

Álgebra Abstrata: ferramentas e aplicações em problemas olímpicos

Vitória Aparecida Santos Ferreira - vitoriaaparecida94@gmail.com

29a Semana Olímpica - Janeiro 2026 - Nível U

1 Definições iniciais

A **Álgebra Abstrata** é um ramo da Álgebra que se caracteriza por estudar diferentes estruturas algébricas (grupos, anéis, corpos, por exemplo). Difere, portanto, da Álgebra Linear, que é dedicada especificamente aos espaços vetoriais e transformações lineares.

Definição 1 (Grupo). Um grupo é um par $(G, *)$ formado por um conjunto G e uma operação $*$: $G \times G \rightarrow G$ tal que

(Elemento neutro) Existe $e \in G$ com $ge = eg = g, \forall g \in G$.

(Inverso) Para cada $g \in G$, existe $h \in G$ com $gh = hg = e$. Denota-se o inverso por g^{-1} .

(Associatividade) $(gh)k = g(hk), \forall g, h, k \in G$.

Se o grupo respeitar que $gh = hg, \forall g, h \in G$, então G é comutativo ou **abeliano**.

Exemplo 1. $(\mathbb{Z}, +)$ é um grupo; $Sym(X)$ é o grupo das bijeções de X em X .

Definição 2 (Subgrupo). $H \subseteq G$ é chamado de **subgrupo** de G se também for um grupo.
Notação: $H \leq G$.

Exemplo 2. Considere, por exemplo, o grupo $(\mathbb{Z}, +)$ e tome o subconjunto dos números pares. Este constitui um subgrupo por ser ele próprio um grupo. Ambos são grupos cíclicos, isto é, gerados por um único elemento, com $\langle 1 \rangle = \{\dots, -1, 0, 1, \dots\}$ e $\langle 2 \rangle = \{\dots, -2, 0, 2, \dots\}$.

Definição 3 (Subgrupo normal). H subgrupo de G é **normal** se, dado qualquer $g \in G$,

$$\{gh \mid h \in H\} = gH = Hg = \{hg \mid h \in H\}.$$

Em particular, em um grupo abeliano todo subgrupo é normal.

1.1 Ordem de um elemento

Definição 4 (Ordem de um elemento). Seja G um grupo. A ordem de $g \in G$ é o menor inteiro positivo n tal que $g^n = e$. Denota-se $ord(g)$ ou $|g|$.

Todo elemento em um grupo finito (de **ordem** finita, $|G| < \infty$) possui ordem finita; há elementos em grupos infinitos cuja ordem é finita.

Exemplo 3. Considere \mathbb{Q}^* munido da multiplicação. Então, este é um grupo infinito tal que $1, -1$ têm ordem finita, mas os demais possuem ordem infinita.

Teorema 1 (Teorema de Lagrange). Em um grupo finito, a ordem de qualquer subgrupo divide a ordem do grupo.

Corolário 1. Um grupo de ordem prima não possui subgrupos próprios.

Teorema 2 (Teoremas de Sylow). Seja G grupo, p primo, $|G| = p^k m$, onde $\text{mdc}(p, m) = 1$.

1° Existe subgrupo de G de ordem p^k .

2° Se H é subgrupo de ordem p^l e P é subgrupo de ordem p^k , então H está contido em algum gPg^{-1} , $g \in G$.

3° A quantidade n_p de subgrupos de ordem p^k é um divisor de m e $n_p \equiv 1 \pmod{p}$.

2 Homomorfismos de grupos

Definição 5 (Homomorfismo). Um **homomorfismo** de um grupo G em um grupo H é uma função $\phi : G \rightarrow H$ que respeita as respectivas operações nos grupos, isto é,

$$\phi(g_1 g_2) = \phi(g_1) \phi(g_2), \forall g_1, g_2 \in G.$$

Lema 1. Se $\phi : G \rightarrow H$ é homomorfismo de grupos, então, para $g \in G$ elemento de ordem finita, tem-se que $|\phi(g)|$ divide $|g|$.

Demonstração. Considere $|g| = n$. Então,

$$e_G = g^n \Rightarrow e_H = \phi(e_G) = \phi(g^n) = (\phi(g))^n.$$

Portanto, $|\phi(g)| := m$ é no máximo n . Tomando a divisão de n por m , escreva $n = mq + r$, $r < m$. Assim,

$$e_H = (\phi(g))^n = (\phi(g))^{mq} (\phi(g))^r = [(\phi(g))^m]^q (\phi(g))^r = e_H^q (\phi(g))^r = (\phi(g))^r.$$

Se $r \neq 0$, teríamos uma contradição com a minimalidade de m . Desse modo, $r = 0$ e tem-se o resultado. \square

Definição 6 (Núcleo). Dado $\phi : G \rightarrow H$ homomorfismo de grupos, o **núcleo de ϕ** é o subconjunto

$$Z := \{g \in G \mid \phi(g) = e_H\}.$$

Teorema 3 (Primeiro teorema do isomorfismo). Seja $\phi : G \rightarrow H$ homomorfismo de grupos. Então,

- a) $\ker(\phi)$ é um subgrupo normal de G .
- b) A imagem, $\text{Im}(\phi)$, é um subgrupo de H .
- c) $\text{Im}(\phi)$ é isomorfa a $G/\ker(\phi)$.

3 Ações de grupos

Definição 7 (Ação). Uma **ação** (à esquerda) de um grupo G sobre um conjunto X é uma função $\varphi : G \times X \rightarrow X$ tal que

- (i) $\varphi(e, x) = x, \forall x \in X$.

(ii) $\varphi(g, \varphi(h, x)) = \varphi(gh, x), \forall g, h \in G, x \in X.$

Se fixarmos $g \in G$, podemos denotar a ação como

$$\varphi_g : X \rightarrow X.$$

Esta é uma bijeção de X em X com inversa $\varphi_{g^{-1}}$. Assim, define-se um homomorfismo $f : G \rightarrow \text{Sym}(X)$, dado por $g \mapsto \varphi_g$.

Exemplo 4. A conjugação, definida por $(g, x) \mapsto gxg^{-1}$, é uma ação de grupos.

Teorema 4 (Órbita-estabilizador). Considere G um grupo finito agindo em um conjunto X . Dado $x \in X$, sejam $O(x) := \{gx \mid g \in G\} \subseteq X$ a órbita de x e $G_x := \{g \in G \mid gx = x\} \subseteq G$ o estabilizador de x . Então,

$$|O(x)| \cdot |G_x| = |G|.$$

Teorema 5 (Lema de Burnside). Seja G grupo agindo em um conjunto X . A quantidade de órbitas é dada por

$$\frac{1}{|G|} \sum_{g \in G} |X^g|,$$

onde $X^g := \{x \in X \mid \varphi(g, x) = x\}$, isto é, o conjunto de pontos fixados por g .

OBS: as órbitas definem uma partição de X . Pode-se pensar que são as classes de equivalência da relação $x \sim y \Leftrightarrow \exists g \in G, gx = y$.

OBS: o estabilizador é um subgrupo de G .

4 Exercícios

1. (OBMU 2018 - 2a fase) Seja $GL_2(\mathbb{R})$ o conjunto das matrizes 2×2 inversíveis com elementos reais. Determine todos os pares de inteiros positivos (m, n) com a seguinte propriedade: se $A, B \in GL_2(\mathbb{R})$ são tais que $A \cdot B^m = B^m \cdot A$ e $A \cdot B^n = B^n \cdot A$, então A e B comutam, isto é, $AB = BA$.
2. (IMC 2021 - P6) Para um primo p , seja $GL_2(\mathbb{Z}_p)$ o grupo de matrizes invertíveis 2×2 cujas entradas são os resíduos módulo p . Seja S_p o grupo simétrico em p elementos. Mostre que não há homomorfismo injetor $\varphi : GL_2(\mathbb{Z}_p) \rightarrow S_p$.
3. (CELM 2021) Seja $Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ o grupo dos quatérnions, cujo produto é determinado pelas equações

$$i^2 = j^2 = k^2 = ijk = -1.$$

Escolhendo-se aleatoriamente e independentemente dois elementos $a, b \in Q_8$ (não necessariamente distintos), qual a probabilidade de $ab = ba$?

4. (CELM 2023) De quantas maneiras distintas é possível pintar as casas de um tabuleiro 1×2023 , sendo que cada casa pode ter exatamente uma entre 3 cores distintas? (Duas configurações são consideradas idênticas se uma puder ser obtida a partir da outra por uma sobreposição através de um movimento de rotação do tabuleiro no plano em que ele está desenhado).
5. (Putnam 2007 - A5) Prove que, se um grupo finito possui exatamente n elementos de ordem p , p primo, então $n = 0$ ou p divide $n + 1$.

6. (Putnam 1968 - B2) Seja G grupo finito e A subconjunto com mais da metade dos elementos de G . Prove que todo elemento do grupo é o produto de dois em A .
7. (Putnam 2012 - B6) Seja p primo ímpar tal que $p \equiv 2 \pmod{3}$. Defina uma permutação π das classes de resíduo módulo p por $\pi(x) \equiv x^3 \pmod{p}$. Mostre que π é uma permutação par se, e somente se, $p \equiv 3 \pmod{4}$.

Referências

- [1] John B. Fraleigh. *A first course in abstract algebra*. Pearson, 7th edition, 2002.
- [2] IMC. International mathematics competition for university students. <https://www.imc-math.org.uk/>, última visita em 18/12/2025.