CONTANDO COM A TEORIA DE AÇÃO DE GRUPOS

Gabriel Eurípedes de Jesus Farias
Universidade Federal de Uberlândia
gabriel-farias1997@hotmail.com

Victor Gonzalo Lopez Neumann
Universidade Federal de Uberlândia
glopezneumann@gmail.com

RESUMO

Neste trabalho, abordaremos a teoria de ação de grupos, apresentando seus principais resultados. Com ajuda de dois exemplos de ações de grupos em si mesmos, demonstraremos o Teorema de Cayley e a Fórmula de Classes. Além disso, apresentaremos o Teorema de Burnside e aplicá-lo-emos à resolução de um problema de contagem.

ABSTRACT

This paper will discuss the theory of group actions, presenting its main results. With the help of two examples of group actions on themselves, we demonstrate the Cayley's Theorem and the Class Formula. Furthermore, we show the Burnside's Theorem and apply it in solving a counting problem.

Palavras-chave: Ação de grupos em conjuntos, Teorema de Burnside e contagem.

1 INTRODUÇÃO

Notemos que os grupos ocorrem, de forma natural, como grupos de permutações, grupos diedrais, grupos de automorfismos e similares, de modo geral, como grupos que agem em algum conjunto. No presente trabalho, faremos uma introdução à teoria de ação de grupos em conjuntos e utilizaremos as ferramentas dessa teoria para resolver este interessante problema de contagem, ilustrando, assim, a teoria.

Problema: *Consideremos um colar constituído de n pérolas distribuídas de forma equiespaçada em torno de um círculo. Sabendo que cada pérola deve receber uma única cor dentre m cores disponíveis e que duas colorações são consideradas equivalentes se são iguais após alguma rotação ou reflexão axial, de quantos modos distintos podemos pintar esse colar?*

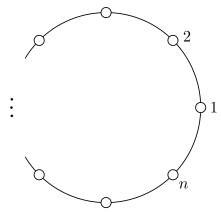

FIGURA 1: Colar constituído de n pérolas.

2 AÇÃO DE GRUPOS EM CONJUNTOS

Definição 2.1: *Consideremos um grupo G e um conjunto X. Uma ação à esquerda de G em X é uma função*

$$\begin{array}{rccc} \cdot : & G \times X & \to & X \\ & (g,x) & \mapsto & g \cdot x \end{array}$$

com as duas propriedades seguintes:
(i) $e \cdot x = x, \forall x \in X$*;*
(ii) $(gh) \cdot x = g \cdot (h \cdot x), \forall g, h \in G$ *e* $\forall x \in X$*.*

Observação 2.1: *Ações à direita de G em X são definidas de modo análogo; neste caso, a função é do tipo $\cdot : X \times G \to X$. Neste trabalho, consideraremos apenas as ações à esquerda. Dessa forma, escreveremos, simplesmente, ação de G em X para nos referirmos a uma ação à esquerda de G em X.*

Exemplo 2.1: *Sejam G um grupo e $X = G$. Definimos $g \cdot x = gx$, para todo $(g,x) \in G \times X$. Pelas propriedades da operação de um grupo, temos que $\cdot$ é uma ação de G em X. Neste caso, dizemos que G age em si mesmo por translação à esquerda.*

Exemplo 2.2: *Seja G um grupo e tomemos novamente $X = G$. Definimos $g \cdot x = gxg^{-1}$, para todo $(g,x) \in G \times X$. Notemos que $\forall g, h \in G$ e $\forall x \in X$, temos*

$$e \cdot x = exe^{-1} = x \text{ e } (gh) \cdot x = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = g(h \cdot x)g^{-1} = g \cdot (h \cdot x).$$

Então, $\cdot$ é uma ação de G em X. Neste caso, dizemos que G age em si mesmo por conjugação.

Lembremos que se X é um conjunto não vazio, uma permutação de X é uma bijeção $f : X \to X$. O conjunto de todas as permutações de X com a operação de composição de funções se chama o grupo simétrico sobre o conjunto X e se denota $S(X)$. Qualquer subgrupo de $S(X)$ é dito um grupo de permutações de X.

Equivalentemente, uma ação de um grupo G em um conjunto X pode ser definida como um homomorfismo $\rho : G \to S(X)$. A seguir, veremos que essas duas noções são equivalentes.

Lema 2.1: *Sejam G um grupo, X um conjunto e γ uma ação de G em X. Então*

$$\begin{array}{rccccccc} \rho : & G & \to & S(X) & & & \\ & g & \mapsto & \rho_g : & X & \to & X \\ & & & & x & \mapsto & g \cdot x \end{array}$$

é um homomorfismo de grupos, onde $g \cdot x$ denota $\gamma(g,x)$.

Demonstração

Primeiramente, mostraremos que ρ é uma função. Sejam $g, h \in G$ e $x \in X$. Veja que:

$$\rho_g \circ \rho_{g^{-1}}(x) = \rho_g(\rho_{g^{-1}}(x)) = \rho_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x = id_X(x);$$

$$\rho_{g^{-1}} \circ \rho_g(x) = \rho_{g^{-1}}(\rho_g(x)) = \rho_{g^{-1}}(g \cdot x) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x = id_X(x).$$

Assim, ρ_g possui a inversa $\rho_{g^{-1}}$ e, consequentemente, ρ_g é bijeção. Logo, $\rho(g)$ é uma permutação dos elementos do conjunto X. Além disso, temos

$$\rho_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot (\rho_h(x)) = \rho_g(\rho_h(x)) = \rho_g \circ \rho_h(x),$$

ou seja, $\rho(gh) = \rho(g) \circ \rho(h)$. Portanto, ρ é um homomorfismo.

■

Lema 2.2: *Sejam G um grupo, X um conjunto e ρ um homomorfismo de G em $S(X)$. Então*

$$\begin{array}{rccc} \gamma: & G\times X & \to & X \\ & (g,x) & \mapsto & \rho_g(x) \end{array}$$

é uma ação de G em X, onde ρ_g denota $\rho(g)$.

