a identidade, 3 são rotações horárias centradas em seu centro de gravidade de ângulos $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$, 2 são reflexões através de suas mediatrizes e 2 são reflexões através de suas diagonais.*

Podemos utilizar números para marcar as figuras e assim relacionar os grupos de simetrias a grupos de permutações. Fazemos isso comumente associando números aos vértices de figuras, mas de uma maneira geral podemos também associar números a lados, diagonais, ou outros elementos das figuras.

Na *Figura 1* abaixo, estão listadas as 6 simetrias do triângulo e as 8 do quadrado, bem como as permutações correspondentes de seus vértices numerados. Também denominamos as simetrias do quadrado para referência futura.

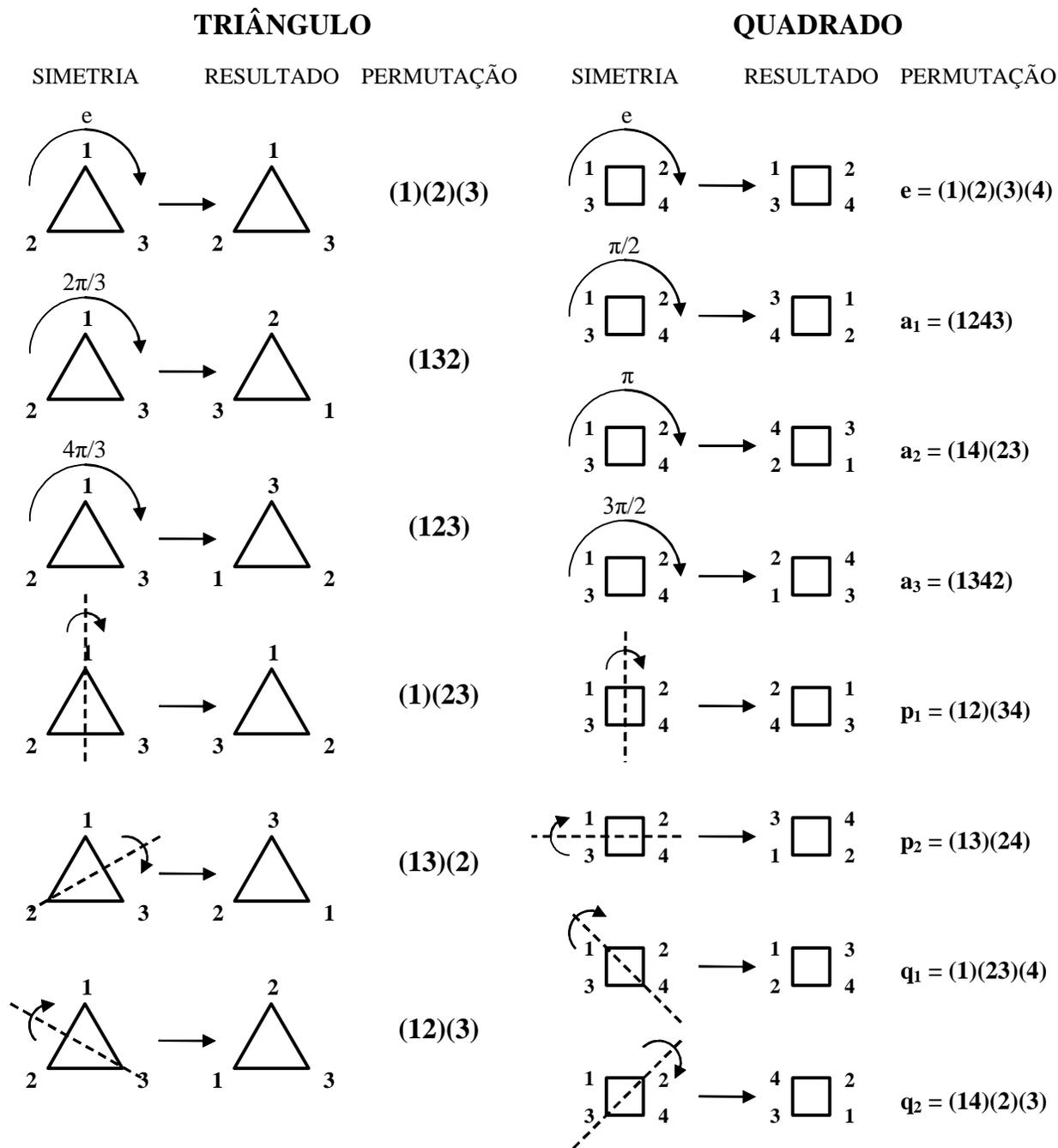


Figura 1: Simetrias do triângulo e do quadrado

Teorema 3.1 *Seja F uma figura. Então o conjunto de todas as simetrias de F , com a operação de composição de funções, forma um grupo.*

Dem. Seja G o conjunto de todas as simetrias de F . Verificamos a seguir que G munido da operação de

composição de funções satisfaz os axiomas de grupo.

A identidade $I_F : F \rightarrow F$ é obviamente uma simetria, e portanto G possui um elemento identidade.

Denotando por $d(x, y)$ a distância entre os pontos x e y , suponha que $f, g \in G$. Inicialmente, temos que $f \circ g$ é uma isometria, pois

$$\begin{aligned} d(f(g(x)), f(g(y))) &= d(g(x), g(y)), \text{ pois } f \text{ é uma isometria} \\ &= d(x, y), \text{ pois } g \text{ é uma isometria} \end{aligned}$$

Como $(f \circ g)(F) = f(g(F)) = f(F) = F$, e $f \circ g$ é uma isometria, segue então que $f \circ g$ é uma simetria e portanto está em G .

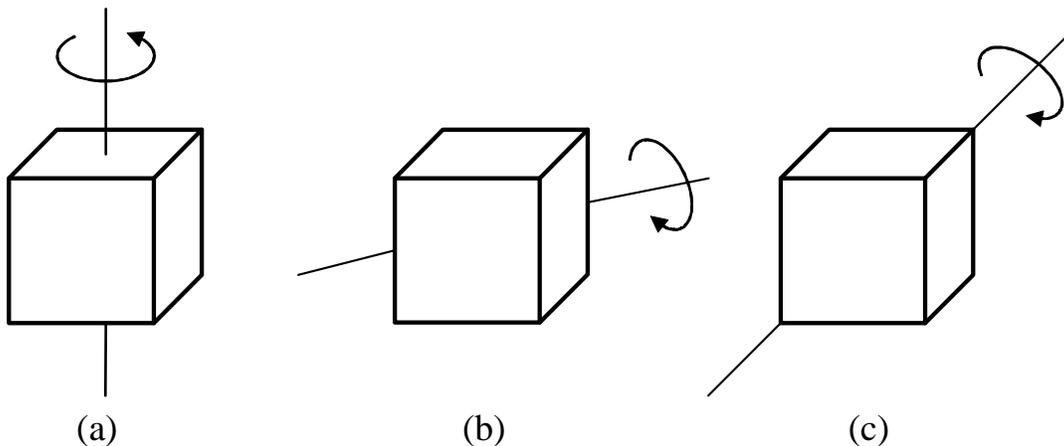
Toda simetria (isometria) f é injetora, e portanto possui uma inversa f^{-1} . Dados $z, w \in F$, como f é sobrejetiva também,

$$d(f^{-1}(z), f^{-1}(w)) = d(f(f^{-1}(z)), f(f^{-1}(w))) = d(z, w)$$

Assim f^{-1} é uma simetria e portanto pertence a G .

A associatividade da composição de simetrias segue diretamente da associatividade de composição de funções. ■

Exemplo 3.3 Temos 3 diferentes tipos de eixos de rotação para um cubo, indicados na figura abaixo:



(a) Rotação em torno de um eixo que passa pelos centros de faces opostas,

(b) Rotação em torno de um eixo que passa pelos pontos médios de arestas opostas

(c) Rotação em torno de um eixo que passa por vértices opostos

Assim, as 24 simetrias rotacionais de um cubo são divididas em:

- 1) A identidade e ;
- 2) 3 rotações de um ângulo de $\frac{\pi}{2}$ pelo eixo indicado em (a);
- 3) 3 rotações de um ângulo de π pelo eixo indicado em (a);
- 4) 3 rotações de um ângulo de $\frac{3\pi}{2}$ pelo eixo indicado em (a);
- 5) 6 rotações de um ângulo de π pelo eixo indicado em (b);
- 6) 4 rotações de um ângulo de $\frac{2\pi}{3}$ pelo eixo indicado em (c) e
- 7) 4 rotações de um ângulo de $\frac{4\pi}{3}$ pelo eixo indicado em (c).

4 - Ordens de Permutações

4.1 Tipo cíclico e partições de inteiros

Pelas observações que fizemos anteriormente, uma permutação $\sigma \in S_n$ possui a seguinte representação por $t = t(\sigma)$ ciclos disjuntos,

$$\sigma = \left(j_1^{(1)} j_2^{(1)} \dots j_{l_1}^{(1)} \right) \left(j_1^{(2)} j_2^{(2)} \dots j_{l_2}^{(2)} \right) \dots \left(j_1^{(t)} j_2^{(t)} \dots j_{l_t}^{(t)} \right)$$

com $t \in \mathbb{N}$, $[n]$ particionado pela seguinte reunião disjunta

$$[n] = \bigcup_{i=1}^t \left\{ j_1^{(i)}, \dots, j_{l_i}^{(i)} \right\}$$

Sabemos que esta representação é única a menos de permutações dos ciclos e de permutações cíclicas dos elementos internos de cada ciclo.

