

Grupos e Corpos

Prof. Lucas Calixto

Aula 6 - Ações de Grupos

Ação de grupos em conjuntos

Uma **ação de um grupo G em um conjunto X** é uma função $G \times X \rightarrow X$, $(g, x) \mapsto gx$ satisfazendo:

- $ex = x \ \forall x \in X$
- $(g_1g_2)x = g_1(g_2x) \ \forall x \in X, \ g_1, g_2 \in G$

Se G age em X , dizemos que X é um **G -conjunto**

Exemplo: $GL(n, \mathbb{R})$ age **naturalmente** em \mathbb{R}^n : multiplicação de matrizes (vetor = matriz coluna)

$$GL(n, \mathbb{R}) \times \mathbb{R}^n \rightarrow \mathbb{R}^n, \quad (g, v) \mapsto gv$$

Exemplo: S_4 age no conjunto $X = \{1, 2, 3, 4\}$ permutando os índices:

$$S_4 \times X \rightarrow X, \quad (f, x) \mapsto f(x)$$

Exemplo: $X = \{1, 2, 3, 4\}$ pode ser identificado com os vértices de um quadrado, e assim D_4 age em X

Exemplo: Se $H \leq G$, então H age em X via multiplicação a esquerda

$$H \times G \rightarrow G, \quad (h, g) \mapsto hg$$

Exemplo: H também em G via conjugação:

$$H \times G \rightarrow G, \quad (h, g) \mapsto hgh^{-1}$$

Note: G age em si mesmo via multiplicação a esquerda e via conjugação

Exemplo: Se $H \leq G$, então G age em $L_H = \{gH \mid g \in G\}$

$$G \times L_H \rightarrow L_H, \quad (g, xH) \mapsto gxH$$

Exercício: Verifique os detalhes dos exemplos acima

Suponha que G age em X . Dois elementos $x, y \in X$ são G -equivalentes (escrevemos $x \sim_G y$, ou somente $x \sim y$) se $\exists g \in G$ tal que $gx = y$

Exercício: Prove que \sim define uma relação de equivalência em X

A classe de equivalência de $x \in X$ é denotada por O_x . O conjunto O_x é chamado de **órbita de x** (com relação a ação de G em X)

$$O_x \cap O_y \neq \emptyset \Leftrightarrow O_x = O_y \Rightarrow X = \dot{\bigcup}_{x \in X} O_x$$

Note: $O_x = \{y \in X \mid x \sim y\} = \{y \in X \mid y = gx \text{ para algum } g \in G\} = \{gx \mid g \in G\}$

As vezes é conveniente denotarmos a órbita de x por $Gx = \{gx \mid g \in G\}$

Exemplo: Seja $G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$ um grupo de permutações de $X = \{1, 2, 3, 4, 5\}$. Então G age em X , e temos

$$O_1 = O_2 = O_3 = \{1, 2, 3\}, \quad O_4 = O_5 = \{4, 5\}$$

O conjunto dos **pontos fixos** por $H \subset G$ é $X_H = \{x \in X \mid hx = x \ \forall h \in H\}$

O **estabilizador** de $x \in X$ é o conjunto $G_x = \{g \in G \mid xg = x\}$. Note: $G_x \leq G$

O estabilizador G_x também recebe o nome de **subgrupo de isotropia** de x

Proposição: O estabilizador G_x é um subgrupo de G

Prova: $e \in G_x \Rightarrow G_x \neq \emptyset$

$$g, h \in G_x \Rightarrow gh^{-1}x = gh^{-1}hx = gx = x \Rightarrow gh^{-1} \in G_x$$

Exemplo: Seja $G = \{(1), (12)(3456), (35)(46), (12)(3654)\}$ um grupo de permutações de $X = \{1, 2, 3, 4, 5, 6\}$. Então G age em X , e temos

Os seguintes conjuntos de pontos fixos

$$X_{(1)} = X, \quad X_{(35)(46)} = \{1, 2\}, \quad X_{(12)(3456)} = X_{(12)(3654)} = \emptyset$$

Os seguintes estabilizadores

$$G_1 = G_2 = \{(1), (35)(46)\}, \quad G_3 = G_4 = G_5 = G_6 = \{(1)\}$$

As seguintes orbitas

$$O_1 = O_2 = \{1, 2\}, \quad O_3 = O_4 = O_5 = O_6 = \{3, 4, 5, 6\}$$

Teorema (órbita-estabilizador) Se G age em um conjunto finito X , então
 $|O_x| = [G : G_x], \forall x \in X$

