

ÁLGEBRA

TIAGO MACEDO

AULA 1

Avisos: Livro-texto: Abstract Algebra de D. Dummit e R. Foote. (Ler e entender a Seção 0.1.)

1.1. Axiomas e exemplos básicos

Vamos começar com a definição abstrata de grupo.

Definição 1.1. Um **grupo** é um conjunto não-vazio G munido de uma função $m: G \times G \rightarrow G$ (ou seja, uma operação binária) satisfazendo as seguintes condições:

- (i) m é associativa, ou seja, $m(m(a, b), c) = m(a, m(b, c))$ para todos $a, b, c \in G$.
- (ii) Existe $e \in G$ tal que $m(e, g) = g = m(g, e)$ para todo $g \in G$.
- (iii) Para cada $g \in G$ existe $\tilde{g} \in G$ tal que $m(g, \tilde{g}) = e = m(\tilde{g}, g)$.

O elemento e é chamado de **elemento neutro** ou **identidade** de G . O elemento \tilde{g} é chamado de **inverso de g** . Um grupo (G, m) é dito **comutativo** ou **abeliano** quando m é uma operação binária comutativa, ou seja, quando $m(g, h) = m(h, g)$ para todos $g, h \in G$. Um grupo (G, m) é dito **finito** quando $|G|$ (a cardinalidade do conjunto G) é finita.

Agora vamos ver alguns exemplos conhecidos de grupos.

Exemplo 1.2. Considere o conjunto dos números inteiros $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ munido da operação binária $m: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ dada por $m(a, b) = a + b$. Verifique que (\mathbb{Z}, m) é um grupo abeliano. (Encontre explicitamente e e \tilde{g} para cada $g \in \mathbb{Z}$.)

Exemplo 1.3. Considere um espaço vetorial $(V, +, \cdot)$. Verifique que o conjunto V munido da operação binária $+: V \times V \rightarrow V$ é um grupo abeliano. Em particular, os conjuntos dos números racionais \mathbb{Q} , dos números reais \mathbb{R} e dos números complexos \mathbb{C} são grupos abelianos quando munidos de suas somas usuais.

Outra operação binária conhecida em \mathbb{R} é a multiplicação.

Exemplo 1.4. Considere o conjunto \mathbb{R} e a operação binária $m: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ dada por $m(a, b) = ab$. Observe que (\mathbb{R}, m) **não** é um grupo. Apesar de m ser associativa (verifique) e existir elemento neutro (verifique que 1 é o único elemento neutro), não existe o inverso de 0. De fato, $m(a, 0) = 0$ para todo $a \in \mathbb{R}$, portanto não existe $\tilde{0} \in \mathbb{R}$ tal que $m(\tilde{0}, 0) = 1$.

Vamos tentar corrigir o (não-)exemplo anterior.

Exemplo 1.5. Considere o conjunto $\mathbb{R} \setminus \{0\}$ e a operação binária $m: \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R} \setminus \{0\}$ dada por $m(a, b) = ab$. Observe que m está bem definida, pois $ab = 0$ se, e somente se, $a = 0$ ou $b = 0$. Verifique que $(\mathbb{R} \setminus \{0\}, m)$ é um grupo abeliano.

Exemplo 1.6. Considere o conjunto $\mathbb{Z} \setminus \{0\}$ e a operação binária $m: \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{Z} \setminus \{0\}$ dada por $m(a, b) = ab$. Verifique que m está bem definida, é associativa, e 1 é o único elemento neutro de $\mathbb{Z} \setminus \{0\}$. Mas $(\mathbb{Z} \setminus \{0\}, m)$ **não** é um grupo, pois, se $g \notin \{-1, 1\}$, então não existe $\tilde{g} \in \mathbb{Z} \setminus \{0\}$ tal que $g\tilde{g} = 1$.

Nós podemos corrigir o (não-)exemplo anterior de duas formas. A primeira é incluir todos os inversos dos números inteiros não-nulos e todos os produtos entre números inteiros e inversos de inteiros não-nulos (ou seja, todos os números racionais).

Exemplo 1.7. Considere o conjunto $\mathbb{Q} \setminus \{0\}$ e a operação binária $m: \mathbb{Q} \setminus \{0\} \times \mathbb{Q} \setminus \{0\} \rightarrow \mathbb{Q} \setminus \{0\}$ dada por $m(a, b) = ab$. Verifique que $(\mathbb{Q} \setminus \{0\}, m)$ é um grupo abeliano.

A segunda é excluir todos os inteiros não-nulos que não têm inversos multiplicativos.

Exemplo 1.8. Considere o conjunto $G = \{-1, 1\}$ e a operação binária $m: G \times G \rightarrow G$ dada por $m(a, b) = ab$. Verifique que m está bem definida e que (G, m) é um grupo abeliano finito.

Pelo Exemplo 1.3, o conjunto de matrizes n por n com entradas reais, $M_n(\mathbb{R})$ é um grupo abeliano quando munido da soma usual de matrizes. Outra operação binária bem conhecida em $M_n(\mathbb{R})$ é o produto de matrizes.