Sendo G um grupo finito, a ordem de um elemento g é definida como o menor inteiro positivo k tal que $g^k = e$. Isto implica que para qualquer múltiplo $m = rk$ de k , também temos a equação $g^m = e$.

Portanto, uma permutação que seja um k -ciclo possui ordem k e este k -ciclo elevado a qualquer múltiplo de k também resulta na identidade. Como os ciclos da representação de σ são disjuntos, para todo $k \in \mathbb{N}$

$$\sigma^k = \left(j_1^{(1)} j_2^{(1)} \dots j_{l_1}^{(1)} \right)^k \left(j_1^{(2)} j_2^{(2)} \dots j_{l_2}^{(2)} \right)^k \dots \left(j_1^{(t)} j_2^{(t)} \dots j_{l_t}^{(t)} \right)^k$$

Assim para encontrarmos a ordem de σ , precisamos que todos os ciclos de sua representação, quando elevados a k , atinjam a identidade, o que ocorrerá quando k for um múltiplo comum de l_1, \dots, l_t . Mas pela definição de ordem de um elemento, queremos o menor k que seja um múltiplo comum. Temos então que a ordem de σ é igual a $mmc[l_1, \dots, l_t]$.

Definimos agora um termo polinomial que de certa forma reflete a estrutura cíclica de uma permutação $\sigma \in S_n$.

Definição 4.1 Definimos o tipo cíclico de $\sigma \in S_n$ como sendo o monômio $TC(\sigma)$ dado por

$$TC(\sigma) = \prod_{i=1}^t x_{l_i} \quad (1)$$

Exemplo 4.1 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix} = (12)(3)(465)$ tem tipo cíclico $TC(\sigma) = x_2 \cdot x_1 \cdot x_3 = x_1 x_2 x_3$. Repare que a comutatividade do produto em $TC(\sigma)$ expressa a propriedade de que a ordem dos ciclos na representação de σ é irrelevante.

Exemplo 4.2 $\sigma = (1)(276)(3)(4589) \in S_9$ tem tipo cíclico $TC(\sigma) = x_1 \cdot x_3 \cdot x_1 \cdot x_4 = x_1^2 x_3 x_4$.

É costume omitir da representação de σ os ciclos unitários, porém é fundamental para a determinação do tipo cíclico de uma permutação, que os ciclos unitários não sejam "esquecidos". Desta forma, ou devemos logo listar os ciclos unitários, ou ter em mente o grupo subjacente ao qual a permutação analisada pertence.

Observe que na representação (1) podemos ter ciclos disjuntos de mesmo comprimento. Assim os números l_1, \dots, l_t podem não ser todos distintos. Suponha, sem perda de generalidade, que no conjunto $\{l_1, \dots, l_t\}$ tenhamos apenas $s \leq t$ números distintos, e os redenominamos na ordem crescente $l_1 < l_2 < \dots < l_s$. Conseqüentemente, podemos afirmar que existem k_1 ciclos de comprimento l_1 , k_2 ciclos de comprimento l_2 , ..., k_s ciclos de comprimento l_s ; onde $k_j, l_j \in [n]$ para $j = 1, 2, \dots, s$. Desta forma, podemos concluir que para toda $\sigma \in S_n$ fixada, temos a unicidade dos números $s(\sigma)$, $k_j(\sigma)$ e $l_j(\sigma)$, onde $j = 1, 2, \dots, s$.

Assim o tipo cíclico de σ toma a seguinte forma, mais intuitiva e explícita,

$$TC(\sigma) = x_{l_1}^{k_1} x_{l_2}^{k_2} \dots x_{l_s}^{k_s}$$

onde k_j é o número de ciclos de comprimento l_j para $j = 1, \dots, s$. Aqui o total de ciclos da representação é $k_1 + k_2 + \dots + k_s$.

Como $\sigma \in S_n$ é uma permutação dos números de $[n]$, devemos ter n símbolos distribuídos entre todos os ciclos de sua representação. Isto implica que $k_1 l_1 + k_2 l_2 + \dots + k_s l_s = n$, e pela ordenação $1 \leq l_1 < l_2 < \dots < l_s \leq n$, e definições de k_j , temos então uma partição do inteiro $n = k_1 l_1 + \dots + k_s l_s$.

Reciprocamente, se temos uma partição do inteiro n dada por

$$\begin{aligned} n &= k_1 l_1 + k_2 l_2 + \dots + k_s l_s \\ k_j, l_j &\in [n], l_1 < \dots < l_s \end{aligned}$$

onde temos k_j partes iguais a l_j para $j = 1, \dots, s$, então é possível encontrar uma permutação $\sigma \in S_n$ com tipo cíclico $TC(\sigma) = x_{l_1}^{k_1} x_{l_2}^{k_2} \dots x_{l_s}^{k_s}$. Na verdade existem muitas permutações em S_n com este tipo cíclico dado, e o teorema a seguir nos diz quantas são. A demonstração abaixo é devida a Cauchy.

Teorema 4.1 *Seja uma partição de n , dada por $n = k_1 l_1 + k_2 l_2 + \dots + k_s l_s$, com $k_j, l_j \in [n]$ e $l_1 < l_2 < \dots < l_s$. Então existem*

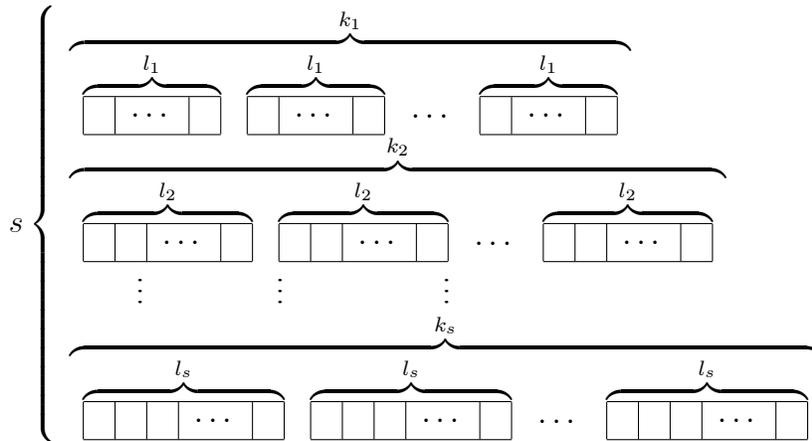
$$\frac{n!}{l_1^{k_1} k_1! l_2^{k_2} k_2! \dots l_s^{k_s} k_s!}$$

permutações $\sigma \in S_n$ com tipo cíclico $x_{l_1}^{k_1} x_{l_2}^{k_2} \dots x_{l_s}^{k_s}$

Dem. Seja h o número de permutações $\sigma \in S_n$ satisfazendo $TC(\sigma) = x_{l_1}^{k_1} x_{l_2}^{k_2} \dots x_{l_s}^{k_s}$, isto é, contendo k_j ciclos de comprimento l_j para $j = 1, \dots, s$.

Vamos considerar as permutações com o tipo cíclico desejado, quebradas em seus ciclos componentes. Primeiro listamos os k_1 ciclos de comprimento l_1 e representamos cada ciclo por l_1 quadrados, depois listamos os k_2 ciclos de comprimento l_2 , e representamos cada ciclo por l_2 quadrados e assim

sucessivamente, até finalmente listarmos os k_s ciclos de comprimento l_s e seus quadrados.



Sabemos que o total de quadrados do diagrama acima é n , pois trata-se de uma permutação em S_n . Então procedemos preenchendo arbitrariamente os n símbolos dentro dos n quadrados, isto é, vamos inserir as $n!$ permutações dos números $[n]$ dentro dos n quadrados. Assim obtemos uma aplicação do conjunto das $n!$ permutações no conjunto das permutações com o tipo cíclico determinado acima.

