NOTAS DE AULA DE ÁLGEBRA

TIAGO MACEDO

Aula 4

1.6. Homomorfismos e isomorfimos

Definição 4.1. Sejam (G, m_G) e (H, m_H) dois grupos. Um homomorfismo de grupos de G para H é uma função $f\colon G \to H$ satisfazendo:

(i) $f(m_G(g_1, g_2)) = m_H(f(g_1), f(g_2))$ para todos $g_1, g_2 \in G$,
(ii) $f(e_G) = e_H$.

Um isomorfismo de grupos é um homomorfismo de grupos que é bijetor. Dizemos que o grupo G é isomorfo ao grupo H quando existe algum isomorfismo de grupos $f\colon G \to H$. Neste caso, denotamos $G \cong H$.

Um homomorfismo entre dois grupos é uma função que preserva a estrutura importante que esses conjuntos têm, a de grupo. Quando existe um isomorfismo entre dois grupos, isso significa que a estrutura de grupo de um pode ser transferida para o outro sem perder informação. Ou seja, quando dois grupos são isomorfos, eles são, de certa forma, idênticos. O próximo resultado mostra algumas evidências disso.

Lema 4.2. *Sejam G e H dois grupos.*

(a) Se $f\colon G \to H$ é um homomorfismo de grupos, então $f(g^n) = f(g)^n$ para todo $n \in \mathbb{Z}$. Em particular, $f(g^{-1}) = f(g)^{-1}$ para todo $g \in G$.
(b) Se $G \cong H$, então $|G| = |H|$ (os dois conjuntos têm a mesma cardinalidade).
(c) Se $G \cong H$ e G é abeliano, então H é abeliano.
(d) Se $f \cong G \to H$ for um isomorfismo, então $o(f(g)) = o(g)$ para todo $g \in G$.

Demonstração. (a) Fixe $g \in G$. Se $n = 0$, então $f(g^0) = f(e_G) = e_H = f(g)^0$. Vamos usar indução para $n > 0$. O caso $n = 1$ é óbvio, então suponha que $f(g^{n-1}) = f(g)^{n-1}$. Como f é um homomorfismo de grupos, pela hipótese de indução, nós temos que

$$f(g^n) = f(gg^{n-1}) = f(g)f(g^{n-1}) = f(g)f(g)^{n-1} = f(g)^n.$$

Isso prova o caso $n \geq 0$. Para $n = -1$, observe que $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$ e $f(g^{-1})f(g) = f(g^{-1}g) = f(e_G) = e_H$. Portanto $f(g^{-1})$ é o inverso de $f(g)$. Para completar a demonstração, use indução para $n < 0$.

(b) Se $G \cong H$, então exite um isomorfismo $f\colon G \to H$. Em particular, f é uma bijeção entre os conjuntos G e H. Portanto $|G| = |H|$.

(c) Seja $f\colon G \to H$ um isomorfismo. Em particular, f é sobrejetora, ou seja, para cada $h \in H$, existe $g \in G$ tal que $f(g) = h$. Dados $h_1, h_2 \in H$, tome $g_1, g_2 \in G$ tais que $f(g_1) = h_1$ e $f(g_2) = h_2$. Como$f$ é um homomorfismo de grupos e G é abeliano, então

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1.$$

Isso mostra que H é abeliano.

(d) Dado $g \in G$, denote $o(g) = n$ e lembre que $g^n = e_G$ e $e_G \notin \{g, g^2, \ldots, g^{n-1}\}$. Como f é um isomorfismo, em particular, $f(e_G) = e_H$ e f é injetora. Logo, $f(g) = e_H$ se, e somente se, $g = e_G$. Portanto $f(g)^n = f(g^n) = f(e_G) = e_H$ e $e_H \notin \{f(g), f(g)^2, \ldots, f(g)^{n-1}\}$. Isso mostra que $o(f(g)) = n$. $\square$

Exercício 4.3. Sejam G, H e K três grupos.

(a) Mostre que $\mathrm{id}_G \colon G \to G$ é um isomorfismo de grupos.
(b) Se $f \colon G \to H$ é um isomorfismo de grupos, mostre que $f^{-1} \colon H \to G$ também é um isomorfismo de grupos.
(c) Se $\phi \colon G \to H$ e $\psi \colon H \to K$ forem homomorfismos (resp. isomorfismos) de grupos, mostre que $(\psi \circ \phi) \colon G \to K$ é um homomorfismo (resp. isomorfismo) de grupos.
(d) Conclua que $\cong$ (isomorfismo de grupos) é uma relação de equivalência.