Exemplo 1.9. Observe que $M_n(\mathbb{R})$ munido do produto usual de matrizes **não** é um grupo. De fato, apesar do produto ser associativo e da matriz identidade ser um elemento neutro para essa operação, nem todas as matrizes têm inversos multiplicativos (por exemplo, a matriz nula). Então denote por $GL_n(\mathbb{R})$ o conjunto de matrizes invertíveis de $M_n(\mathbb{R})$ e considere a operação binária $m: GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R})$ dada por $m(A, B) = AB$. Verifique que $(GL_n(\mathbb{R}), m)$ é um grupo e que esse grupo **não** é abeliano.

Proposição 1.10. *Seja (G, m) um grupo.*

- (a) *Existe um único elemento neutro em G .*
- (b) *Para cada $g \in G$ existe um único elemento inverso.*
- (c) *Para todo $g \in G$ o elemento inverso de \tilde{g} (o inverso de g) é g .*
- (d) *Para todos $g, h \in G$, $m(g, h) = m(\tilde{h}, \tilde{g})$.*
- (e) *Dados $a, b \in G$, existe um único $x \in G$ tal que $m(a, x) = b$.*
- (f) *Dados $a, b \in G$, existe um único $x \in G$ tal que $m(x, a) = b$.*
- (g) *Se $a, b, c \in G$ são tais que $m(a, b) = m(a, c)$, então $b = c$.*
- (h) *Se $a, b, c \in G$ são tais que $m(b, a) = m(c, a)$, então $b = c$.*

Demonstração. (a) Pela Definição 1.1(ii), existe pelo menos um elemento neutro em G . Suponha que $e, e' \in G$ sejam tais que $m(e, g) = g = m(g, e)$ e $m(e', g) = g = m(g, e')$ para todo $g \in G$. Então temos que $e = m(e, e') = e'$. Isso mostra a unicidade do elemento neutro.

(b) Pela Definição 1.1(iii), para cada $g \in G$, existe pelo menos um elemento inverso para g . Suponha que $\tilde{g}, \tilde{g}' \in G$ sejam tais que $m(g, \tilde{g}) = e = m(\tilde{g}, g)$ e $m(g, \tilde{g}') = e = m(\tilde{g}', g)$. Então temos que $\tilde{g} = m(\tilde{g}, e) = m(\tilde{g}, m(g, \tilde{g}')) = m(m(\tilde{g}, g), \tilde{g}') = m(e, \tilde{g}') = \tilde{g}'$. Isso mostra a unicidade do inverso de g .

(c) Fixe $g \in G$. Pela Definição 1.1(iii) e item (b), o inverso de \tilde{g} é o único $x \in G$ que satisfaz $m(\tilde{g}, x) = e = m(x, \tilde{g})$. Também pela Definição 1.1(iii), \tilde{g} satisfaz $m(g, \tilde{g}) = e = m(\tilde{g}, g)$. Ou seja, g é o (único) inverso de \tilde{g} .

(d) Fixe $g, h \in G$. Pela Definição 1.1(iii) e item (b), o inverso de $m(g, h)$ é o único $x \in G$ que satisfaz $m(m(g, h), x) = e = m(x, m(g, h))$. Vamos mostrar que $x = m(\tilde{h}, \tilde{g})$ satisfaz essas equações.

$$\begin{aligned}
 m(m(g, h), m(\tilde{h}, \tilde{g})) &= m(m(m(g, h), \tilde{h}), \tilde{g}) & m(m(\tilde{h}, \tilde{g}), m(g, h)) &= m(m(m(\tilde{h}, \tilde{g}), g), h) \\
 &= m(m(g, m(h, \tilde{h})), \tilde{g}) & &= m(m(\tilde{h}, m(\tilde{g}, g)), h) \\
 &= m(m(g, e), \tilde{g}) & &= m(m(\tilde{h}, e), h) \\
 &= m(g, \tilde{g}) & &= m(\tilde{h}, h) \\
 &= e, & &= e.
 \end{aligned}$$

(e) Observe que, se $m(a, x) = b$, então $m(\tilde{a}, b) = m(\tilde{a}, m(a, x)) = m(m(\tilde{a}, a), x) = m(e, x) = x$. Por outro lado, $m(a, m(\tilde{a}, b)) = m(m(a, \tilde{a}), b) = m(e, b) = b$. Como $m(\tilde{a}, b) \in G$ e \tilde{a} é único, então $x = m(\tilde{a}, b)$ é o único elemento de G que satisfaz $m(a, x) = b$.

(f) Similar à do item (e).

(g) Segue do item (e) substituindo x por b e b por $m(a, c)$.

(h) Segue do item (f) substituindo x por b e b por $m(c, a)$. □

Observação 1.11. A definição de grupo é completamente abstrata. Ou seja, um grupo é um conjunto não-vazio qualquer, munido de uma operação binária qualquer, desde que essa operação binária satisfaça as condições (i)-(iii) da Definição 1.1. Em particular, podemos criar um grupo a partir de um conjunto $G \neq \emptyset$ qualquer, se especificarmos toda uma *tabela de multiplicação*

G	e	g	h	\dots
e	e	g	h	\dots
g	g	$?$	$??$	\dots
h	h	$???$		
\vdots	\vdots	\vdots		

satisfazendo as condições (i)-(iii).

Além disso, é fácil ver que existe uma quantidade enorme de grupos (não só os que nós exemplificamos acima). Portanto um problema interessante seria descrever todos os possíveis grupos que existem e classificá-los.