Claramente, ao preencher os quadrados, podemos ter mais de uma permutação determinando o mesmo resultado. Por exemplo, se $n = 8$, $TC(\sigma) = x_1x_2^2x_3$, ambos os preenchimentos abaixo resultam na mesma permutação (4) (23) (15) (687):

4	2	3	5	1	7	6	8
4	1	5	3	2	8	7	6

Seja P uma das h permutações de S_n com o tipo cíclico desejado. Como P possui k_1 ciclos de comprimento l_1 , a fim de produzirmos P no preenchimento, suas k_1 l_1 -uplas de elementos devem ser colocados nos k_1 blocos de l_1 quadrados cada. Cada l_1 -upla pode ser colocada em qualquer ordem entre os k_1 blocos, assim temos $k_1!$ possibilidades para isso. Cada um dos k_1 blocos, pode ser rotacionado ciclicamente e isto pode ser feito de l_1 maneiras por bloco, pois seu comprimento é l_1 . Assim temos $l_1^{k_1}$ possibilidades para as rotações cíclicas dos elementos dos blocos e portanto no total temos $k_1!l_1^{k_1}$ maneiras de obtermos os k_1 ciclos de comprimento l_1 de P . O mesmo raciocínio pode ser aplicado aos demais ciclos de P , isto é, temos $k_j!l_j^{k_j}$ maneiras de obter os k_j ciclos de comprimento l_j para $j = 1, \dots, s$. Portanto, temos um total de

$$k_1!l_1^{k_1} k_2!l_2^{k_2} \dots k_s!l_s^{k_s}$$

permutações que quando colocadas nos quadrados geram os ciclos de P . Portanto, se plugarmos todas as $n!$ permutações nos quadrados do diagrama, cada permutação com esse tipo cíclico é gerada exatamente o número de vezes indicado acima. Assim concluímos que

$$h \cdot k_1!l_1^{k_1} k_2!l_2^{k_2} \dots k_s!l_s^{k_s} = n!$$

de onde segue o resultado. ■

Corolário 4.1 *Existe uma correspondência biunívoca entre os tipos cíclicos dos elementos de S_n e as partições do inteiro n . Portanto, existem $p(n)$ diferentes tipos cíclicos para as permutações de S_n , onde $p(n)$ é o número de partições do inteiro n .*

Abaixo colocamos, a título de curiosidade, uma tabela contendo alguns valores de $p(n)$.

n	$p(n)$	n	$p(n)$
1	1	10	42
2	2	20	627
3	3	30	5604
4	5	40	37338
5	7	50	204226
6	11	60	966467
7	15	70	4087968
8	22	80	15796476
9	30	90	56634173

Para encontrarmos a maior ordem que um elemento de S_n pode ter, por exemplo, uma maneira é procurar nas partições de $n = x_1 + \dots + x_s$, aquela que tem o maior valor para $mmc[x_1, \dots, x_s]$.

4.2 Índice de ciclos

Definição 4.2 Se G é um grupo de permutações, o índice de ciclos de G , denotado $Z(G)$, é definido como sendo o polinômio

$$Z(G) = \frac{1}{|G|} \sum_{\sigma \in G} TC(\sigma)$$

Observe que a soma dos coeficientes do polinômio deve ser igual a 1, isto porque temos $|G|$ termos na soma, divididos pelo fator $|G|$.

Exemplo 4.3 Em S_1 temos apenas a permutação identidade que possui tipo cíclico x_1 . Isto nos dá trivialmente

$$Z(S_1) = x_1$$

Em S_2 temos as permutações (1)(2) e (12), que possuem tipos cíclicos iguais a x_1^2 e x_2 , respectivamente. Portanto,

$$Z(S_2) = \frac{1}{2} (x_1^2 + x_2)$$

Para S_3 , temos a permutação (1)(2)(3) com tipo cíclico igual a x_1^3 , as permutações (12)(3), (13)(2), (23)(1) com tipo cíclico x_1x_2 e as permutações (123), (132) com tipo cíclico x_3 . Assim, obtemos para o índice de ciclos

$$Z(S_3) = \frac{1}{6} (x_1^3 + 3x_1x_2 + 2x_3)$$

Abaixo fornecemos a fórmula fechada para os coeficientes do índice de ciclos de S_n .

Teorema 4.2 Temos a seguinte expressão geral para o índice de ciclos do grupo simétrico S_n

$$Z(S_n) = \sum_{k_1l_1 + \dots + k_sl_s = n} \frac{1}{l_1^{k_1} k_1! l_2^{k_2} k_2! \dots l_s^{k_s} k_s!} x_{l_1}^{k_1} x_{l_2}^{k_2} \dots x_{l_s}^{k_s}$$

onde a soma é efetuada sobre todas as partições do inteiro n .

Dem. Este resultado sai diretamente do teorema 4.1 e da definição de índice de ciclos. Basta somar nos $p(n)$ diferentes tipos cíclicos possíveis para as permutações de S_n . ■

5 - Ações de Grupos

Considerando um tabuleiro 2×2 temos um total de $2^4 = 16$ colorações utilizando 2 cores (preta e branca):

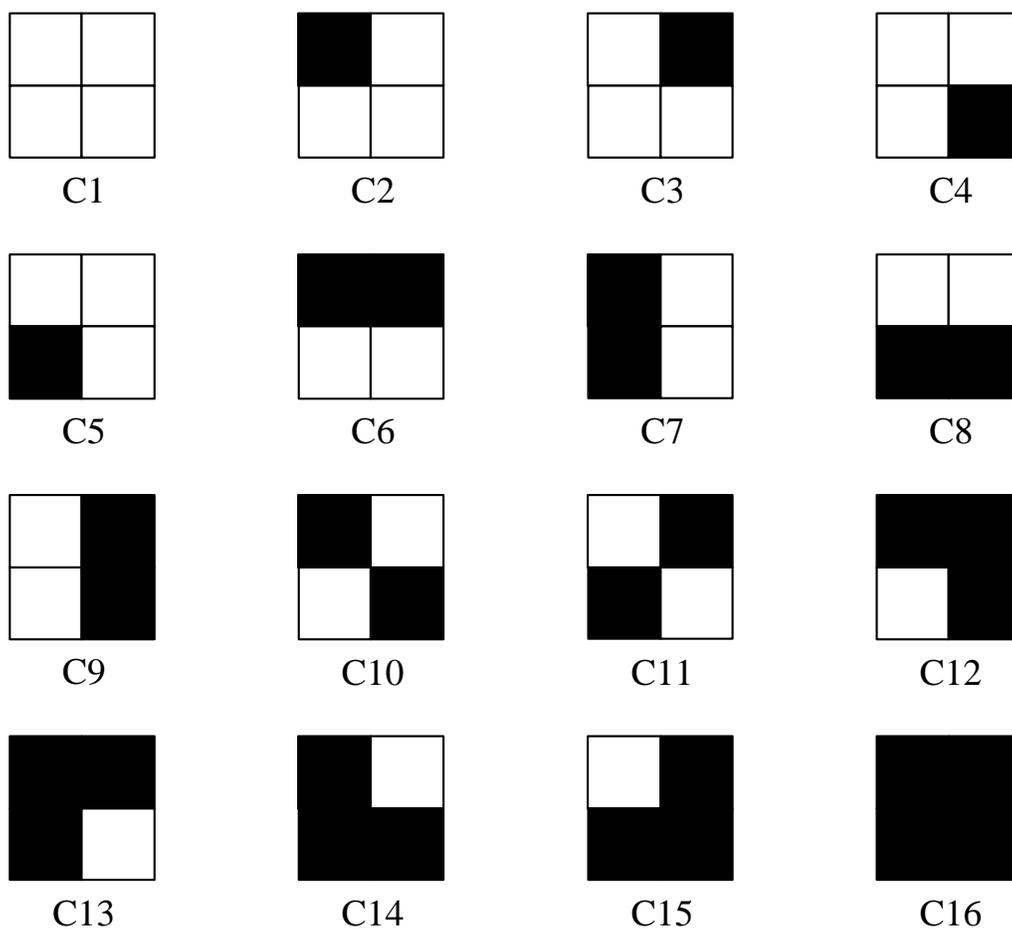
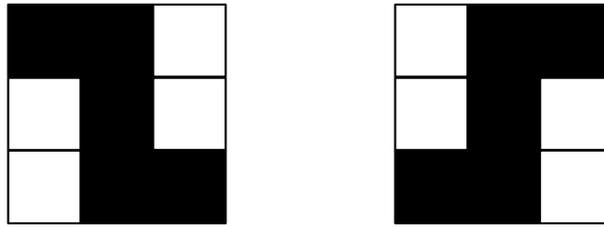


Figura 2: 16 colorações de um tabuleiro de xadrez 2×2 , nas cores preto e branco. Do total listado acima, podemos inferir os seguintes conjuntos de padrões equivalentes:

$$\begin{aligned}
 &\{C1\} \\
 &\{C2, C3, C4, C5\} \\
 &\{C6, C7, C8, C9\} \\
 &\{C10, C11\} \\
 &\{C12, C13, C14, C15\} \\
 &\{C16\}
 \end{aligned}$$

Assim, por exemplo $C6$ e $C8$ estão no mesmo conjunto, pois um pode ser obtido do outro através de uma rotação de um ângulo π . Num tabuleiro 2×2 por ser mais simples, não faz diferença se considerarmos ou não as reflexões; isto é, basta considerarmos as rotações para diferenciar os padrões.

Se tivéssemos por exemplo, considerando tabuleiros 3×3 , os diagramas abaixo não poderiam ser obtidos um do outro apenas por rotações; necessitaríamos também das reflexões.



De qualquer forma, nas nossas observações sobre padrões de coloração equivalentes são as simetrias do quadrado que estão sendo consideradas na diferenciação. O que estão implícitos em toda esta discussão são conceitos sobre a interação entre um grupo (como o de simetrias de um quadrado, por exemplo) e os membros de algum outro conjunto (como as 16 colorações do tabuleiro 2×2).

6 - Colorações

A seguir definiremos rigorosamente o que se entende por colorações de objetos, sejam tabuleiros, contas, vértices, faces, etc...

Primeiro, como um exemplo mais concreto, consideramos novamente o tabuleiro de xadrez 2×2 .

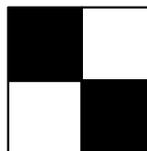
α_1	α_2
α_3	α_4

Então, se estamos colorindo de branco e preto, podemos considerar uma *coloração* f como uma aplicação do conjunto dos quadrados $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ no conjunto das cores $\{preto, branco\}$, isto é

$$f : \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \rightarrow \{preto, branco\}$$

As 16 colorações diferentes correspondem então às 16 aplicações diferentes com os domínios e contradomínios definidos acima.