Prova: A função $\phi : O_x \rightarrow L_{G_x} = \{gG_x \mid g \in G\}$, $\phi(gx) = gG_x$ é bijeção

• $\psi : L_{G_x} \rightarrow O_x$, $\psi(gG_x) = gx$ é bem definida

$gG_x = hG_x \Leftrightarrow g \in hG_x \Leftrightarrow g = hg', g' \in G_x$. Logo,

$$\psi(gG_x) = gx = hg'x = hx = \psi(hG_x)$$

$$\psi = \phi^{-1}$$

$$\psi \circ \phi(gx) = \psi(gG_x) = gx$$

e

$$\phi \circ \psi(gG_x) = \phi(gx) = gG_x$$

Como $[G : G_x] = |L_{G_x}|$, o resultado segue

Corolário: $|O_x|$ divide $|G|$ para todo $x \in X$

Equação de classes

Note: $x \in X_G = \{x \in X \mid gx = x, \forall g \in G\} \Leftrightarrow |O_x| = 1$. Logo

$$X_G = \bigcup_{|O_x|=1} O_x \Rightarrow X = X_G \cup \left(\bigcup_{|O_x|>1} O_x \right) \Rightarrow |X| = |X_G| + \sum_{|O_x|>1} |O_x|$$

Considere G agindo em G por conjugação, então

$$\begin{aligned} G_G &= \{x \in G \mid gxg^{-1} = x, \forall g \in G\} = \{x \in G \mid gx = xg, \forall g \in G\} \\ &= Z(G) = \text{centro de } G \end{aligned}$$

As orbitas O_x dessa ação tais que $|O_x| > 1$ são chamadas **classes de conjugação** de G

Também

$$G_x = \{x \in G \mid gxg^{-1} = x\} = \{x \in G \mid gx = xg\} = C(x) = \text{centralizador de } x \text{ em } G$$

Logo,

$$|G| = |Z(G)| + \sum_{|O_x|>1} |O_x| \Rightarrow |G| = |Z(G)| + \sum_{|O_x|>1} [G : C(x)]$$

Essa equação é chamada **equação de classes**

Classes de conjugação em S_n

Lembre: dois ciclos $\sigma, \tau \in S_n$ tem mesmo comprimento se e só se eles são conjugados por um elemento de S_n (ou seja, se e só se eles estão na mesma classe de conjugação). Logo,

$$C(\sigma) = C(\tau) \Leftrightarrow \sigma, \tau \text{ tem o mesmo comprimento}$$

Se $\sigma \in S_n \Rightarrow \sigma = \sigma_1 \sigma_2 \cdots \sigma_r$ decomposição (única) em termos de ciclos disjuntos, onde o comprimento de σ_i é m_i

Assuma que $m_1 \geq \cdots \geq m_r$, e que **todo elemento de $\{1, \dots, n\}$ aparece em algum σ_i** (se $\sigma(a) = a$, então a aparece no 1-ciclo $(a) = id$)

O **tipo cíclico** de σ é (m_1, \dots, m_r)

Note: (m_1, \dots, m_r) é uma partição de n , ou seja, $\sum m_i = n$

Exemplo: Em S_7 , temos

$(1) = (1)(2) \cdots (7)$ tem tipo cíclico $(1, \dots, 1)$

$(123)(45) = (123)(45)(6)(7)$ tem tipo cíclico $(3, 2, 1, 1)$

$(1234) = (1234)(5)(6)(7)$ tem tipo cíclico $(4, 1, 1, 1)$

$(12 \cdots 7)$ tem tipo cíclico (7)

Proposição: Se $\sigma, \tau \in S_n$, então $C(\sigma) = C(\tau) \Leftrightarrow \sigma$ e τ tem o mesmo tipo cíclico

$(\Rightarrow) C(\sigma) = C(\tau) \Leftrightarrow \tau = \rho\sigma\rho^{-1} = \rho\sigma_1\sigma_2 \cdots \sigma_r\rho^{-1} = \rho\sigma_1\rho^{-1}\rho\sigma_2\rho^{-1}\rho \cdots \rho^{-1}\rho\sigma_r\rho^{-1}$

$\rho\sigma_i\rho^{-1}$ e σ_i tem o mesmo tipo cíclico $\Rightarrow \sigma$ e τ tem o mesmo tipo cíclico

(\Leftarrow) Exercício

Corolário: Existe bijeção

$$\{\text{partições de } n\} \leftrightarrow \{\text{classes de conjugação de } S_n\}$$