Um exemplo de homomorfismo de grupos que já é familiar é o seguinte.

Exemplo 4.4. Considere dois $\mathbb{R}$-espaços vetoriais $(V, +_V, \cdot_V)$ e $(W, +_W, \cdot_W)$. Pela definição, toda transformação linear $T \colon V \to W$ é um homomorfismo do grupo $(V, +_V)$ para o grupo $(W, +_W)$. Além disso, todo isomorfismo linear $T \colon V \to W$ é um isomorfismo do grupo $(V, +_V)$ para o grupo $(W, +_W)$.

Um caso particular do exemplo anterior é o seguinte.

Exemplo 4.5. Considere o grupo aditivo $\mathbb{R}$, o grupo multiplicativo $\mathbb{R}_{>0} = \{\alpha \in R \mid \alpha > 0\}$ e a função $\exp \colon \mathbb{R} \to \mathbb{R}_{>0}$ dada por $\exp(a) = e^a$. Vamos mostrar que exp é um isomorfismo de grupos.

(i) $\exp(a + b) = e^{a+b} = e^a e^b = \exp(a) \cdot \exp(b)$ para todos $a, b \in \mathbb{R}$.
(ii) $\exp(0) = e^0 = 1$

Isso mostra que exp é um homomorfismo de grupos. Além disso, $\ln \colon \mathbb{R}_{>0} \to \mathbb{R}$ é a inversa de exp. Portanto, exp é uma bijeção, e consequentemente, um isomorfismo de grupos.

O próximo exemplo mostra que, dados quaisquer dois grupos, sempre existe algum homomorfismo entre eles.

Exemplo 4.6. Sejam G e H dois grupos. Verifique que a função $f \colon G \to H$ dada por $f(g) = e_H$ para todo $g \in G$ é um homorfismo de grupos. Esse homomorfismo é chamado de homomorfismo trivial. Observe que esse homomorfismo é um isomorfismo se, e somente se, $G = H = \{e\}$.

Exemplo 4.7. Seja $n \geq 3$. Verifique que a função $\vartheta \colon D_{2n} \to S_n$ definida na Seção 1.2 (Aula 3) é um homomorfismo de grupos. Além disso, mostre que ϑ é um isomorfismo se, e somente se, $n = 3$.

Nos próximos exemplos, vamos usar geradores e relações para construir homomorfismo de grupos.

Exemplo 4.8. Considere os grupos abelianos $\mathbb{Z}$ e $\mathbb{Z}_n$ ($n \geq 2$). Para cada $k \in \mathbb{Z}$, podemos definir um único homomorfimo de grupos $f_k \colon \mathbb{Z} \to \mathbb{Z}_n$ satisfazendo $f_k(1) = \overline{k}$. De fato, como 1 gera $\mathbb{Z}$ e queremos que f_k seja um homomorfismo de grupos, então $f_k(\ell) = k\ell$ para todo $\ell \in \mathbb{Z}$. Em particular, se escolhermos $k = 0$, obteremos o homoorfismo trivial; e se escolhermos $k = 1$, obteremos um homomorfismo chamado de projeção canônica.

Exemplo 4.9. Considere agora os grupos aditivos $\mathbb{Z}_2$ e $\mathbb{Z}_6$. Assim como no exemplo anterior, para cada $k \in \mathbb{Z}$, vamos tentar construir um homomorfismo de grupos $f_k \colon \mathbb{Z}_2 \to \mathbb{Z}_6$. Se definirmos $f_k(\overline{1}) = \overline{k}$, como queremos que f_k seja um homomorfismo de grupos, teremos que:

$$f_k(\overline{0}) = f_k(\overline{1} + \overline{1}) = f_k(\overline{1}) + f_k(\overline{1}) = \overline{2k} = \overline{0}.$$

Mas, observe que $\overline{2k} = \overline{0}$ se, e somente se, $\overline{k} \in \{\overline{0}, \overline{3}\}$. Em particular, $f_1(\overline{1}) = \overline{1}$ **não** induz um homomorfismo de grupos.

Mas se, assim como $\mathbb{Z}$, o grupo $\mathbb{Z}_2$ é gerado por um único elemento, qual é a diferença desse exemplo para o anterior? A diferença é que o gerador $\overline{1} \in \mathbb{Z}_2$ satisfaz a relação $2\overline{1} = \overline{0}$ (enquanto o gerador $1 \in \mathbb{Z}$ não satisfaz relação nenhuma). Então, no caso de $\mathbb{Z}_2$, nós podemos definir f_k só no gerador $\overline{1}$, mas nós temos que verificar que $f_k(\overline{1})$ também satisfaz a relação $2f_k(\overline{1}) = \overline{0}$.

Vamos usar a idéia do exemplo anterior no próximo exemplo.

Exemplo 4.10. Sejam $n \geq 2$ e $f\colon \mathbb{Z}_n \to \mathbb{Z}$ um homomorfismo de grupos. Como $\mathbb{Z}_n$ é gerado por $\overline{1}$, então f é únicamente determinado por $f(\overline{1})$. Ou seja, se $f(\overline{1}) = k$, então $f(\overline{\ell}) = \overline{k\ell}$ para todo $\overline{\ell} \in \mathbb{Z}_n$. Agora, como $f(\overline{1}) = k$ deve satisfazer a relação $nk = 0$ e $n \neq 0$, concluímos que $k = 0$. Ou seja, não existe nenhum homomorfismo de grupos $f\colon \mathbb{Z}_n \to \mathbb{Z}$ além do trivial.

1.7. Ações de grupos

Definição 4.11. Sejam G um grupo e X um conjunto. Uma ação de G em X é uma função $\alpha\colon G \times X \to X$ satisfazendo:

(i) $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$ para todos $g, h \in G$ e $x \in X$,
(ii) $\alpha(e, x) = x$ para todo $x \in X$.

Nesse caso, dizemos que G age em X. Quando não gerar confusão, nós denotaremos $\alpha(g, x)$ por $g \cdot x$ ou simplesmente gx.

Um exemplo que deve ser familiar é o seguinte.

Exemplo 4.12. Considere um $\mathbb{R}$-espaço vetorial $(V, +\cdot)$ e o grupo multiplicativo $\mathbb{R} \setminus \{0\}$. A multiplicação escalar em V induz uma função $\alpha\colon \mathbb{R} \setminus \{0\} \times V \to V$ dada por $\alpha(\lambda, v) = \lambda \cdot v$. Vamos verificar que α é uma ação de $\mathbb{R} \setminus \{0\}$ em V.

(i) Para todos $\lambda, \mu \in \mathbb{R} \setminus \{0\}$ e $v \in V$, por um dos axiomas de espaço vetorial, temos:

$$\alpha(\lambda, \alpha(\mu, v)) = \alpha(\lambda, \mu \cdot v) = \lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot x = \alpha(\lambda\mu, v).$$

(ii) Para todo $v \in V$, por outro axioma de espaço vetorial, temos $\alpha(1, v) = 1 \cdot v = v$.

Exemplo 4.13. Considere um conjunto X (por exemplo, tome $X = \{1, \ldots, n\}$) e o grupo S_X formado por todas as permutações de X (bijeções de X em X) munido da composição (por exemplo, $S_{\{1,\ldots,n\}} = S_n$). Defina uma função $\alpha\colon S_X \times X \to X$ como sendo $\alpha(\sigma, x) = \sigma(x)$. Vamos verificar que α é uma ação de S_X em X:

(i) Para todos $\sigma, \rho \in S_X$ e $x \in X$, temos:

$$\alpha(\sigma, \alpha(\rho, x)) = \alpha(\sigma, \rho(x)) = \sigma(\rho(x)) = (\sigma \circ \rho)(x) = \alpha(\sigma\rho, x).$$

(ii) Para todo $x \in X$, temos $\alpha(e, x) = \mathrm{id}_X(x) = x$.

Exemplo 4.14. Considere $G = D_{2n}$, $X = \Delta_n$ um n-ágono regular, e defina uma função $\alpha\colon G \times X \to X$ como sendo $\alpha(\sigma, x) = \sigma(x)$. Verifique que α define uma ação de D_{2n} em Δ_n.

Exemplo 4.15. Considere um grupo G e a função $m\colon G \times G \to G$. Vamos verificar que m define uma ação de G em G:

(i) Pela associatividade de m, para todos $a, b, c \in G$, temos $m(a, m(b, c)) = m(ab, c)$.

(ii) Como e é o elemento neutro de G, para todo $g \in G$, temos $m(e, g) = g$.

Proposição 4.16. *Sejam G um grupo e X um conjunto.*

(a) Se $\alpha\colon G \times X \to X$ é uma ação de G em X, então a função $\varphi_\alpha\colon G \to S_X$ dada por $\varphi_\alpha(g) = \alpha(g, -)$ é um homomorfismo de grupos.
(b) Se $\phi\colon G \to S_X$ é um homomorfismo de grupos, então $\alpha_\phi\colon G \times X \to X$ dada por $\alpha_\phi(g, x) = \phi(g)(x)$ é uma ação de G em X.

Demonstração. (a) Como α é uma ação, para quaisquer $g_1, g_2 \in G$, temos que

$$\varphi_\alpha(g_1) \circ \varphi_\alpha(g_2) = \alpha(g_1, \alpha(g_2, -)) = \alpha(g_1 g_2, -) = \varphi_\alpha(g_1 g_2).$$

Além disso, como α é uma ação, $\varphi_\alpha(e_G) = \alpha(e_G, -) = \mathrm{id}_X$. Juntando esses dois fatos, temos que, para todo $g \in G$,

$$\varphi_\alpha(g) \circ \varphi_\alpha(g^{-1}) = \alpha(gg^{-1}, -) = \mathrm{id}_X = \alpha(g^{-1}g, -) = \varphi_\alpha(g^{-1}) \circ \varphi_\alpha(g).$$

Ou seja, $\varphi_\alpha(g)$ é uma bijeção (com inversa $\varphi_\alpha(g^{-1})$) e φ_α é um homomorfismo de grupos.

(b) Como ϕ é um homomorfismo de grupos, para quaisquer $g_1, g_2 \in G$, temos que

$$\alpha_\phi(g_1, \alpha_\phi(g_2, x)) = \phi(g_1)(\phi(g_2)(x)) = (\phi(g_1) \circ \phi(g_2))(x) = \phi(g_1 g_2)(x) = \alpha_\phi(g_1 g_2, x)$$

para todo $x \in X$. Além disso, $\alpha_\phi(e_G, x) = \phi(e_G)(x) = \mathrm{id}_X(x) = x$ para todo $x \in X$. Isso mostra que α_ϕ é uma ação de G em X. □

Corolário 4.17. *Sejam G, H dois grupos e X um conjunto. Se $f\colon G \to H$ é um homomorfismo de grupos e $\alpha\colon H \times X \to X$ é uma ação de H em X, então a função $\beta\colon G \times X \to X$, dada por $\beta(g, x) = \alpha(f(g), x)$, é uma ação de G em X.*

Demonstração. Pela Proposição 4.16(a), $\varphi_\alpha\colon H \to S_X$ é um homomorfismo de grupos dado por $\varphi_\alpha(h) = \alpha(h, -)$. Pelo Exercício 4.3(c), $(\varphi_\alpha \circ f)\colon G \to S_X$ é um homomorfismo de grupos dado por $(\varphi_\alpha \circ f)(g) = \alpha(f(g), -)$. Pela Pela Proposição 4.16(b), $\alpha_{(\varphi_\alpha \circ f)}\colon G \times X \to X$ é uma ação de G em X dada por $\alpha_{(\varphi_\alpha \circ f)}(g, x) = \alpha(f(g), x)$. Como $\beta = \alpha_{(\varphi_\alpha \circ f)}$, o resultado segue. □

Exemplo 4.18. Sejam G um grupo e X um conjunto. Verifique que a função $\alpha\colon G \times X \to X$ dada por $\alpha(g, x) = x$ para todo $g \in G$, $x \in X$, é uma ação de G em X. (Sugestão: mostre que φ_α é o homomorfismo trivial.) Essa ação é chamada de ação trivial.

Exemplo 4.19. Seja $n \geq 3$. Lembre do Exemplo 4.13 que $\alpha\colon S_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ dada pela permutação dos elementos de $\mathbb{Z}_n$ é uma ação, e lembre do Exemplo 4.7 que $\vartheta\colon D_{2n} \to S_n$ é um homomorfismo de grupos. Verifique que a ação de D_{2n} no conjunto $\mathbb{Z}_n$ (que enumera os vértices de um n-ágono regular Δ_n) é dada por $\alpha_{(\varphi_\alpha \circ \vartheta)}$.