A título de exemplo, a coloração correspondente a C_{10} denotada por f_{10} é a coloração



determinada por

$$\begin{aligned} f_{10}(\alpha_1) &= f_{10}(\alpha_4) = preto \\ f_{10}(\alpha_2) &= f_{10}(\alpha_3) = branco \end{aligned}$$

Como utilizaremos este exemplo do tabuleiro 2×2 de maneira recorrente, é conveniente denotar por f_j a coloração correspondente ao diagrama C_j da *Figura 2*.

Procedemos agora para o conceito geral. Sejam C e D dois conjuntos não-vazios (em geral são diferentes também), e $X = \mathcal{F}(D, C)$, o conjunto de todas as funções com domínio D e contradomínio C .

Então dizemos que qualquer função $f \in X$ é uma *coloração* de D . Este é o caso mais abstrato.

Estaremos mais interessados nos casos em que C e D são finitos, e se $\#D = n$, $\#C = m$, temos pelo princípio multiplicativo um total de m^n colorações de D diferentes, isto é $\#X = m^n$

Exemplo 6.1 *Se D é um conjunto de provas de alunos, podemos ter C como conjunto de notas (números)*

Exemplo 6.2 *Se D é um conjunto de contas ou pedrinhas, podemos ter C como conjunto de cores.*

Exemplo 6.3 *Se D é um conjunto de quadrados de um tabuleiro 2×2 , podemos ter C como o conjunto das cores $\{\text{preto, branco}\}$*

7 - Os Axiomas de Ação de Grupos

Queremos descrever a situação geral onde temos uma interação entre um grupo G e um conjunto X não vazio.

Definição 7.1 *Seja G um grupo e X um conjunto não-vazio. Dizemos que G age em X se, para todo $g \in G$ e para todo $x \in X$, existir um elemento $g \cdot x \in X$ satisfazendo as seguintes propriedades:*

(A1) *Para todo $x \in X$, $e_G \cdot x = x$, onde e_G é a identidade de G .*

(A2) *Para todo $g, h \in G$, $x \in X$, temos*

$$g \cdot (h \cdot x) = (gh) \cdot x$$

O axioma A1 significa que a ação do elemento identidade de G é sempre trivial, isto é, fixa todo elemento de X .

O segundo relaciona a ação do grupo à sua operação.

Sempre que um grupo age em um conjunto, dizemos que temos uma *ação de grupo*, e os axiomas A1 e A2 são chamados de *axiomas de ação de grupos*.

Ao contrário do que fazemos com as operações de grupos, jamais devemos omitir o símbolo \cdot que representa a ação de grupos. Isto porque estamos combinando elementos de conjuntos que geralmente são diferentes (G e X).

Exemplo 7.1 *Tome G como o grupo das simetrias do quadrado, e seja X o conjunto das colorações de um tabuleiro 2×2 nas cores preta e branca.*

Exemplo 7.2 *Tome G como o grupo das simetrias rotacionais de um cubo, e X o conjunto de colorações das faces do cubo usando vermelho, preto e verde.*

Exemplo 7.3 Seja G qualquer grupo e X o conjunto dos elementos de G . Definimos uma ação de grupo por

$$\forall g, x \in G, \text{ temos } g \cdot x = gxg^{-1}$$

Esta ação é chamada de conjugação e o elemento do grupo gxg^{-1} é chamado de conjugado de x .

Lema 7.1 Seja G um grupo que age no conjunto X . Então para todo $g \in G, x, y \in X$, temos

$$g \cdot x = y \iff g^{-1} \cdot y = x$$

Dem. Sejam $g \in G, x, y \in X$ e suponha que $g \cdot x = y$. Então

$$\begin{aligned} g^{-1} \cdot y &= g^{-1} \cdot (g \cdot x) \\ &= (g^{-1} \cdot g) \cdot x \\ &= e \cdot x \\ &= x \end{aligned}$$

A recíproca é obtida aplicando o que acabamos de demonstrar, trocando x por y e g por g^{-1} . ■

Retornamos agora ao exemplo de colorações de tabuleiros 2×2 , e vamos avaliar como uma permutação age sobre uma coloração. Considere novamente o tabuleiro:

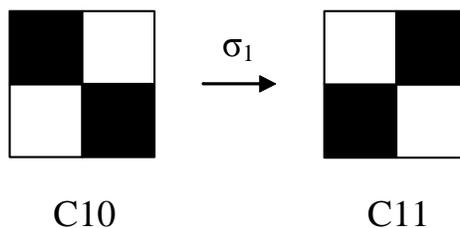
$\alpha 1$	$\alpha 2$
$\alpha 3$	$\alpha 4$

É fácil ver que para cada simetria do quadrado aplicada no tabuleiro, existe uma permutação correspondente σ do conjunto dos quadrados $\{\alpha 1, \alpha 2, \alpha 3, \alpha 4\}$. Assim, se considerarmos a rotação a_1 do tabuleiro por um ângulo de $\frac{\pi}{2}$, temos

$\alpha 1$	$\alpha 2$	$\xrightarrow{a_1}$	$\alpha 3$	$\alpha 1$
$\alpha 3$	$\alpha 4$		$\alpha 4$	$\alpha 2$

que corresponde à permutação $\sigma_1 = (\alpha 1 \alpha 2 \alpha 4 \alpha 3)$. Vamos tomar então nosso grupo G como sendo o das permutações dos símbolos $\{\alpha 1, \alpha 2, \alpha 3, \alpha 4\}$ e considerar sua ação no conjunto de colorações $X = \mathcal{F}(\{\alpha 1, \alpha 2, \alpha 3, \alpha 4\}, \{\text{preto}, \text{branco}\})$.

Por exemplo, a permutação σ_1 agindo na coloração f_{10} resulta na coloração f_{11}



e portanto

$$\sigma_1 \cdot f_{10} = f_{11}$$

Desta forma notamos que $\sigma_1 \cdot f_{10}$ designa a cor *branca* para o quadrado α_1 , porque esta é a cor que f_{10} designa para o quadrado α_3 que acabou de ser movido para o quadrado α_1 por σ_1 . Como $\sigma_1^{-1}(\alpha_1) = \alpha_3$, podemos concluir que este processo é equacionado por

$$\sigma_1 \cdot f_{10}(\alpha_1) = f_{10}(\sigma_1^{-1}(\alpha_1))$$

Esta fórmula se aplica em geral, e abaixo desenvolvemos mais rigorosamente este conceito.

Na notação da seção anterior, temos o conjunto de colorações $X = \mathcal{F}(D, C)$ e tomamos G como algum grupo de permutações de símbolos de D . Isto é, G é algum subgrupo de $S(D)$, o grupo de todas as permutações do conjunto D .

Definimos uma ação de G no conjunto das colorações X , por

$$\forall \sigma \in G, \forall f \in X \Rightarrow \sigma \cdot f = f \circ \sigma^{-1} \quad (2)$$

e verificamos que realmente isto define uma ação de grupo.

Teorema 7.1 *A fórmula (2) acima define uma ação de grupo.*

Dem. Seja e a identidade de G . Então e é a aplicação identidade $e : D \rightarrow D$ e para toda $f \in X$,

$$e \cdot f = f \circ e^{-1} = f \circ e = f$$

e assim (A1) se verifica.

Sejam $\sigma_1, \sigma_2 \in G$ e $f \in X$. Então, pela nossa definição,

$$\begin{aligned} \sigma_2 \cdot (\sigma_1 \cdot f) &= \sigma_2 \cdot (f \circ \sigma_1^{-1}) \\ &= (f \circ \sigma_1^{-1}) \circ \sigma_2^{-1} \\ &= f \circ (\sigma_1^{-1} \circ \sigma_2^{-1}) \\ &= f \circ (\sigma_2 \circ \sigma_1)^{-1} \\ &= (\sigma_2 \circ \sigma_1) \cdot f \end{aligned}$$

e portanto (A2) também é válido concluindo a demonstração. ■

8 - Órbitas

8.1 Relações de equivalência por ação de grupos

Definimos o conceito de ação de grupos, de forma a estabelecer o que entendemos por diferentes padrões de coloração. No caso do tabuleiro 2×2 , o grupo relevante é o grupo de simetrias do quadrado. Consideramos que duas colorações do tabuleiro são essencialmente as mesmas se a ação de uma das simetrias leva uma coloração na outra. Agora tornamos mais precisos estes conceitos de equivalência.

Definição 8.1 *Seja G um grupo agindo em X . Definimos uma relação \sim_G em X da seguinte forma:*

$$\begin{aligned} \text{Para todo } x, y &\in X, \\ x \sim_G y &\iff \exists g \in G \text{ tal que } g \cdot x = y \end{aligned}$$

Lema 8.1 A relação \sim_G no conjunto X é uma relação de equivalência.

Dem. Mostramos que \sim_G é reflexiva, simétrica e transitiva.

Sejam $x, y, z \in X$. Como $e \in G$ é sua identidade, por (A1) segue que $e \cdot x = x$ e portanto temos que $x \sim_G x$ e \sim_G é reflexiva.