Exemplo Em S_3 temos o seguinte esquema **partição** \leftrightarrow **classes de conjugação**

$$(3) \leftrightarrow O_{(123)} = O_{(132)} = \{(123), (132)\}$$

$$(2, 1) \leftrightarrow O_{(12)} = O_{(13)} = O_{(23)} = \{(12), (13), (23)\} \text{ (lembre: } (12) = (12)(3))$$

$$(1, 1, 1) \leftrightarrow Z(G) = \{(1)\}$$

A equação de classes de S_3 é $|O_{(12)}| + |O_{(123)}| + |Z(G)| = 3 + 2 + 1 = |S_3|$

Teorema: Se $|G| = p^n$ então $Z(G) \neq \{e\}$

Prova: todos $[G : C(x)]$ dividem $|G| \Rightarrow p \mid [G : C(x)] \Rightarrow [G : C(x)] = k_i p$

$$|G| = |Z(G)| + \sum_{|O_x| > 1} [G : C(x)] = |Z(G)| + \sum k_i p \Rightarrow |Z(G)| = p^n - (\sum k_i) p \Rightarrow p \text{ divide } |Z(G)|$$

Como $|Z(G)| > 0 \Rightarrow |Z(G)| \geq p \Rightarrow Z(G) \neq \{e\}$

Corolário: Se $|G| = p^2$, então G é abeliano

Prova: slide anterior $\Rightarrow |Z(G)| = p$ ou p^2

$|Z(G)| = p^2 \Rightarrow \text{OK}$

$|Z(G)| = p \Rightarrow |G/Z(G)| = p \Rightarrow G/Z(G)$ é cíclico $\Rightarrow G/Z(G) = \langle aZ(G) \rangle$

$\forall g, h \in G \Rightarrow \exists m, n \in \mathbb{Z}$ tais que $gZ(G) = a^m Z(G)$, $hZ(G) = a^n Z(G)$

$\Rightarrow \exists x, y \in Z(G)$ tais que $g = a^m x$, $h = a^n y$

Assim, $gh = a^m x a^n y = a^m a^n xy = a^n a^m xy = a^n y a^m x = hg \Rightarrow G$ é abeliano

Teorema de Burnside

Lema: Se G age em X e $x, y \in X$ são tais que $x \sim y$, então $G_x \cong G_y$

Prova: $x \sim y \Leftrightarrow \exists g \in G$ tal que $y = gx$

Defina $\phi : G_x \rightarrow G_y$, $\phi(a) = gag^{-1}$

Note: $a \in G_x \Rightarrow gag^{-1}y = gag^{-1}(gx) = gax = gx = y \Rightarrow gag^{-1} \in G_y \Rightarrow \phi$ é bem definida

ϕ é homomorfismo

$$\phi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi(a)\phi(b)$$

$\psi : G_y \rightarrow G_x$, $\psi(a) = g^{-1}ag$ é inversa de ϕ

$$\psi\phi(a) = \psi(gag^{-1}) = g^{-1}gag^{-1}g = a$$

$$\phi\psi(b) = \psi(g^{-1}bg) = gg^{-1}bgg^{-1}g = b$$

Logo, $G_x \cong G_y$

Teorema (Burnside): Suponha que G é finito e age em um conjunto finito X . Se k é a quantidade de orbitas de X , então

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

Prova: Considere $Y = \{(g, x) \in G \times X \mid gx = x\}$

Para cada $g \in G$ existem exatamente $|X_g|$ pares (g, x) tal que $gx = x$, ou seja para cada $g \in G$ existem exatamente $|X_g|$ pares $(g, x) \in Y$. Logo

$$|Y| = \sum_{g \in G} |X_g|$$

Analogamente, para cada $x \in X$ existem $|G_x|$ pares (g, x) em Y , e portanto

$$|Y| = \sum_{x \in X} |G_x|$$

Escrevendo $X = \dot{\bigcup}_{i=1}^k O_{x_i}$, temos

$$|Y| = \sum_{y \in O_{x_1}} |G_y| + \cdots + \sum_{y \in O_{x_k}} |G_y|$$

Último lema + Teorema órbita-estabilizador + Teorema de Lagrange implicam

$$\sum_{y \in O_{x_i}} |G_y| = |O_{x_i}| |G_{x_i}| = [G : G_{x_i}] |G_{x_i}| = |G|$$