Demonstração

Sejam $g,h\in G$ e $x\in X$. Notemos que a função γ satisfaz:

$$\gamma(e,x)=\rho_e(x)=id_X(x)=x;$$

$$\gamma(gh,x)=\rho_{gh}(x)=\rho_g\circ\rho_h(x)=\rho_g(\gamma(h,x))=\gamma(g,\gamma(h,x)).$$

Portanto, γ é uma ação de G em X.

Teorema 2.1: *Consideremos um grupo G e um conjunto X. Ações de G em X e homomorfismos de G em $S(X)$ são noções equivalentes.*

Demonstração

Sejam A o conjunto de todas as ações de G em X e $\mathrm{Hom}(G,S(X))$ o conjunto de todos os homomorfismos de G em $S(X)$. Basta mostrarmos que existem funções $\alpha:\ A\to\mathrm{Hom}(G,S(X))$ e $\beta:\ \mathrm{Hom}(G,S(X))\to A$ que são inversas uma da outra.
Definamos as funções seguintes:

$$\begin{array}{rccccc} \alpha: & A & \to & \mathrm{Hom}(G,S(X)), & \text{onde} & \alpha_\gamma: \ G\to S(X) \\ & \gamma & \mapsto & \alpha_\gamma & & g\mapsto \alpha_\gamma(g): \ X\to X \\ & & & & & x\mapsto \gamma(g,x); \end{array}$$

$$\begin{array}{rccccc} \beta: & \mathrm{Hom}(G,S(X)) & \to & A, & \text{onde} & \beta_\rho: \ G\times X\to X \\ & \rho & \mapsto & \beta_\rho & & (g,x)\mapsto \rho(g)(x). \end{array}$$

Notemos que o Lema 2.1 garante que α é função, enquanto o Lema 2.2 garante que β é função. Consideremos $\rho\in\mathrm{Hom}(G,S(X))$. Notemos que, para quaisquer $g\in G$ e $x\in X$, temos

$$\alpha(\beta_\rho)(g)(x)=\beta_\rho(g,x)=\rho(g)(x),$$

ou seja, $\alpha\circ\beta(\rho)=\rho$.
Reciprocamente, tomemos $\gamma\in A$. Observemos que, para todo $(g,x)\in G\times X$, temos

$$\beta(\alpha_\gamma)(g,x)=\alpha_\gamma(g)(x)=\gamma(g,x),$$

isto é, $\beta\circ\alpha(\gamma)=\gamma$. Portanto, $\alpha\circ\beta=id_{\mathrm{Hom}(G,S(X))}$ e $\beta\circ\alpha=id_A$. Isso conclui a demonstração. ■

Observação 2.2: *Como temos essa equivalência de noções, dizemos que uma ação*

$$\gamma: G\times X\to X$$

induz o homomorfismo α_γ e que, reciprocamente, um homomorfismo $\rho: G\to S(X)$ induz a ação β_ρ.

Uma abordagem de ações de grupos por meio de homomorfismos pode ser conferida em [1, capítulo VI]. Nesse texto, uma ação de um grupo G em um conjunto X é chamada de representação de G no grupo de permutações de X.

Exemplo 2.3 (Solução – Parte 1): *Definiremos, por meio de um homomorfismo de grupos, a ação que nos ajudará a resolver o problema do colar. Representemos cada uma das m cores por um elemento de $\mathbb{Z}_m$, o conjunto de inteiros módulo m. Assim, cada atribuição de cores ao colar corresponde a um elemento do conjunto $(\mathbb{Z}_m)^n$.*

Seja $D_n = \langle r, s \mid r^n = s^2 = e,\ sr = r^{n-1}s\rangle$ o grupo diedral de ordem $2n$. Definamos o homomorfismo ρ de D_n em $S((\mathbb{Z}_m)^n)$ tal que:

$$\begin{array}{rccc} \rho(r): & (\mathbb{Z}_m)^n & \to & (\mathbb{Z}_m)^n \\ & (x_1, x_2, \ldots, x_n) & \mapsto & (x_n, x_1, x_2, \ldots, x_{n-1}); \end{array}$$

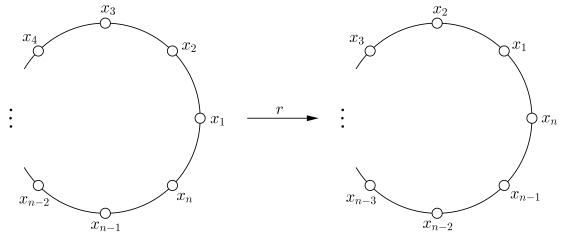

FIGURA 2: Interpretação geométrica da ação de r em uma n-upla.

$$\begin{array}{rccc} \rho(s): & (\mathbb{Z}_m)^n & \to & (\mathbb{Z}_m)^n \\ & (x_1, x_2, \ldots, x_n) & \mapsto & (x_1, x_n, x_{n-1}, \ldots, x_3, x_2). \end{array}$$

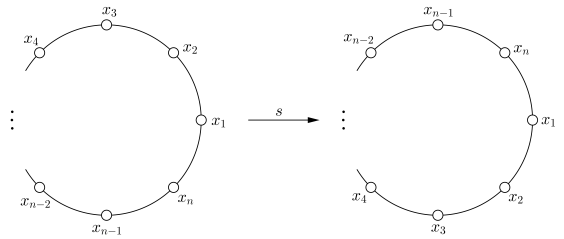

FIGURA 3: Interpretação geométrica da ação de s em uma n-upla.

Dessa forma, para ρ ser um homomorfismo, devemos ter:

$$\rho(r^k):\ (x_1, x_2, \ldots, x_n) \mapsto (x_{n-k+1}, \ldots, x_n, x_1, \ldots, x_{n-k});$$
$$\rho(r^k s):\ (x_1, x_2, \ldots, x_n) \mapsto (x_{k+1}, x_k, \ldots, x_1, x_n, x_{n-1}, \ldots, x_{k+2}).$$

Para que os índices de x nas n-uplas acima sempre estejam no conjunto $\{1, \ldots, n\}$, consideraremos, para qualquer $i \in \mathbb{Z}$, $x_i = x_{[i]_n}$, onde $[i]_n$ denota o resto da divisão euclidiana de i por n.