Se tivermos que $x \sim_G y$, então existe $g \in G$ com $g \cdot x = y$. Como G é grupo, existe o inverso g^{-1} e pelo lema 7.1 temos que $g^{-1} \cdot y = x$ e portanto $y \sim_G x$. Assim \sim_G é simétrica.

Suponhamos agora que $x \sim_G y$ e $y \sim_G z$. Então existem $g, h \in G$ tais que $g \cdot x = y$ e $h \cdot y = z$. Como G é grupo, temos que $hg \in G$ e usando (A2) obtemos

$$(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z$$

o que implica em $x \sim_G z$. Isto mostra que \sim_G é transitiva, e encerramos a demonstração do lema. ■

No exemplo envolvendo as colorações do tabuleiro de xadrez, temos que as classes de equivalência são aqueles conjuntos que possuem colorações todas com o mesmo padrão.

Em geral, as classes de equivalência da relação \sim_G são chamadas de *órbitas* da ação do grupo. A órbita à qual o elemento x pertence é denotada por O_x . Assim

$$O_x = O_y \iff x \sim_G y$$

e como $x \sim_G y \iff y = g \cdot x$ para algum $g \in G$, segue que

$$O_x = \{g \cdot x : g \in G\}$$

No exemplo 7.3, as classes de equivalência são chamadas de classes de conjugação do grupo em questão. Pode-se mostrar, por exemplo, que duas permutações em S_n são conjugadas se, e somente se, possuírem o mesmo tipo cíclico. Assim, se $G = S_n$, existe um total de $p(n)$ classes de conjugação.

Como as órbitas são classes de equivalência, elas particionam o conjunto X em conjuntos disjuntos.

Assim nossa pergunta de quantos padrões diferentes temos ao colorir os tabuleiros é na verdade a de quantas órbitas diferentes existem.

8.2 Inventários de colorações

Vamos desenvolver um método algébrico para descrever colorações, utilizando funções geradoras. Aqui a situação ideal é obter uma função geradora que determine o número de padrões de cada tipo para a situação em questão.

Já vimos que temos um total de 16 maneiras de colorir um tabuleiro de xadrez 2×2 , sem considerarmos as relações de equivalência de padrões; isto é, não estamos contando as órbitas. Observe que na expansão

$$(p + b)^4 = (p + b)(p + b)(p + b)(p + b) = p^4 + 4p^3b + 6p^2b^2 + 4pb^3 + b^4$$

obtemos cada coeficiente escolhendo de cada parênteses o símbolo p ou b , e isso corresponde às 16 colorações diferentes do tabuleiro 2×2 nas cores preta e branca. Mais ainda, cada termo na expansão lista o número de colorações de acordo com quantas cores brancas e pretas estão sendo utilizadas. Deste modo, o termo p^3b tem como coeficiente 4, que é o número de colorações ($C12$, $C13$, $C14$ e $C15$) contendo 3 cores pretas e 1 branca. O termo p^4 tem coeficiente 1, indicando que temos apenas 1 coloração ($C16$) contendo 4 cores pretas.

No entanto, esta expressão algébrica não nos diz nada acerca de quantos padrões diferentes existem por equivalência; isto é, não nos exhibe informações sobre as órbitas das colorações. Mais à frente,

enunciaremos um teorema que nos permitirá obter uma função geradora que contenha tal informação; e as definições a seguir serão necessárias para a aplicação daquele resultado.

Os símbolos algébricos p e b correspondem às cores *preta* e *branca*, respectivamente, ambas elementos do conjunto C . No caso geral, entendemos por uma *função peso* no conjunto C , uma função ω que associa a cada $c \in C$, um símbolo algébrico ou um número denotado por $\omega(c)$, denominado peso de c .

O *enumerador de estoque* é definido pela soma $\sum_{c \in C} \omega(c)$, isto é, representa de maneira algébrica todos os valores que os elementos do conjunto D podem receber através das colorações de D em C . Por exemplo, sejam $C = \{\text{vermelho claro}, \text{vermelho escuro}, \text{azul}\}$, $\omega(\text{vermelho claro}) = r$, $\omega(\text{vermelho escuro}) = R$ e $\omega(\text{azul}) = a$. Então o enumerador de estoque (de tintas, ou cores, no caso) é $r + R + a$; isto é, interpretando a soma como função geradora, significa que temos exatamente 1 cor vermelho clara, 1 cor vermelho escura e 1 cor azul. Assim, nosso enumerador de estoque é na verdade uma generalização do conceito de função geradora. Se colocarmos $r = R$, temos como enumerador de estoque $2R + a$, o que significa que temos 2 cores vermelhas e 1 cor azul para designar aos elementos de D . Vale ressaltar que os dois tipos de tinta vermelha ainda são dois tipos distintos, mesmo que tenhamos designado o mesmo peso para as duas. Se os dois tipos de tinta vermelha fossem indistinguíveis, o enumerador de estoque seria dado por $R + a$, ao invés de $2R + a$.

Para cada coloração $f \in X$, definimos seu *peso* $W(f)$ pela equação

$$W(f) = \prod_{d \in D} \omega(f(d))$$

Finalmente, dado um subconjunto S de X , o *inventário* de S é definido por

$$\sum_{f \in S} W(f)$$

Exemplo 8.1 *Suponha que desejamos saber todas as maneiras de pintarmos 3 bolas distintas nas cores sólidas vermelho claro, vermelho escuro e azul. Seja D o conjunto das 3 bolas, e seja C o conjunto dos 3 tipos de tinta mencionados. Designamos os pesos para as cores como anteriormente, obtendo o enumerador de estoque $r + R + a$ que nos fornece o número de maneiras que 1 bola pode ser pintada nas cores de C . Assim, como as bolas são distintas, $(r + R + a)^3$ nos dá o total de maneiras diferentes de pintarmos 3 bolas com as cores escolhidas. Em outras palavras, $(r + R + a)^3$ é o inventário do conjunto de todas as colorações de D em C .*

Retornamos ao exemplo do tabuleiro 2×2 para tornar claras as definições dadas acima.

Relembramos que $D = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, o conjunto dos 4 quadrados do tabuleiro, $C = \{\text{preto}, \text{branco}\}$, o conjunto das cores e $X = \mathcal{F}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}, \{\text{preto}, \text{branco}\})$ é o conjunto das colorações de D em C .

A função peso no nosso exemplo é dada por

$$\begin{aligned} \omega(\text{preto}) &= p \\ \omega(\text{branco}) &= b \end{aligned}$$

A coloração f_{10} é tal que

$$\begin{aligned} f_{10}(\alpha_1) &= \text{preto} \\ f_{10}(\alpha_2) &= \text{branco} \\ f_{10}(\alpha_3) &= \text{branco} \\ f_{10}(\alpha_4) &= \text{preto} \end{aligned}$$

e portanto

$$\begin{aligned}
 W(f_{10}) &= \prod_{d \in D} \omega(f_{10}(d)) = \omega(f_{10}(\alpha_1)) \omega(f_{10}(\alpha_2)) \omega(f_{10}(\alpha_3)) \omega(f_{10}(\alpha_4)) \\
 &= \omega(\text{preto}) \omega(\text{branco}) \omega(\text{branco}) \omega(\text{preto}) \\
 &= pbbp \\
 &= p^2b^2
 \end{aligned}$$

O inventário de todas as 16 colorações (isto é $S = X$), como visto anteriormente, é dado por

$$\sum_{f \in X} W(f) = p^4 + 4p^3b + 6p^2b^2 + 4pb^3 + b^4 = (p + b)^4$$

O problema de maior interesse para nosso estudo é o de determinar o inventário das colorações que contém exatamente 1 coloração de cada padrão (órbita). No caso dos tabuleiros ele seria dado por

$$p^4 + p^3b + 2p^2b^2 + pb^3 + b^4$$

conforme pode ser visto na *Figura 2* da página 14.

Este inventário é chamado de *inventário padrão*, e o teorema que determina sua função geradora é o celebrado *Teorema Enumerador de Pólya*.

9 - Estabilizadores

Na seção 7, através do axioma (A1), determinamos que a identidade e de um grupo G agindo em X , fixasse todos os elementos de X . No entanto, podemos ter, além da identidade, outros elementos de G fixando elementos de X .

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

Em símbolos, o estabilizador de x é definido por

$$S_x = \{g \in G : g \cdot x = x\}$$

A seguir mostramos que para qualquer $x \in X$, o estabilizador S_x é um subgrupo de G .

Lema 9.1 *Seja G um grupo agindo em X . Então, para todo $x \in X$, temos que S_x é subgrupo de G .*

Dem. Verificamos as condições de subgrupo para S_x . Primeiro suponha que $g, h \in S_x$. Então $g \cdot x = x$ e $h \cdot x = x$, e pelo axioma (A2) temos que

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

e assim $gh \in S_x$, o que mostra que S_x é fechado.

Por (A1), $e \cdot x = x$ e assim S_x contém a identidade de G .