Assim, igualando as duas expressões de $|Y|$, obtemos

$$\sum_{g \in G} |X_g| = \sum_{y \in O_{x_1}} |G_y| + \cdots + \sum_{y \in O_{x_k}} |G_y| = k|G|$$

e portanto,

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

Exemplo: Se $X = \{1, 2, 3, 4, 5\}$ e $G = \{(1), (13), (13)(25), (25)\}$, os pontos fixos são

$$X_{(1)} = X, \quad X_{(13)} = \{2, 4, 5\}, \quad X_{(13)(25)} = \{4\}, \quad X_{(25)} = \{1, 3, 4\}$$

Teorema de Burnside \Rightarrow número de órbitas $= \frac{1}{4}(5 + 3 + 1 + 3) = 3$

De fato, as órbitas de X são

$$\{1, 3\}, \quad \{2, 5\}, \quad \{4\}$$

Aplicação Geométrica

O **teorema de Burnside** pode ser usado para contar de quantas formas diferentes podemos colorir os vértices de um polígono regular de branco e preto. Duas formas de colorir são consideradas iguais se uma pode ser obtida da outra por meio de movimentos rígidos, ou seja, por meio de ação de D_n (pintar somente o primeiro vértice de preto, é a mesma coisa de pintar somente o segundo)

Exemplo: Considere essa pergunta para um quadrado Q . O conjunto de vértices de Q é $X = \{1, 2, 3, 4\}$

$D_4 = \{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\} \leq S_4$ age em X por permutações

Cada forma de colorir o quadrado pode ser identificada com uma função $f : X \rightarrow Y = \{B, P\}$ (B =branco e P =preto)

Seja $\tilde{X} = \{f : X \rightarrow Y\}$. Note: D_4 também age em \tilde{X} : $(\sigma, f) \mapsto f\sigma$

Duas formas de colorir $f, g \in \tilde{X}$ são iguais $\Leftrightarrow g = f\sigma$ para $\sigma \in D_4$, ou seja, $O_f = O_g$

Logo, por Burnside, existem $k = \frac{1}{|D_4|} \sum_{\sigma \in D_4} |\tilde{X}_\sigma| = 6$ (cheque os detalhes usando o próximo slide)

Proposição: Suponha que G é um grupo de permutações de X . Para um dado conjunto Y , considere $\tilde{X} = \{f : X \rightarrow Y\}$. Então G também é grupo de permutações de \tilde{X} , onde $(\sigma, f) = f\sigma \in \tilde{X}$. Além disso, se a decomposição de σ em ciclos disjuntos tem n ciclos, então $|\tilde{X}_\sigma| = |Y|^n$

Prova: $(\sigma, f) = f\sigma \in \tilde{X}$ define ação (exercício)

Suponha $\sigma = \sigma_1 \cdots \sigma_n$ é a decomposição em ciclos disjuntos de σ

Seja $X_i = \{a \in X \mid a \text{ aparece em } \sigma_i\}$. Assim, $X = \bigcup_{i=1}^n X_i$, pois todo $a \in X$ aparece em algum σ_i (σ_i podendo ser o 1-ciclo $(a) = id$)

$f \in \tilde{X}_\sigma \Leftrightarrow f = f\sigma$. Assim, se $\sigma_i = (a_1 a_2 \cdots a_k)$, então

$$f(a_1) = f\sigma(a_1) = f(a_2) = f\sigma(a_2) = f(a_3) = \cdots = f(a_k)$$

Logo, $f \in \tilde{X}_\sigma \Leftrightarrow |f(X_i)| = 1$ para cada i

Em particular, $\tilde{X}_\sigma = \{f : \{\{X_1\}, \dots, \{X_n\}\} \rightarrow Y\} \Rightarrow |\tilde{X}_\sigma| = |Y|^n$

Exemplo: No exemplo anterior, tínhamos:

$$G = D_4 = \{(1), (13), (24), (1432), (1234), (12)(34), (14)(23), (13)(24)\}$$

$X = \{1, 2, 3, 4\}$, $Y = \{B, P\}$. Assim:

$$(1) = (1)(2)(3)(4) \Rightarrow \tilde{X}_{(1)} = |Y|^4 = 2^4 = 16$$

$$(13) = (13)(2)(4) \Rightarrow \tilde{X}_{(13)} = |Y|^3 = 2^3 = 8$$

$$\tilde{X}_{(1432)} = |Y|^1 = 2^1 = 2$$

Exercícios:

Cap 14: 2, 3, 4, 5, 7, 8, 15, 20, 21, 22, 23