Notemos que $\rho(r)^n = \rho(s)^2 = id_{(\mathbb{Z}_m)^n}$ e $\rho(s) \circ \rho(r) = \rho(r)^{n-1} \circ \rho(s)$. Logo, ρ é, de fato, um homomorfismo de grupos. Esse homomorfismo induz a ação de D_n em $(\mathbb{Z}_m)^n$ dada por

$$g \cdot (x_1, \ldots, x_n) = \rho(g)(x_1, \ldots, x_n),\ \forall g \in D_n.$$

Observemos que r age em uma configuração do colar por rotação e s por reflexão axial.

3 ESTABILIZADOR, ÓRBITA E PONTOS FIXOS

Definição 3.1: *Suponha que um grupo G age em um conjunto X. Definimos:*
(i) o estabilizador de $x \in X$, denotado por G_x, como o conjunto $\{g \in G;\ g \cdot x = x\}$;
(ii) a órbita de $x \in X$, denotada por Gx, como o conjunto $\{g \cdot x;\ g \in G\}$;

(iii) o conjunto de todas as órbitas, denotado por $G\backslash X$, como o conjunto $\{Gx;\ x \in X\}$;
(iv) o conjunto dos pontos fixos de $g \in G$, denotado por $\mathrm{Fix}(g)$, como o conjunto $\{x \in X;\ g \cdot x = x\}$. Além disso, cada elemento de $\mathrm{Fix}(g)$ é chamado de ponto fixo de g.

Exemplo 3.1: *Consideremos um grupo G agindo no conjunto G por translação à esquerda. Tomemos $x \in G$. Notemos que o estabilizador de x é $\{e\}$. Evidentemente, $\{e\} \subseteq G_x$. Seja $g \in G_x$, isto é, $g \cdot x = gx = x$. Assim, $gx = ex$. Pela lei do cancelamento à direita, temos $g = e$. Logo, $G_x = \{e\}$.*

Além disso, observemos que a órbita de x é G. Claramente, $Gx \subseteq G$. Seja $g \in G$, então existe $gx^{-1} \in G$ tal que $(gx^{-1}) \cdot x = g(x^{-1}x) = g$. Assim, $g \in Gx$. Portanto, $Gx = G$.

Neste caso, concluímos que todos os estabilizadores são triviais e que existe uma única órbita.

Exemplo 3.2: *Consideremos um grupo G agindo em si mesmo, desta vez, por conjugação. Neste caso, o estabilizador de $x \in G$ se chama o centralizador de x e se denota $C_G(x)$. Ele é o maior subgrupo de G em que x é central, isto é, comuta com todos os elementos. De fato, se D é um subgrupo de G tal que x é central e $d \in D$, temos $d \cdot x = dxd^{-1} = xdd^{-1} = x$, uma vez que x comuta com qualquer elemento de D. Isso implica que $d \in C_G(x)$. Portanto, $D \subseteq C_G(x)$.*

Além disso, a interseção de todos os centralizadores é o centro do grupo. Lembremos que o centro de G é o subgrupo $Z(G) = \{h \in G;\ hg = gh,\ \forall g \in G\}$. De fato, temos as equivalências seguintes:

$$y \in \bigcap_{x \in G} C_G(x) \Leftrightarrow yxy^{-1} = x,\ \forall x \in G \Leftrightarrow yx = xy,\ \forall x \in G \Leftrightarrow y \in Z(G).$$

Portanto, $\bigcap_{x \in G} C_G(x) = Z(G)$.

As órbitas dessa ação são chamadas classes de conjugação.

Exemplo 3.3: *Consideremos o caso particular do problema do colar no qual esse possui 3 pérolas e as cores disponíveis são o cinza e o preto. Neste caso, temos D_3 agindo em $(\mathbb{Z}_2)^3$, onde as classes $\overline{0}$ e $\overline{1}$ representam o cinza e o preto, respectivamente. Encontremos a órbita e o estabilizador do elemento $(\overline{0}, \overline{1}, \overline{0})$.*

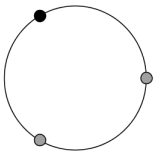

FIGURA 4: Colar correspondente ao elemento $(\overline{0}, \overline{1}, \overline{0})$.

Notemos que:

$$\begin{array}{lll} e \cdot (\overline{0}, \overline{1}, \overline{0}) = (\overline{0}, \overline{1}, \overline{0}); & r \cdot (\overline{0}, \overline{1}, \overline{0}) = (\overline{0}, \overline{0}, \overline{1}); & r^2 \cdot (\overline{0}, \overline{1}, \overline{0}) = (\overline{1}, \overline{0}, \overline{0}); \\ s \cdot (\overline{0}, \overline{1}, \overline{0}) = (\overline{0}, \overline{0}, \overline{1}); & rs \cdot (\overline{0}, \overline{1}, \overline{0}) = (\overline{1}, \overline{0}, \overline{0}); & r^2 s \cdot (\overline{0}, \overline{1}, \overline{0}) = (\overline{0}, \overline{1}, \overline{0}). \end{array}$$

Geometricamente, temos

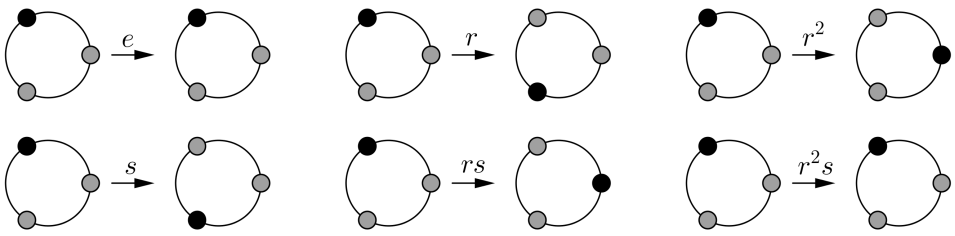

FIGURA 5: Ação dos elementos de D_3 no colar correspondente à terna $(\overline{0}, \overline{1}, \overline{0})$.

Assim, a órbita de $(\overline{0},\overline{1},\overline{0})$ *é*

$$\begin{aligned} D_3(\overline{0},\overline{1},\overline{0}) &= \{g\cdot(\overline{0},\overline{1},\overline{0});\ g\in D_3\} \\ &= \{(\overline{0},\overline{1},\overline{0}),(\overline{0},\overline{0},\overline{1}),(\overline{1},\overline{0},\overline{0})\}. \end{aligned}$$

Além disso, vemos que os únicos elementos que fixam essa terna são o elemento neutro e r^2s*, ou seja, o estabilizador de* $(\overline{0},\overline{1},\overline{0})$ *é*

$$\begin{aligned} D_{3_{(\overline{0},\overline{1},\overline{0})}} &= \{g\in D_3;\ g\cdot(\overline{0},\overline{1},\overline{0})=(\overline{0},\overline{1},\overline{0})\} \\ &= \{e, r^2s\}. \end{aligned}$$

Note que o estabilizador do elemento $(\overline{0},\overline{1},\overline{0})$ é um subgrupo de D_3. Veja também que o produto do número de elementos do estabilizador pelo número de elementos da órbita, ambos com relação à terna $(\overline{0},\overline{1},\overline{0})$, é igual à ordem de D_3. De maneira geral, se um grupo G age em um conjunto X e x é um elemento de X, o estabilizador de x é um subgrupo de G; em adição a isso, se G é finito, o produto do número de elementos da órbita de x pelo número de elementos do estabilizador de x é igual à ordem de G. Os dois próximos resultados fornecerão exatamente essas proposições.

Lema 3.1: *Consideremos uma ação de um grupo* G *em um conjunto* X*. Para todo* $x\in X$*,* G_x *é um subgrupo de* G*.*

Demonstração

Tomemos x em X. Notemos que $e\in G_x$, pois $e\cdot x = x$. Sejam g e h elementos de G_x, então $g\cdot x = x$ e $h\cdot x = x$. Temos:

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

$$g^{-1}\cdot x = g^{-1}\cdot(g\cdot x) = (g^{-1}g)\cdot x = e\cdot x = x.$$

Assim, gh e g^{-1} também são elementos de G_x. Logo, G_x é um subgrupo de G. ■

Teorema 3.1 (Teorema Órbita-Estabilizador)**:** *Se um grupo* G *age em um conjunto* X*, então, para todo* $x\in X$*, temos uma bijeção canônica*

$$\begin{aligned} f_x:\ G/G_x &\to Gx \\ gG_x &\mapsto g\cdot x. \end{aligned}$$

Em particular, se G *é finito, temos* $|Gx| = (G:G_x)$*.*

Demonstração

Seja x elemento de X. Primeiramente, provemos que f_x é uma função bem definida. Sejam $gG_x, hG_x\in G/G_x$ tais que $gG_x = hG_x$. Então, $g\in hG_x$, isto é, existe $j\in G_x$ que satisfaz $g = hj$. Visto que x é um ponto fixo de j, temos

$$f_x(gG_x) = g\cdot x = (hj)\cdot x = h\cdot(j\cdot x) = h\cdot x = f_x(hG_x).$$

Agora, tomemos $gG_x, hG_x\in G/G_x$ tais que $f_x(gG_x) = f_x(hG_x)$, isto é, $g\cdot x = h\cdot x$. Então,

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

ou seja, $h^{-1}g\in G_x$. Isso implica que $gG_x = hG_x$. Logo, f_x é injetora. Notemos que f_x é também sobrejetora, pois se $g\cdot x\in Gx$, então existe $gG_x\in G/G_x$ que satisfaz $f_x(gG_x) = g\cdot x$. Portanto, f_x é uma bijeção.

■

Lema 3.2: *Sejam $\cdot$ uma ação de um grupo G em um conjunto X e ρ o homomorfismo de G em $S(X)$ induzido por essa ação. Então o núcleo de ρ é a interseção de todos os estabilizadores, ou seja,*

$$\ker \rho = \bigcap_{x \in X} G_x.$$

Demonstração

Notemos que

$$\begin{array}{rccccccc} \rho: & G & \to & S(X) & & & \\ & g & \mapsto & \rho_g: & X & \to & X \\ & & & & x & \mapsto & g \cdot x. \end{array}$$

Tomemos $k \in \ker \rho$. Daí $\rho_k = id_X$ ou, de modo equivalente, $\rho_k(x) = k \cdot x = x$, para todo $x \in X$. Assim, $k \in \bigcap_{x \in X} G_x$. Reciprocamente, seja $l \in \bigcap_{x \in X} G_x$. Isto é, $\rho_l(x) = l \cdot x = x$, para todo $x \in X$. Dessa forma, temos que $\rho_l = id_X$, isto é, $l \in \ker \rho$. Portanto, $\ker \rho = \bigcap_{x \in X} G_x$.

■

Lema 3.3: *Sejam G um grupo e X um conjunto. As órbitas de uma ação $\cdot$ de G em X formam uma partição de X.*

Demonstração

Sobre X, definamos a relação $\sim$ da maneira seguinte:

$$x \sim y \Leftrightarrow \exists\ g \in G \text{ tal que } x = g \cdot y.$$

Provemos que $\sim$ é uma relação de equivalência. Consideremos $x, y, z \in G$. Notemos que $e \cdot x = x$, ou seja, $x \sim x$. Se $x = g \cdot y$ para algum $g \in G$, então

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = e \cdot y = y.$$

Logo, $x \sim y$ implica $y \sim x$. Se $x = g \cdot y$ e $y = h \cdot z$ para certos $g, h \in G$, então

$$(gh) \cdot z = g \cdot (h \cdot z) = g \cdot y = x.$$

Assim, $x \sim y$ e $y \sim z$ implicam $x \sim z$. Isso prova que $\sim$ é uma relação de equivalência sobre X. Claramente, as classes de equivalência, módulo $\sim$, são as órbitas, as quais formam uma partição do conjunto X.

■

Lema 3.4: *Consideremos um grupo G agindo em um conjunto X. Sejam $g \in G$ e $x \in X$ tais que $g \cdot x = x$. Se a é um inteiro, então $g^a \cdot x = x$.*

Demonstração

Dividamos em dois casos.
Caso 1: Suponhamos que a é um inteiro não negativo. Neste caso, provamos por indução sobre a. Para $a = 0$, o lema é verdadeiro, pois $g^0 \cdot x = e \cdot x = x$. Suponhamos, como hipótese de indução, que o lema é válido para a igual a um certo inteiro não negativo k, ou seja, $g^k \cdot x = x$; queremos mostrar que o lema é válido para $a = k + 1$. Para isso, basta ver que $g^{k+1} \cdot x = (g^k g) \cdot x = g^k \cdot (g \cdot x) = g^k \cdot x = x$; notemos que a última igualdade é fornecida pela hipótese de indução. Pelo Princípio da Indução, o lema é válido para todo a não negativo.
Caso 2: Suponhamos que a é um inteiro negativo. Pelo caso anterior, temos $g^{-a} \cdot x = x$, uma vez que $-a$ é um inteiro positivo. Segue que $g^a \cdot x = g^a \cdot (g^{-a} \cdot x) = (g^a g^{-a}) \cdot x = e \cdot x = x$.

■

As demonstrações dos dois próximos teoremas são aplicações das ações de grupos em si mesmos definidas nos Exemplos 2.1 e 2.2. Com ajuda da ação por translação à esquerda, concluiremos que todo grupo é, a menos de isomorfismo, um grupo de permutações de certo conjunto. E com auxílio da ação por conjugação, obteremos a Fórmula de Classes.

Teorema 3.2 (Cayley): *Se G é um grupo, então G é isomorfo a um subgrupo de $S(G)$.*

Demonstração

Consideremos G agindo em si mesmo pela translação à esquerda. Essa ação induz o homomorfismo

$$\begin{array}{rccccccc} \rho: & G & \to & S(G) & & & & \\ & g & \mapsto & \rho_g: & G & \to & G \\ & & & & x & \mapsto & gx. \end{array}$$

No Exemplo 3.1, concluímos que, para todo $x \in G$, o estabilizador de x é $\{e\}$. Pelo Lema 3.2, $ker\rho = \{e\}$ ou, equivalentemente, ρ é injetor. Logo, G é isomorfo a $Im(\rho)$, um subgrupo de $S(G)$.

■

Teorema 3.3 (Fórmula de Classes): *Se G é um grupo finito, então vale a igualdade seguinte:*

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} (G : C_G(x_\alpha)),$$

onde $\{x_\alpha\}_{\alpha\in\Gamma}$ é um sistema de representantes da partição formada pelas classes de conjugação.

Demonstração

Consideremos G agindo em si mesmo pela conjugação. Pelo Teorema 3.1, o número de elementos da classe de conjugação de $x \in G$ é igual a $(G : C_G(x))$. Primeiramente, mostremos que a classe de x possui um único elemento se, e somente se, $x \in Z(G)$.
Sabemos que $C_G(x)$ é um subconjunto de G. Suponhamos que a classe de x possui um único elemento, ou seja, $(G : C_G(x)) = 1$. Pelo Teorema de Lagrange, temos $|C_G(x)| = |G|$. Segue que $C_G(x) = G$. Isso implica que $gxg^{-1} = x$, para todo $g \in G$. Equivalentemente, $gx = xg$, para todo $g \in G$. Logo, $x \in Z(G)$. Reciprocamente, suponhamos que $x \in Z(G)$. Seja $g \in G$, então $gxg^{-1} = xgg^{-1} = x$, uma vez que x comuta com qualquer elemento de G. Assim, $g \in C_G(x)$. Logo, $G = C_G(x)$ e, por consequência, $|G| = |C_G(x)|$. Portanto, $(G : C_G(x)) = 1$.
Seja $\{x_\alpha\}_{\alpha\in\Gamma}$ um sistema de representantes da partição formada pelas classes de conjugação. Dessa forma, temos

$$|G| = \sum_{\alpha\in\Gamma}(G : C_G(x_\alpha)) = \sum_{x_\alpha\in Z(G)} (G : C_G(x_\alpha)) + \sum_{x_\alpha\notin Z(G)} (G : C_G(x_\alpha)).$$

Do fato de que $x \in Z(G)$ equivale a $(G : C_G(x)) = 1$, obtemos

$$|G| = \sum_{x_\alpha\in Z(G)} 1 + \sum_{x_\alpha\notin Z(G)} (G : C_G(x_\alpha)) = |Z(G)| + \sum_{x_\alpha\notin Z(G)} (G : C_G(x_\alpha)).$$

■

4 O TEOREMA DE BURNSIDE

Consideremos a ação de D_n em $(\mathbb{Z}_m)^n$ que definimos para resolver o problema do colar. Note que cada órbita é o conjunto das n-uplas que correspondem às rotações e reflexões

axiais de certo colar. Além disso, elementos pertencentes a órbitas distintas correspondem a colares que não podem ser transformados um no outro por rotação ou reflexão axial. Dessa forma, esse problema é equivalente a determinar o número de órbitas dessa ação. Nesse contexto, o próximo teorema é uma poderosa ferramenta para a contagem do número de órbitas.

Teorema 4.1 (Burnside): *Se um grupo G age em um conjunto X, ambos finitos, então o número de órbitas é a média aritmética do número de pontos fixos de cada elemento de G, isto é,*

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

Demonstração

Consideremos o conjunto $S = \{(g,x) \in G \times X;\ g\cdot x = x\}$. Notemos que

$$|S| = \sum_{g\in G}|\{x \in X;\ g\cdot x = x\}| = \sum_{g\in G}|\mathrm{Fix}(g)|.$$

Por outro lado, temos

$$|S| = \sum_{x\in X}|\{g \in G;\ g\cdot x = x\}| = \sum_{x\in X}|G_x|.$$

Pelo Teorema 3.1, $|Gx| = (G : G_x)$. Multiplicando por $|G_x|$ em ambos os lados e empregando o Teorema de Lagrange, obtemos $|G_x|\cdot|Gx| = |G|$. Assim, $|G_x| = \dfrac{|G|}{|Gx|}$. Prosseguindo,

$$|S| = \sum_{x\in X}\frac{|G|}{|Gx|} = \sum_{O\in G\backslash X}\sum_{x\in O}\frac{|G|}{|O|} = \sum_{O\in G\backslash X}|G| = |G\backslash X|\cdot|G|.$$

Os dois métodos de contagem do número de elementos do conjunto S fornecem a igualdade seguinte:

$$|G\backslash X|\cdot|G| = \sum_{g\in G}|\mathrm{Fix}(g)|.$$

■

Veja que podemos determinar o número de órbitas contando a quantidade de pontos fixos de cada elemento do grupo. Mas fazer tal contagem pode ser uma tarefa árdua. A seguir, apresentaremos um resultado que, em alguns casos, simplifica esse procedimento.

Teorema 4.2: *Consideremos um grupo G agindo em um conjunto X e $g \in G$ um elemento de ordem n. Se k é um inteiro e $d = mdc(k,n)$, então* $\mathrm{Fix}(g^k) = \mathrm{Fix}(g^d)$.

Demonstração

Pelo Lema 3.4, temos $\mathrm{Fix}(g^d) \subseteq \mathrm{Fix}(g^k)$. Assim, resta mostrar que $\mathrm{Fix}(g^k) \subseteq \mathrm{Fix}(g^d)$. Seja $x \in \mathrm{Fix}(g^k)$, então $g^k\cdot x = x$. Pelo Teorema de Bézout, existem inteiros a e b tais que $ak + bn = d$. Desse modo,

$$g^d\cdot x = g^{ak+bn}\cdot x = (g^k)^a\cdot x.$$

Aplicando o Lema 3.4 novamente, obtemos $(g^k)^a\cdot x = x$, ou seja, $x \in \mathrm{Fix}(g^d)$. Isso conclui a prova.

■

Agora temos as ferramentas necessárias para concluirmos a resolução do problema do colar.

Exemplo 4.1 (Solução – Parte 2): *No início desta seção, observamos que o número de modos de pintar o colar é igual ao número de órbitas da ação de D_n em $(\mathbb{Z}_m)^n$ que definimos no Exemplo 2.3. Pelo Teorema de Burnside,*

$$\begin{aligned} |D_n\backslash(\mathbb{Z}_m)^n| &= \frac{1}{|D_n|}\left(\sum_{k=1}^{n}|\mathrm{Fix}(r^k)| + \sum_{k=1}^{n}|\mathrm{Fix}(r^k s)|\right) \\ &= \frac{1}{2n}\left(\sum_{k=1}^{n}|\mathrm{Fix}(r^k)| + \sum_{k=1}^{n}|\mathrm{Fix}(r^k s)|\right). \end{aligned}$$

Primeiramente, contemos a quantidade de elementos do conjunto $\mathrm{Fix}(r^k)$ para cada potência $k \in \{1,\ldots,n\}$. Como r tem ordem n, pelo Teorema 4.2, se $d = mdc(k,n)$, então $\mathrm{Fix}(r^k) = \mathrm{Fix}(r^d)$. Veja que essa proposição ajuda a restringir tal contagem para cada potência que é um divisor de n. Nesse contexto, seja d um divisor positivo de n. Temos

$$\begin{aligned} \mathrm{Fix}(r^d) &= \{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ (x_{n-d+1},\ldots,x_n,x_1,\ldots,x_{n-d}) = (x_1,\ldots,x_n)\} \\ &= \{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ x_{n-d+i} = x_i \text{ e } x_{j-d} = x_j, \text{ para } 1\le i\le d \text{ e } d+1\le j\le n\} \\ &= \{(x_1,\ldots,x_d,x_1,\ldots,x_d,\ldots,x_1,\ldots,x_d)\in(\mathbb{Z}_m)^n;\ (x_1,\ldots,x_d)\in(\mathbb{Z}_m)^d\}. \end{aligned}$$

Pelo Princípio Fundamental da Contagem, $|\mathrm{Fix}(r^d)| = m^d$. Agora, definamos o conjunto seguinte:

$$A_d = \{k\in\mathbb{Z};\ 1\le k\le n \text{ e } mdc(k,n) = d\}.$$

Observemos que

$$\begin{aligned} A_d &= \left\{k\in\mathbb{Z};\ 1\le k\le n \text{ e } mdc\left(\tfrac{n}{d},\tfrac{k}{d}\right) = 1\right\} \\ &= \left\{k\in\mathbb{Z};\ 1\le \tfrac{k}{d}\le \tfrac{n}{d} \text{ e } mdc\left(\tfrac{n}{d},\tfrac{k}{d}\right) = 1\right\}. \end{aligned}$$

Claramente, $|A_d| = \varphi\left(\frac{n}{d}\right)$, onde φ é a função phi de Euler e, consequentemente, $\varphi\left(\frac{n}{d}\right)$ denota o número de inteiros positivos que não são maiores que $\frac{n}{d}$ e que são relativamente primos com $\frac{n}{d}$. Além disso, temos $\{1,2,\ldots,n\} = \bigcup_{d|n} A_d$, onde essa união é disjunta. Com essas considerações, temos

$$\sum_{k=1}^{n}|\mathrm{Fix}(r^k)| = \sum_{d|n}\sum_{k\in A_d}|\mathrm{Fix}(r^k)| = \sum_{d|n}\sum_{k\in A_d}|\mathrm{Fix}(r^d)| = \sum_{d|n}|A_d|\cdot|\mathrm{Fix}(r^d)| = \sum_{d|n}\varphi\left(\frac{n}{d}\right)\cdot m^d.$$

Neste momento, contemos o número de elementos do conjunto $\mathrm{Fix}(r^k s)$ para cada $k\in\{1,\ldots,n\}$. Para tal, consideremos a paridade de k.

Suponhamos que k é par. Neste caso, $x\in\mathrm{Fix}(r^k s)$ se, e somente se, $r^{n-\frac{k}{2}}\cdot x\in\mathrm{Fix}(s)$, pois temos as equivalências seguintes:

$$r^k s\cdot x = x \Leftrightarrow r^{\frac{k}{2}}s\cdot x = r^{n-\frac{k}{2}}\cdot x \Leftrightarrow s\cdot(r^{n-\frac{k}{2}}\cdot x) = r^{n-\frac{k}{2}}\cdot x.$$

Logo, $|\mathrm{Fix}(r^k s)| = |\mathrm{Fix}(s)|$.

Suponhamos que k é ímpar. Neste caso, $x\in\mathrm{Fix}(r^k s)$ se, e somente se, $r^{n-\frac{k-1}{2}}\cdot x\in\mathrm{Fix}(rs)$, porque, de forma similar, temos:

$$r^k s\cdot x = x \Leftrightarrow r^{\frac{k+1}{2}}s\cdot x = r^{n-\frac{k-1}{2}}\cdot x \Leftrightarrow rs\cdot(r^{n-\frac{k-1}{2}}\cdot x) = r^{n-\frac{k-1}{2}}\cdot x,$$

uma vez que $r^{\frac{k+1}{2}}s = rr^{\frac{k-1}{2}}s = rsr^{n-\frac{k-1}{2}}$. Logo, $|\mathrm{Fix}(r^k s)| = |\mathrm{Fix}(rs)|$.

Desse modo, podemos restringir essa contagem ao número de elementos dos conjuntos $\mathrm{Fix}(s)$ e $\mathrm{Fix}(rs)$. Consideremos dois casos.

Caso 1: Se n é par. Notemos que:

$$\begin{aligned}\mathrm{Fix}(s) &= \{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ (x_1,x_n,x_{n-1},\ldots,x_3,x_2)=(x_1,\ldots,x_n)\}\\ &= \left\{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ x_{n-i+2}=x_i,\ \text{para } 2\le i\le \tfrac{n}{2}\right\}\\ &= \left\{\left(x_1,x_2,x_3,\ldots,x_{\frac{n}{2}},x_{\frac{n+2}{2}},x_{\frac{n}{2}},\ldots,x_3,x_2\right)\in(\mathbb{Z}_m)^n;\ \left(x_1,x_2,\ldots,x_{\frac{n+2}{2}}\right)\in(\mathbb{Z}_m)^{\frac{n+2}{2}}\right\};\end{aligned}$$

$$\begin{aligned}\mathrm{Fix}(rs) &= \{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ (x_2,x_1,x_n,x_{n-1},\ldots,x_3)=(x_1,\ldots,x_n)\}\\ &= \left\{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ x_1=x_2 \text{ e } x_{n-i+3}=x_i,\ \text{para } 3\le i\le \tfrac{n+2}{2}\right\}\\ &= \left\{\left(x_2,x_2,x_3,\ldots,x_{\frac{n}{2}},x_{\frac{n+2}{2}},x_{\frac{n+2}{2}},x_{\frac{n}{2}},\ldots,x_3\right)\in(\mathbb{Z}_m)^n;\ \left(x_2,x_3,\ldots,x_{\frac{n+2}{2}}\right)\in(\mathbb{Z}_m)^{\frac{n}{2}}\right\}.\end{aligned}$$

Então, $|\mathrm{Fix}(s)| = m^{\frac{n+2}{2}}$ *e* $|\mathrm{Fix}(rs)| = m^{\frac{n}{2}}$*. Segue que* $|\mathrm{Fix}(r^k s)| = m^{\frac{n+2}{2}}$ *se* k *é par e* $|\mathrm{Fix}(r^k s)| = m^{\frac{n}{2}}$ *quando* k *é ímpar. Como no conjunto* $\{1,\ldots,n\}$ *há* $\frac{n}{2}$ *pares e* $\frac{n}{2}$ *ímpares, temos*

$$\sum_{k=1}^{n}|\mathrm{Fix}(r^k s)| = \frac{n}{2}\cdot m^{\frac{n+2}{2}} + \frac{n}{2}\cdot m^{\frac{n}{2}}.$$

Caso 2: Se n é ímpar. Neste caso, observemos que:

$$\begin{aligned}\mathrm{Fix}(s) &= \{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ (x_1,x_n,x_{n-1},\ldots,x_3,x_2)=(x_1,\ldots,x_n)\}\\ &= \left\{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ x_{n-i+2}=x_i,\ \text{para } 2\le i\le \tfrac{n+1}{2}\right\}\\ &= \left\{\left(x_1,x_2,x_3,\ldots,x_{\frac{n+1}{2}},x_{\frac{n+1}{2}},\ldots,x_3,x_2\right)\in(\mathbb{Z}_m)^n;\ \left(x_1,x_2,\ldots,x_{\frac{n+1}{2}}\right)\in(\mathbb{Z}_m)^{\frac{n+1}{2}}\right\};\end{aligned}$$

$$\begin{aligned}\mathrm{Fix}(rs) &= \{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ (x_2,x_1,x_n,x_{n-1},\ldots,x_3)=(x_1,\ldots,x_n)\}\\ &= \left\{(x_1,\ldots,x_n)\in(\mathbb{Z}_m)^n;\ x_1=x_2 \text{ e } x_{n-i+3}=x_i,\ \text{para } 3\le i\le \tfrac{n+1}{2}\right\}\\ &= \left\{\left(x_2,x_2,x_3,\ldots,x_{\frac{n+1}{2}},x_{\frac{n+3}{2}},x_{\frac{n+1}{2}},\ldots,x_3\right)\in(\mathbb{Z}_m)^n;\ \left(x_2,x_3,\ldots,x_{\frac{n+3}{2}}\right)\in(\mathbb{Z}_m)^{\frac{n+1}{2}}\right\}.\end{aligned}$$

Então, $|\mathrm{Fix}(s)| = |\mathrm{Fix}(rs)| = m^{\frac{n+1}{2}}$*. Isso implica que, independentemente da paridade de* k*,* $|\mathrm{Fix}(r^k s)| = m^{\frac{n+1}{2}}$*. Por consequência,*

$$\sum_{k=1}^{n}|\mathrm{Fix}(r^k s)| = n\cdot m^{\frac{n+1}{2}}.$$

Portanto, o número de modos de pintar o colar é

$$|D_n\backslash(\mathbb{Z}_m)^n| = \begin{cases}\dfrac{1}{2n}\left(\displaystyle\sum_{d|n}\varphi\left(\frac{n}{d}\right)\cdot m^d + \frac{n}{2}\cdot\left(m^{\frac{n+2}{2}}+m^{\frac{n}{2}}\right)\right) & \textit{se n é par}\\[2ex] \dfrac{1}{2n}\left(\displaystyle\sum_{d|n}\varphi\left(\frac{n}{d}\right)\cdot m^d + n\cdot m^{\frac{n+1}{2}}\right) & \textit{se n é ímpar.}\end{cases}$$

Apliquemos a fórmula obtida acima à resolução de alguns casos particulares do problema do colar.

Exemplo 4.2: *Resolvamos o caso particular considerado no exemplo 3.3, no qual* $n=3$ *e* $m=2$*. Neste caso, visto que* n *é ímpar, o número de modos de pintar o colar é*

$$\begin{aligned}
|D_3\backslash(\mathbb{Z}_2)^3| &= \frac{1}{2\cdot 3}\left(\sum_{d|3}\varphi\left(\frac{3}{d}\right)\cdot 2^d + 3\cdot 2^{\frac{3+1}{2}}\right)\\
&= \frac{1}{6}\left(\varphi\left(\frac{3}{1}\right)\cdot 2^1 + \varphi\left(\frac{3}{3}\right)\cdot 2^3 + 3\cdot 2^2\right)\\
&= \frac{1}{6}\left(2\cdot 2 + 1\cdot 8 + 3\cdot 4\right)\\
&= 4.
\end{aligned}$$

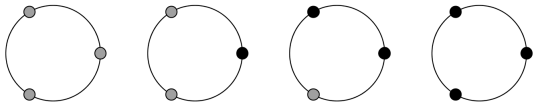

FIGURA 6: Maneiras de pintar um colar de 3 pérolas dispondo de 2 cores.

Exemplo 4.3: *Calculemos o número de modos de pintar um colar constituído de* 4 *pérolas, dispondo das cores cinza e preta. Notemos que* $n = 4$ *e* $m = 2$*. Neste caso, o número de modos de pintar o colar é*

$$\begin{aligned}
|D_4\backslash(\mathbb{Z}_2)^4| &= \frac{1}{2\cdot 4}\left(\sum_{d|4}\varphi\left(\frac{4}{d}\right)\cdot 2^d + \frac{4}{2}\cdot\left(2^{\frac{4+2}{2}} + 2^{\frac{4}{2}}\right)\right)\\
&= \frac{1}{8}\left(\varphi\left(\frac{4}{1}\right)\cdot 2^1 + \varphi\left(\frac{4}{2}\right)\cdot 2^2 + \varphi\left(\frac{4}{4}\right)\cdot 2^4 + 2\cdot\left(2^3 + 2^2\right)\right)\\
&= \frac{1}{8}\left(2\cdot 2 + 1\cdot 4 + 1\cdot 16 + 2\cdot(8+4)\right)\\
&= 6.
\end{aligned}$$

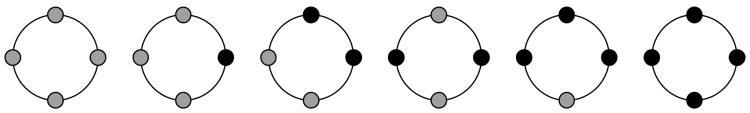

FIGURA 7: Formas de pintar um colar de 4 pérolas tendo 2 cores à disposição.

Exemplo 4.4: *Determinemos a quantidade de maneiras de pintar um colar constituído de* 6 *pérolas, dispondo de* 5 *cores. Como* n *é par, temos*

$$\begin{aligned}
|D_6\backslash(\mathbb{Z}_5)^6| &= \frac{1}{2\cdot 6}\left(\sum_{d|6}\varphi\left(\frac{6}{d}\right)\cdot 5^d + \frac{6}{2}\cdot\left(5^{\frac{6+2}{2}} + 5^{\frac{6}{2}}\right)\right)\\
&= \frac{1}{12}\left(\varphi\left(\frac{6}{1}\right)\cdot 5^1 + \varphi\left(\frac{6}{2}\right)\cdot 5^2 + \varphi\left(\frac{6}{3}\right)\cdot 5^3 + \varphi\left(\frac{6}{6}\right)\cdot 5^6 + 3\cdot\left(5^4 + 5^3\right)\right)\\
&= \frac{1}{12}\left(2\cdot 5 + 2\cdot 25 + 1\cdot 125 + 1\cdot 15625 + 3\cdot(625+125)\right)\\
&= 1505.
\end{aligned}$$

Portanto, há 1505 *modos distintos de pintar um colar constituído de* 6 *pérolas, dispondo de* 5 *cores. Neste caso, percebemos que a aplicação da fórmula é prática, enquanto a ilustração de todas as configurações é inviável.*

Bons livros para o estudo da teoria de ações de grupos são [2], [3] e [4]. Em particular, [2] apresenta outros exemplos interessantes de aplicação dessa teoria e ainda demonstra uma generalização do Teorema de Burnside.

5 CONCLUSÃO

No presente trabalho, utilizamos a noção de ação de grupos para concluir que todo grupo é, a menos de isomorfismo, um grupo de permutações de certo conjunto e também para aplicarmos ideias geométricas à resolução de um problema de contagem. Desse modo, concluímos que essa noção fornece resultados importantes tanto para enriquecer o conhecimento sobre os grupos quanto para a modelagem e a simplificação de problemas de análise combinatória.

REFERÊNCIAS

[1] A. Garcia and Y. Lequain, *Elementos de álgebra*. IMPA, 2013.

[2] S. R. Nagpaul and S. K. Jain, *Topics in applied abstract algebra*. Thomson Brooks/Cole, 2005.

[3] H. E. Rose, *A course on finite groups*. Springer, 2009.

[4] M. Stoll, *Introductory algebra*. 2005. Disponível em: http://www.mathe2.uni-bayreuth.de/stoll/lecture-notes/IntroductoryAlgebra.pdf. Acesso em: 4 set. 2016.