Novamente, se $g \in S_x$, temos que $g \cdot x = x$ e pelo lema 7.1 temos que $g^{-1} \cdot x = x$ o que mostra que g^{-1} também está em S_x . Assim S_x é um subgrupo de G . ■

Abaixo colocamos um quadro com os estabilizadores e as órbitas das colorações de um tabuleiro de xadrez 2×2 :

Elemento de X	Estabilizador	Órbita
$C1$	$\{e, a_1, a_2, a_3, p_1, p_2, q_1, q_2\}$	$\{C1\}$
$C2$	$\{e, q_1\}$	$\{C2, C3, C4, C5\}$
$C3$	$\{e, q_2\}$	
$C4$	$\{e, q_1\}$	
$C5$	$\{e, q_2\}$	
$C6$	$\{e, p_2\}$	$\{C6, C7, C8, C9\}$
$C7$	$\{e, p_1\}$	
$C8$	$\{e, p_2\}$	
$C9$	$\{e, p_1\}$	
$C10$	$\{e, a_2, q_1, q_2\}$	$\{C10, C11\}$
$C11$	$\{e, a_2, q_1, q_2\}$	
$C12$	$\{e, q_2\}$	$\{C12, C13, C14, C15\}$
$C13$	$\{e, q_1\}$	
$C14$	$\{e, q_2\}$	
$C15$	$\{e, q_1\}$	
$C16$	$\{e, a_1, a_2, a_3, p_1, p_2, q_1, q_2\}$	$\{C16\}$

Observe que quanto maior o estabilizador, menor a órbita e vice-versa. Mais ainda, repare que em todas as linhas (elementos x de X) temos a equação $\#(O_x) \times \#(S_x) = 8$. Isto não é uma coincidência e abaixo provamos este resultado, muito importante para nosso estudo.

Teorema 9.1 (O Teorema Órbita-Estabilizador) *Seja G um grupo que age em X . Então para cada $x \in X$,*

$$\#(O_x) \times \#(S_x) = \#(G)$$

Dem. Pelo lema 9.1, temos que S_x é um subgrupo de G , e pelo teorema de Lagrange segue que

$$|G : S_x| \times \#(S_x) = \#(G)$$

Assim precisamos mostrar que

$$\#(O_x) = |G : S_x| \tag{3}$$

Os elementos de O_x possuem a forma $g \cdot x$, para $g \in G$ e as classes laterais de S_x possuem a forma gS_x para $g \in G$. Podemos provar a equação (3) mostrando que a correspondência $g \cdot x \leftrightarrow gS_x$ é uma correspondência um-a-um entre os elementos de O_x e as classes laterais de S_x em G . Em outras palavras, basta mostrar que, para todo $g, h \in G$,

$$gS_x = hS_x \iff g \cdot x = h \cdot x$$

Sejam $g, h \in G$. Então

$$\begin{aligned} gS_x = hS_x &\iff h^{-1}g \in S_x, \text{ pelo lema 2.4} \\ &\iff (h^{-1}g) \cdot x = x, \text{ pela definição de } S_x \\ &\iff h^{-1} \cdot (g \cdot x) = x, \text{ por (A2)} \\ &\iff g \cdot x = h \cdot x, \text{ pelo lema 7.1} \end{aligned}$$

■

Corolário 9.1 *Seja G um grupo finito que age no conjunto X . Então o número de elementos de X em cada órbita é um divisor da ordem de G .*

Dem. Imediata a partir da equação multiplicativa do teorema Órbita-Estabilizador. ■

O Teorema Órbita-Estabilizador fornece uma relação entre o número de elementos em cada órbita e o número de elementos em cada estabilizador. Abaixo provamos facilmente um teorema que modifica esta relação para derivarmos uma fórmula para o número de diferentes órbitas da ação.

Teorema 9.2 *Seja G um grupo finito agindo em X . Então o número de órbitas distintas é dado por*

$$\frac{1}{\#(G)} \sum_{x \in X} \#(S_x)$$

Dem. Suponhamos que existam m órbitas distintas O_{x_1}, \dots, O_{x_m} . Se $1 \leq j \leq m$, temos para a j -ésima órbita que

$$\begin{aligned} \sum_{x \in O_{x_j}} \#(S_x) &= \sum_{x \in O_{x_j}} \frac{\#(G)}{\#(O_x)}, \text{ pelo Teorema Órbita-Estabilizador} \\ &= \#(G) \sum_{x \in O_{x_j}} \frac{1}{\#(O_{x_j})}, \text{ pois } O_x = O_{x_j} \text{ para todo } x \in O_{x_j} \\ &= \frac{\#(G)}{\#(O_{x_j})} \sum_{x \in O_{x_j}} 1 \\ &= \#(G) \end{aligned}$$

Assim, somando para todas as órbitas obtemos,

$$\sum_{x \in X} \#(S_x) = \sum_{j=1}^m \sum_{x \in O_{x_j}} \#(S_x) = \sum_{j=1}^m \#(G) = m\#(G)$$

o que nos fornece o resultado desejado. ■

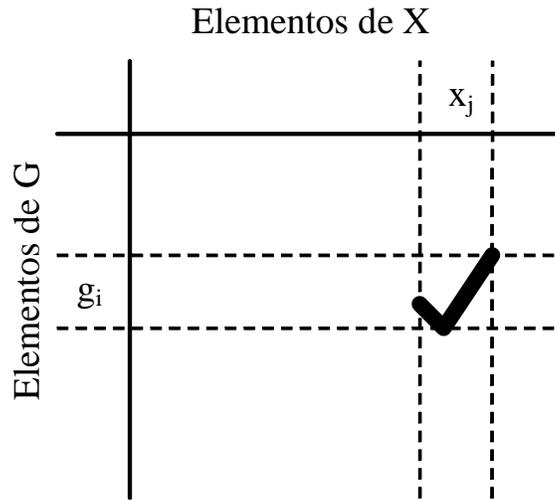
Observe que esta fórmula ainda não é de muito uso, pois devemos listar todos os elementos de X , o que nos possibilitaria, sem nenhuma teoria elaborada, diferenciar os padrões desejados por inspeção. No caso do tabuleiro 2×2 , temos que $\#(X) = 16$, mas no caso do tabuleiro de xadrez 8×8 , por exemplo, temos que $\#(X) = 2^{64} > 10^{19}$, o que torna impraticável listar todos os elementos de X .

Na seção seguinte, demonstramos um resultado que nos permite obter o número de órbitas somando nos elementos de G , ao invés de X .

10 - O Teorema de Burnside

Apesar do teorema (usualmente chamado de lema) a seguir ter se 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, por exemplo. 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.

A fim de obtermos a versão desejada para o número de órbitas, consideramos a tabela abaixo,



onde as linhas correspondem a elementos de G e as colunas a elementos de X .

Marcamos uma entrada na tabela na interseção de uma j -ésima coluna com uma i -ésima linha, isto é, da coluna de um elemento de X , com a linha de um elemento de G , se e somente se,

$$g_i \cdot x_j = x_j$$

isto é, se e somente se, $g_i \in S_{x_j}$.

Assim, o número de marcas em uma coluna j é $\#(S_{x_j})$ e portanto o número total de marcas na tabela é $\sum_{x \in X} \#(S_x)$.

Agora ao invés de adicionarmos as marcas por colunas, adicionaremos por linhas.

O número de marcas na i -ésima linha é dado pelo número de elementos do conjunto

$$\{x \in X : g_i \cdot x = x\}$$

isto é, o número de elementos de X que são fixados pelo elemento g_i de G .

Definição 10.1 *Seja G um grupo agindo em X , definimos o Fix de $g \in G$ como*

$$\text{Fix}(g) = \{x \in X : g \cdot x = x\}$$

Desta forma se somarmos o total de marcas de cada linha, obtemos todas as marcas da tabela, isto é,

$$\sum_{g \in G} \#(\text{Fix}(g)) = \sum_{x \in X} \#(S_x)$$

Demonstramos então o seguinte teorema:

Teorema 10.1 (Teorema de Burnside) *Se G é um grupo finito agindo em um conjunto X , então o número de órbitas distintas é dado por*

$$\frac{1}{\#(G)} \sum_{g \in G} \#(\text{Fix}(g))$$

11 - Aplicações

Problema 11.1 *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.*

Solução 11.1 *Neste problema, o conjunto X de colorações é formado pelas $n!$ permutações (aqui $C = D = [n]$) 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 o composto pela identidade e por $(n - 1)$ rotações. A identidade e fixa todos os $n!$ elementos de X , mas qualquer outro elemento $g \in G$ é tal que $Fix(g) = 0$. 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*

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

Problema 11.2 *De quantas maneiras diferentes podemos pintar as faces de um cubo, utilizando c cores diferentes? Calcule o número de pinturas utilizando as cores vermelho, preto e verde.*

Solução 11.2 *O número total de colorações presentes em X neste caso é dado por c^6 , pois um cubo tem 6 faces. Entendemos por igualdade entre uma pintura e outra, se uma puder ser obtida da outra por alguma simetria de rotação do cubo. No exemplo 3.3 listamos as 24 simetrias rotacionais do cubo descrevendo-as em 7 itens. Uma coloração de X é fixada por $g \in G$ se, e somente se, todas as faces no mesmo ciclo de g possuem a mesma cor. Vamos calcular aqui para cada simetria de cada item quantos elementos de X ela fixa:*

(1) *A identidade e fixa todos os elementos de $X \Rightarrow Fix(e) = c^6$;*

(2) *Cada rotação de $\frac{\pi}{2}$ pelo eixo indicado em (a) possui 1 ciclo de comprimento 4 e 2 ciclos de comprimento 1 nas faces. Assim, se uma coloração destas faces permanece inalterada após a rotação, teremos c diferentes possibilidades de cores para as 4 faces que compõem o ciclo de comprimento 4 e c cores diferentes para as faces de cada ciclo unitário. Portanto pelo princípio multiplicativo, temos $c \cdot c \cdot c$ diferentes colorações que são fixadas por cada rotação de $\frac{\pi}{2}$ indicada em (a). A contribuição destas 3 rotações é de $3c^3$;*

(3) *Para a rotação de π pelo eixo indicado em (a), temos 2 ciclos de comprimento 2 e 2 ciclos de comprimento 1. Pelas mesmas considerações feitas no item (2) acima, concluímos pelo princípio multiplicativo que o Fix de cada uma das 3 rotações é dado por $c \cdot c \cdot c \cdot c$. Assim a contribuição destas 3 rotações é de $3c^4$;*

(4) *Uma rotação de $\frac{3\pi}{2}$ pelo eixo de (a) é equivalente a uma de $-\frac{\pi}{2}$ pelo mesmo eixo. Por simetria temos a mesma contribuição do item (2), isto é, $3c^3$;*

(5) *Cada rotação de π pelo eixo indicado em (b) possui 3 ciclos de comprimento 2. Assim temos uma contribuição de $6c^3$;*

(6) Cada rotação de $\frac{2\pi}{3}$ pelo eixo indicado em (c) possui 2 ciclos de comprimento 3. Portanto temos uma contribuição de $4c^2$;

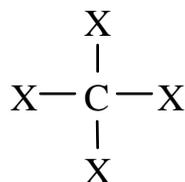
(7) Uma rotação de $\frac{4\pi}{3}$ é equivalente a uma de $-\frac{2\pi}{3}$, e por simetria temos a mesma contribuição do item (6), isto é, $4c^2$.

Pelo teorema de Burnside, temos então que o número de pinturas distintas das faces do cubo utilizando c cores é

$$\frac{1}{24} (c^6 + 3c^3 + 3c^4 + 3c^3 + 6c^3 + 4c^2 + 4c^2) = \frac{1}{24} (c^6 + 3c^4 + 12c^3 + 8c^2)$$

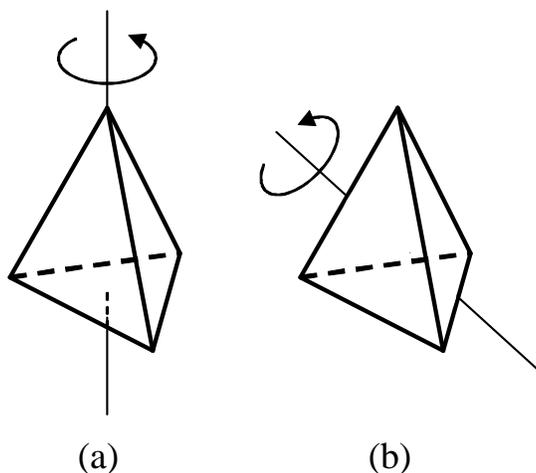
Para 3 cores, basta substituir $c = 3$ no polinômio acima para obter 57 pinturas distintas.

Problema 11.3 Quantas moléculas orgânicas diferentes da forma



existem, onde C é um átomo de carbono e cada X denota qualquer um dos 4 componentes CH_3 (metil), C_2H_5 (etil), H (hidrogênio) ou Cl (cloro)? (Aqui da química sabemos que cada molécula desse tipo pode ser modelada por um tetraedro regular com o carbono ocupando seu centro e os componentes X ocupando os vértices).

Solução 11.3 Considere a figura abaixo exibindo os dois tipos de eixo de rotação que o tetraedro regular possui:



Temos um total de $4^4 = 256$ colorações diferentes no conjunto X , pois neste caso estamos colorindo os vértices do tetraedro com 4 "cores" distintas. G é definido como o grupo das 12 simetrias rotacionais do tetraedro regular e vamos calcular o Fix de cada uma delas:

(1) A identidade fixa todas as 256 colorações de X .

(2) Temos 8 simetrias de rotaç3o pelo tipo de eixo indicado em (a), que passa por um v3rtice e pelo centro da face oposta. S3o 4 simetrias de rotaç3o de um 3ngulo de $\frac{2\pi}{3}$ e 4 simetrias de rotaç3o de um 3ngulo de $-\frac{2\pi}{3}$. Cada rotaç3o 3 composta de 1 ciclo de comprimento 1 e 1 ciclo de comprimento 3. Assim temos uma contribuiç3o de $8 \cdot 4 \cdot 4 = 128$ coloraç3es fixadas.

(3) Temos 3 simetrias de rotaç3o de um 3ngulo de π pelo tipo de eixo indicado em (b), que passa pelos pontos m3dios de arestas opostas. Cada rotaç3o desta 3 composta de 2 ciclos de comprimento 2. Portanto temos uma contribuiç3o de $3 \cdot 4 \cdot 4 = 48$ coloraç3es fixadas.

Aplicando o teorema de Burnside obtemos que o n3mero de mol3culas distintas nas condiç3es do problema 3 igual a

$$\frac{1}{12} (256 + 128 + 48) = 36$$

12 - O Teorema Enumerador de P3lya

Enunciamos o teorema de P3lya e apresentamos nesta seç3o uma de suas aplicaç3es aos problemas anteriores.

Teorema 12.1 (Teorema de P3lya) *Seja $X = \mathcal{F}(D, C)$ o conjunto de todas as coloraç3es do conjunto D em C , e seja ω uma funç3o peso em C . Seja G o grupo das permutaç3es de D que age em X de maneira usual. Se o 3ndice de ciclos de G 3*

$$Z(G; x_1, x_2, x_3, \dots)$$

ent3o o invent3rio padr3o 3 dado por

$$Z \left(G; \sum_{c \in C} \omega(c), \sum_{c \in C} \omega(c)^2, \sum_{c \in C} \omega(c)^3, \dots \right)$$

Problema 12.1 *De quantas maneiras podemos colorir as faces de um cubo utilizando as cores verde, amarelo e branco, de maneira que em cada pintura tenhamos exatamente 2 faces amarelas e 2 verdes? E a quantidade de pinturas contendo exatamente 1 face amarela?*

Soluç3o 12.1 *Baseado nas consideraç3es do problema 11.2, podemos obter facilmente a seguinte express3o para o 3ndice de ciclos das simetrias de rotaç3o de um cubo:*

$$\frac{1}{24} (x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2)$$

Colocamos como peso de cada cor

$$\omega(\text{amarelo}) = a$$

$$\omega(\text{verde}) = v$$

$$\omega(\text{branco}) = b$$

e assim obtemos o enumerador de estoque

$$a + v + b$$

Então, pelo teorema de Pólya, temos que o inventário padrão é dado por

$$\frac{1}{24}((a+v+b)^6 + 3(a+v+b)^2(a^2+v^2+b^2)^2 + 6(a+v+b)^2(a^4+v^4+b^4) + 6(a^2+v^2+b^2)^3 + 8(a^3+v^3+b^3)^2)$$

É conveniente usar algum software de álgebra simbólica para expandir esta soma e obter

$$\begin{aligned} & a^6 + b^6 + v^6 + ab^5 + a^5b + av^5 + a^5v + bv^5 + b^5v + \\ & + 2abv^4 + 2ab^4v + 2a^4bv + 2a^2b^4 + 2a^3b^3 + 2a^4b^2 + \\ & + 2a^2v^4 + 2a^3v^3 + 2a^4v^2 + 2b^2v^4 + 2b^3v^3 + 2b^4v^2 + \\ & + 3ab^2v^3 + 3ab^3v^2 + 3a^2bv^3 + 3a^2b^3v + 3a^3bv^2 + 3a^3b^2v + 6a^2b^2v^2 \end{aligned}$$

Para responder a primeira parte do problema, buscamos o coeficiente do termo $a^2v^2b^2$, que é igual a 6. Para a segunda pergunta, devemos agrupar todos os termos que contém a^1 :

$$a(b^5 + v^5 + 2bv^4 + 2b^4v + 3b^2v^3 + 3b^3v^2)$$

totalizando então 12 maneiras distintas.

Problema 12.2 No problema 11.3, qual é o número de moléculas que contém um ou mais átomos de hidrogênio?

Solução 12.2 O índice de ciclos para o problema 11.3 é facilmente obtido de sua resolução, sendo dado por

$$\frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2)$$

Designamos os pesos

$$\begin{aligned} \omega(CH_3) &= w_1 \\ \omega(C_2H_5) &= w_2 \\ \omega(Cl) &= w_3 \\ \omega(H) &= 0 \end{aligned}$$

a cada um dos componentes do problema.

Assim nosso enumerador de estoque é

$$w_1 + w_2 + w_3$$

que, pelas nossas considerações na seção 8.2, é a função geradora para 1 componente CH_3 , 1 componente C_2H_5 , 1 componente Cl e nenhum componente H . Desta forma estaremos enumerando primeiro as moléculas que não possuem átomos de hidrogênio.

Pelo teorema de Pólya, temos então que o inventário padrão é dado por

$$\frac{1}{12}((w_1 + w_2 + w_3)^4 + 8(w_1 + w_2 + w_3)(w_1^3 + w_2^3 + w_3^3) + 3(w_1^2 + w_2^2 + w_3^2)^2)$$

que ao ser expandido resulta em:

$$\begin{aligned} &w_1^4 + w_2^4 + w_3^4 + w_1w_2^3 + w_1^3w_2 + w_1w_3^3 + w_1^3w_3 + \\ &+ w_2w_3^3 + w_2^3w_3 + w_1w_2w_3^2 + w_1w_2^2w_3 + w_1^2w_2w_3 + \\ &+ w_1^2w_2^2 + w_1^2w_3^2 + w_2^2w_3^2 \end{aligned}$$

Portanto temos um total de 15 moléculas não contendo átomos de hidrogênio. Repare que a expressão acima diz muito mais que isso, pois nela está determinada qual a composição em componentes de cada uma das 15 moléculas. Também é interessante observar que, na função geradora acima, temos apenas 1 molécula para cada combinação dos 3 componentes CH_3 , C_2H_5 e Cl .

Como nesta resolução estamos interessados no número total de moléculas, pouparíamos trabalho se tivéssemos logo atribuído o peso 0 ao componente hidrogênio e peso 1 aos 3 componentes restantes. Do teorema de Pólya obteríamos diretamente o número

$$\frac{1}{12} (3^4 + 8 \cdot 3 \cdot 3 + 3 \cdot 3^2) = 15$$

Assim, como o número total de moléculas obtidas no problema 11.3 é 36, temos

$$36 - 15 = 21$$

moléculas que contém pelo menos 1 átomo de hidrogênio.

13 - Apêndice: Enumerando colares distintos

Ao contar colares, necessitamos encontrar o índice de ciclos do grupo cíclico C_n (se considerarmos apenas rotações) e do grupo diedral D_{2n} (se inversões são permitidas). Isto porque, num colar contendo n contas distintas, podemos considerar cada conta como ocupando cada um dos vértices de um polígono regular de n lados. Se um colar não puder ser invertido (virado, refletido), então não utilizamos as simetrias de reflexões presentes em D_{2n} , nos limitando às rotações que compõe C_n .

Neste apêndice, denotamos o $mdc(a, b)$ simplesmente por (a, b) .

Definição 13.1 A função totiente de Euler $\phi : \mathbb{N} \rightarrow \mathbb{N}$ é definida por

$$\phi(n) = \sum_{\substack{1 \leq d \leq n \\ (d, n) = 1}} 1$$

sendo dada pelo número de inteiros positivos menores ou iguais a n que são coprimos com n . Esta função também pode ser interpretada como o número de classes de congruência módulo n que são coprimas com n .

Para nossas aplicações, fazemos uso do seguinte resultado:

Lema 13.1 O grupo C_n (cíclico de ordem n) contém para cada divisor d de n , $\phi(d)$ elementos de ordem d . Cada um desses elementos possui n/d ciclos de comprimento d .

Assim temos que o índice de ciclos de C_n é dado por

$$Z(C_n) = \frac{1}{n} \sum_{d|n} \phi(d) x_d^{n/d}$$

onde a soma é efetuada nos divisores d de n e ϕ é a função totiente de Euler.

O grupo diedral D_{2n} contém o subgrupo C_n mais n reflexões. Se $n \equiv 1 \pmod{2}$ então cada reflexão tem um ponto fixo e $\frac{(n-1)}{2}$ transposições (2-ciclos); enquanto que se $n \equiv 0 \pmod{2}$, temos metade que são $\frac{n}{2}$ transposições e a outra metade são 2 pontos fixos e $\frac{(n-2)}{2}$ transposições. Desta forma

$$Z(D_{2n}) = \frac{1}{2} (Z(C_n) + R_n)$$

onde

$$R_n = \begin{cases} x_1 x_2^{\frac{n-1}{2}}, & \text{se } n \equiv 1 \pmod{2} \\ \frac{1}{2} \left(x_2^{\frac{n}{2}} + x_1^2 x_2^{\frac{(n-2)}{2}} \right), & \text{se } n \equiv 0 \pmod{2} \end{cases}$$

A seguir apresentamos a enumeração geral dos colares e alguns exemplos particulares.

Problema 13.1 *Qual o número de colares distintos, formados por n contas de m cores diferentes? (Considere os argumentos iniciais desta seção e divida o problema em dois casos).*

Solução 13.1 *Se considerarmos apenas as rotações, pelo teorema de Pólya, temos que o número é dado por*

$$\frac{1}{n} \sum_{d|n} \phi(d) m^{n/d} \quad (4)$$

onde atribuímos peso 1 a cada uma das m cores, e substituímos

$$x_d = \sum_{c \in C} \omega(c)^d = \sum_{c \in C} 1^d = m$$

no índice de ciclos de C_n .

Ao considerarmos também as inversões (reflexões), aplicamos o teorema de Pólya e substituímos o enumerador de estoque no índice de ciclos de D_{2n} . Desta forma obtemos a expressão

$$\frac{1}{2} \left(\frac{1}{n} \sum_{d|n} \phi(d) m^{n/d} + R_n(m) \right) \quad (5)$$

onde

$$R_n(m) \begin{cases} m^{\frac{n+1}{2}}, & \text{se } n \equiv 1 \pmod{2} \\ \frac{1}{2} m^{\frac{n}{2}} (1 + m), & \text{se } n \equiv 0 \pmod{2} \end{cases}$$

Problema 13.2 *Calcule:*

- (a) o número de colares diferentes, por rotações, com 6 contas coloridas em preto e branco;
- (b) o número de colares diferentes, por rotações e inversões, com 5 contas coloridas em preto, cinza e branco;
- (c) as mesmas condições do item (b), exceto que cada colar deverá ter exatamente 1 conta na cor preta.

Solução 13.2 (a) Na fórmula 4 do problema 13.1 colocamos $n = 6, m = 2$ para obter

$$\begin{aligned} \frac{1}{6} \sum_{d|6} \phi(d) 2^{6/d} &= \frac{1}{6} (\phi(1) 2^6 + \phi(2) 2^3 + \phi(3) 2^2 + \phi(6) 2) \\ &= \frac{1}{6} (64 + 8 + 8 + 4) \\ &= 14 \end{aligned}$$

Portanto temos 14 colares distintos como resposta.

(b) Substituímos na fórmula 5 do problema anterior $n = 5, m = 3$ e obtemos

$$\begin{aligned} \frac{1}{2} \left(\frac{1}{5} \sum_{d|5} \phi(d) 3^{5/d} + R_5(3) \right) &= \frac{1}{2} \left(\frac{1}{5} (\phi(1) 3^5 + \phi(5) 3) + 3^3 \right) \\ &= \frac{1}{2} \left(\frac{1}{5} (243 + 12) + 27 \right) \\ &= \frac{1}{2} \left(\frac{255}{5} + 27 \right) \\ &= \frac{1}{2} (78) \\ &= 39 \end{aligned}$$

Temos então 39 colares distintos como resposta. É interessante comparar as respostas dos itens (a) e (b) e suas condições. De lá para cá, diminuimos 1 conta do total e consideramos colares refletidos como idênticos; isto tende a diminuir o número de padrões distintos. No entanto, aumentamos 1 cor no estoque e isso foi o suficiente para termos quase o triplo de padrões distintos do item anterior. (Esta análise pode ser facilmente inferida no caso geral do formato do índice de ciclos utilizado)

(c) Desta vez atribuímos os pesos

$$\begin{aligned} \omega(\text{preto}) &= p \\ \omega(\text{cinza}) &= 1 \\ \omega(\text{branco}) &= 1 \end{aligned}$$

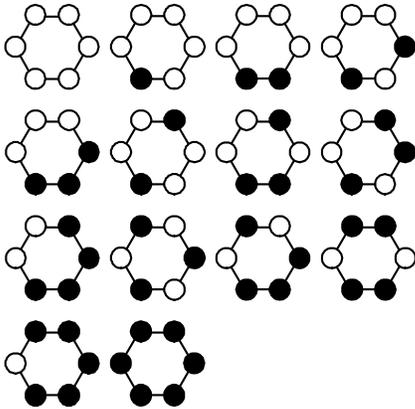
Aplicamos o teorema de Pólya e substituímos nosso enumerador de estoque no índice de ciclos de D_{10} , obtendo

$$\begin{aligned} &\frac{1}{2} \left(\frac{1}{5} \sum_{d|5} \phi(d) (p^d + 1^d + 1^d)^{5/d} + (p + 1 + 1) (p^2 + 1^2 + 1^2)^2 \right) \\ &= \frac{1}{10} ((p + 2)^5 + 4(p^5 + 2)) + \frac{(p + 2)(p^2 + 2)^2}{2} \\ &= 10p + 12p^2 + 6p^3 + 2p^4 + p^5 + 8 \end{aligned}$$

Nesta função geradora buscamos o coeficiente de p^1 que é igual a 10. Portanto temos 10 colares diferentes nas condições requisitadas e contendo exatamente 1 conta preta (verifique na figura a seguir os 10 colares!).

Na página seguinte listamos todos os colares correspondentes aos números encontrados neste problema:

Colares diferentes por rotação,
contendo 6 contas nas cores
preto e branco:



Colares diferentes por rotação e inversão
contendo 5 contas nas cores preto, cinza e
branco:

