



UNIVERSIDADE DE SÃO PAULO

INSTITUTO DE CIÊNCIAS MATEMÁTICAS E COMPUTACIONAIS - ICMC

# Notas de Aula de Álgebra

**Renan Wenzel - 11169472**

**Roberto Carlos - alvarago@icmc.usp.br**

16 de março de 2023

# Conteúdo

# 1 Aula 01 - 14/03/2023

## 1.1 Motivações

- Compreender o que será estudado ao longo do curso;

## 1.2 Introdução ao Curso

Este curso é sobre teoria de grupos, a qual possui origem no estudo de simetrias, sejam elas de figuras ou de objetos algébricos. Um exemplo de grupo seria o seguinte:

Considere um triângulo equilátero. Existem algumas formas de olharmos para as simetrias do triângulo, como rotacionando-o, refletindo-o com relação a um ponto médio e um vértice fixo. Contabilizando todas as possíveis formas delas acontecerem, há seis simetrias deste retângulo. Ademais, compondo simetrias resulta em outra, i.e., rotacionar e refletir um certo vértice continuará sendo uma simetria do triângulo. Além disto, é um fato (futuramente visto) que essas seis simetrias totalizam todas as possíveis simetrias de um triângulo equilátero. De fato, dado um polígono regular de n lados, ele possui n! simetrias.

## 1.3 Grupos e Operações

**Definição.** *Seja $S$ um conjunto não-vazio. Uma operação em $S$ é um mapa*

$$\begin{aligned}\mu :& S \times S \to S \\ & (a, b) \mapsto \mu(a, b)\end{aligned}$$

**Exemplo 1.** *A operação soma em $\mathbb{Z}, + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b$ é uma operação.*

**Exemplo 2.** *Uma operação em $\mathbb{R}$ é a multiplicação $. : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a, b) \mapsto ab$.*

**Exemplo 3.** *Um exemplo do que não é operação seria a subtração dos naturais, $- : \mathbb{N}\times\mathbb{N} \to \mathbb{N}, (a, b) \mapsto a-b$. (Consegue responder por que não é?)*

**Exemplo 4.** *Se $S$ é o conjunto de simetrias de um triângulo equilátero, então a composição*

$$\begin{aligned}\circ :& S \times S \to S \\ & (\sigma, \tau) \mapsto \sigma \circ \tau\end{aligned}$$

*é uma operação binária.*

Faremos a convenção de denotar $\mu(a, b)$ por $a.b$ ou $a + b$, com base no contexto.

**Definição.** *Uma operação $\mu$ em $S$ não-vazio, denotada pelo produto, é dita associativa se, para todos a, b, c em $S$,*

$$(a.b).c = a.(b.c), \quad \Big(\mu(a, \mu(b, c)) = \mu(\mu(a, b), c)\Big).$$

*Por outro lado, será dita comutativa se*

$$a.b = b.a, \quad \Big(\mu(a, b) = \mu(b, a)\Big).$$

*Diremos, também, que ela tem elemento neutro (ou identidade) se existe um elemento $e$ em $S$ tal que*

$$a.e = e.a = a, \forall a \in S.$$

*Neste caso, diremos que $e$ é o elemento neutro, ou a identidade, para $\mu$.*

Utilizaremos a notação 1 para a identidade no caso em que $\mu$ é denotada por um produto e 0 pro caso em que é denotada por adição.

**Exemplo 5.** *A multiplicação de matrizes é associativa, não é comutativa e possui identidade.*

**Exemplo 6.** *A soma de números inteiros é associativa, comutativa e possui identidade.*

**Exemplo 7.** *A potência nos números reais é não associativa, nem comutativa, mas possui identidade:* $a^{(b^c)} \neq (a^b)^c = a^{bc}$

**Proposição.** *Seja S um conjunto não-vazio e $\mu$ uma operação em S denotada pelo produto. Então, existe um único jeito de definir o produto (denotado temporariamente por $[a_1, \cdots, a_n]$) de n elementos em S tal que*

$$(i) \quad [a_1] = a_1;$$
$$(ii) \quad [a_1, a_2] = \mu(a_1, a_2) = a_1 a_2;$$
$$(iii) \quad \forall 1 \leq i < n, [a_1, \cdots, a_n] = [a_1, \cdots, a_i][a_{i+1}, \cdots, a_n].$$

**Prova.** *(iii)⇒ Para o caso $n \leq 2$ é ok. Agora, suponha o produto bem-definido de r elementos em S, $r \leq n = 1$. Então, defina $[a_1, \cdots, a_n]coloneqq[a_1, \cdots, a_{n-1}][a_n]$. Como a definição acima satisfaz a condição (iii) para i=n-1, se ela estiver bem-definida, ela será única. Com efeito, seja $1 \leq i < n-1$, tal que*

$$\begin{aligned}[a_1, \cdots, a_n] &= [a_1, \cdots, a_{n-1}][a_n] = [a_1, \cdots, a_i][a_{i+1}, \cdots, a_{n-1}][a_n] \\ &= \Big([a_1, \cdots, a_i]\Big)\Big([a_{i+1}, \cdots, a_{n-1}][a_n]\Big) \\ &= [a_1, \cdots, a_i][a_{i+1}, \cdots, a_n]. \blacksquare\end{aligned}$$

**Definição.** *Seja S não-vazio e $\mu$ uma operação em S com identidade 1. Um elemento a de S é dito inversível se existe b em S tal que $ab = ba = 1$. Neste caso, b é o inverso de a, denotado por $bcoloneqqa^{-1}$.*

Note que tanto o elemento inverso quanto o elemento neutro, se existirem, são únicos (c.f. Lema abaixo). Além disso, o inverso da adição é denotad por -a.

**Lema.** *Seja S não-vazio, $\mu$ uma operação associativa denotada pelo produto. Então,*

*i) Existe no máximo um elemento neutro para S e $\mu$;*

*ii) Se o elemento neutro existe, então para cada elemento de S, existe no máximo um inverso;*

*iii) Se um elemento a de S tem inverso à esquerda l e à direita r, i.e. $l.a = 1$ e $a.r = 1$, então a é inversível com inverso $l = r$.*

*iv) Se a, b em S são inversíveis, então o produto ab é inversível, com inverso $b^{-1}a^{-1}$.*

Antes de provar, observe que a existência de um elemento inverso à esquerda ou à direita não garante que um elemento seja inversível (exercício), eles devem coincidir.

**Prova.** *(i) ⇒) Suponha que existem 1, 1' em S como seus elementos neutros. Basta mostramos que eles coincidem. Com efeito,*

$$1 = 1.1' = 1'.1 = 1'.$$

*Portanto, o elemento neutro é único. (ii) ⇒) Assuma a existência de dois elementos inversos em S para um elemento a, denotados por b, b'. Então, como ab = ba = 1, temos*

$$b = b1 = b(ab') = (ba)b' = 1b' = b'.$$

*Portanto, o elemento inverso é único. Os itens (iii) e (iv) são exercícios.* $\blacksquare$

**Definição.** *Um monoide é um par (G, $\mu$), em que G é um conjunto não-vazio e $\mu$ uma operação associativa e com elemento neutro em G. Se, ainda por cima, $\mu$ for comutativa, (G, $\mu$) é um monoide abeliano (ou comutativo).*

**Definição.** *Um grupo é um par (G, $\mu$) é um monoide (G, $\mu$) com a condição extra que todo elemento de G possui inverso. Caso $\mu$ seja comutativa, chamamos G de grupo abeliano.*

**Exemplo 8.** *Os inteiros com a soma, $(\mathbb{Z}, +)$, é um grupo comutativo, enquanto $(\mathbb{Z}, .)$ não é um grupo, mas sim um monoide.*

**Exemplo 9.** *O grupo das matrizes com entradas reais e sua multiplicação, $(\mathbb{M}_n(\mathbb{R}), .)$, é um grupo não-abeliano.*

# 2 Aula 02 - 16/03/2023

## 2.1 Motivações

- Outras estruturas algébricas e exemplos;
- Tamanho de um grupo;
- Subgrupos

## 2.2 Usos de Grupos

Podemos usar grupos para definir outras construções algébricas, como segue.

**Definição.** *Um anel é uma terna $(A, \mu, \phi)$, em que $(A, \mu)$ é um grupo abeliano e $(A, \phi)$ é um monoide. Além disso, vale a distributiva.*

$$\phi(a, \mu(c, d)) = \phi(\mu(a, c), \mu(a, d)), \quad (a(b + c) = ab + ac).$$

*Usualmente, escrevemos $(A, \mu, \phi) = (A, +, .)$.* □

**Definição.** *Um corpo é um anel $(A, +, .)$ tal que $(A - \{0\}, .)$ é um grupo abeliano.* □

Deste ponto em diante, abandonaremos as letras gregas para usar apenas os símbolos "+" ou "." para um grupo com adição ou com multiplicação. Vejamos alguns exemplos.

**Exemplo 10.**

| *Conjunto* | *Monoide* | *Monoide Comutativo* | *Grupo* | *Grupo Comutativo* |
|---|---|---|---|---|
| $(GL_n, .)$ | *Sim* | *Sim* | *Sim* | *Não* |
| $(SL_n, .)$ | *Sim* | *Não* | *Sim* | *Não* |
| $(\mathbb{Z}, +)$ | *Sim* | *Sim* | *Sim* | *Sim* |
| $(\mathbb{Z}, .)$ | *Sim* | *Sim* | *Não* | *Não* |
| $(\mathbb{Q}, +)$ | *Sim* | *Sim* | *Sim* | *Sim* |
| $(\mathbb{Q}, .)$ | *Sim* | *Sim* | *Não* | *Não* |
| $(S = \{z \in \mathbb{C} : \lvert z\rvert = 1\}, .)$ | *Sim* | *Sim* | *Sim* | *Sim* |
| $(\mathbb{M}_n(\mathbb{R}), +)$ | *Sim* | *Sim* | *Sim* | *Sim* |
| $(\mathbb{M}_n(\mathbb{R}), .)$ | *Sim* | *Não* | *Não* | *Não* |

■

**Exemplo 11.** *Seja $T$ um conjunto qualquer e*

$$G = \{f : T \to T : f \text{ bijetora.}\}$$

*Então, $(G, \circ)$ é um grupo, chamado grupo das permutações ou simetrias de $T$. Se $T$ é um conjunto finito, e.g. $T = \{1, \cdots, n\}$, então denotamos $(G, \circ)$ por $(S_n, \circ)$.* ■

**Definição.** *A ordem de um grupo $(G, \cdot)$ é a cardinalidade de $G$: $|G|$. Caso $|G| < \infty$, dizemos que $(G, +)$ é um grupo finito.* □

**Exemplo 12.** *A ordem de $|\mathbb{Z}| = \infty$ e $|S_n| = n!$* ■

**Proposição.** *Se $(G, \cdot)$ é um grupo e $a$, $b$, $c$ são elementos de $G$ tais que $ab = ac$ ou $ba = ca$, então $b = c$. Além disso, se $ab = a$ ou $ba = a$, então $b = 1$.*

**Prova.** *Seja $a^{-1}$ o inverso de $a$, então $a^{-1}(ab) = a^{-1}(ac)$. Mais ainda, se $ab = a$, então $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}a = 1$.*

Fica de exercício mostrar que só existe um grupo de ordem 2 e que $S_3$ é um grupo não-comutativo.

## 2.3 Subgrupos

**Definição.** *Um subgrupo $H$ de um grupo $(G, \cdot)$ é um subconjunto $H$ de contido em $G$ tal que*

$$1) 1 \in H;$$
$$2) a, b \in H \Rightarrow ab \in H;$$
$$3) a \in H \Rightarrow a^{-1} \in H.$$

*Denotaremos subrupos por $H \leq G$ ou $(H, \cdot) \leq (G, \cdot)$.*□

**Proposição.** *Com operação induzida pela multiplicação de $G$ restrita a $H$, $(H, \cdot)$ é um grupo.*

**Prova.** *Como $H$ está contido em $G$, podemos restringir o produto de $G$ a $H$ para*

$$._H : H \times H \to H.$$

*Afirmamos que $(H, \cdot)$ é um grupo. Com efeito, a restrição de . a $H$ está bem-definida pelo segundo item da definição de subgrupo. Mais ainda, ela é associativa em $H$ por ser em $G$ e todo elemento em $H$ tem inverso pela condição 3. Por fim, ela tem elemento neutro pela primeira requisição ao definir subgrupo. Portanto, $(H, \cdot)$ é um grupo.*

Observe que todo grupo tem ao menos dois subgrupos, chamados triviais, sendo eles $\{1\}$ e ele mesmo. Qualquer outro leva o nome de subgrupo próprio.

**Exemplo 13.** $(SL_n, \cdot) \leq (GL_n, \cdot)$ *e* $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$. ■

**Exemplo 14.** *Seja $n$ um inteiro, então $n\mathbb{Z} \coloneqq \{nk : k \in \mathbb{Z}\}$ é um subgrupo dos inteiros. De fato, 0 = n0 pertence a $n\mathbb{Z}$. Além disso, se nk e nk' pertencem a $n\mathbb{Z}$, então*

$$nk + nk' = n(k + k') \in n\mathbb{Z}.$$

*Por fim, se nk pertence a $n\mathbb{Z}$, então n(-k) também pertence a $n\mathbb{Z}$ e nk + n(-k) = 0.* ■

**Proposição.** *Todo subgrupo de $(\mathbb{Z}, +)$ é da forma $n\mathbb{Z}$ para algum $n$ inteiro.*

**Prova.** *Caso $n$ seja 1, $n\mathbb{Z} = \mathbb{Z}$ e, se $n = 0$, então $n\mathbb{Z} = \{0\}$. Agora, seja $H$ um subgrupo próprio dos inteiros e $n$ o menor inteiro positivo em $H$. Afirmamos que $n\mathbb{Z} = H$.*

*De fato, $n\mathbb{Z} \leq H$, pois $n$ é um elemento de $H$, então $nk = \underbrace{n + \ldots + n}_{k\text{-vezes}} \in H$. Além disso, $-n \in H$, de forma que $-nk = \underbrace{(-n) + \ldots + (-n)}_{k\text{-vezes}} \in H$. Portanto, $n\mathbb{Z} \in H$.*

*Por outro lado, seja $m$ um inteiro de $H$ e considere $m = nq + r, 0 \leq r < n, q \in \mathbb{Z}$. Pelo algoritmo de divisão de Euclides,*

$$m - nq = r \Rightarrow r \in H \Rightarrow r = 0.$$

*e, assim, $m = nq$ pertence a $n\mathbb{Z}$. Portanto, $H = n\mathbb{Z}$.* ■

**Proposição.** *1) $n\mathbb{Z} + m\mathbb{Z}$ é subgrupo de $\mathbb{Z}$;*

*2) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, em que $d$ é tal que*

*2.1) $d|n$ e $d|m$;*

*2.2) Se $l|n$ e $l|m$, então $l|d$;*

*2.3) Existem $r$, $s$ inteiros tais que $rn + sm = d$.*

*Definimos $d = \gcd(n, m)$ como o máximo divisor comum de $m$ e $n$.*

**Prova.** *A prova do item 1 fica como exercício.*
2.1) $\Rightarrow$ *$n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. Em particular, se $n$, $m$ pertencem a $d\mathbb{Z}$, então $d|n$ e $d|m$.*
2.2) $\Rightarrow$ *Suponha que $n = lq_1, m = lq_2$. Se $x$ pertence a $n\mathbb{Z} + m\mathbb{Z}$, então*

$$x = nk_1 + mk_2 = lq_1k_1 + lk_2q_2 \in l\mathbb{Z}$$
$$\Rightarrow n\mathbb{Z} + m\mathbb{Z} \subseteq l\mathbb{Z} \Rightarrow l|d.$$

*também é possível mostrar isso usando o item 3 da proposição.*
2.3) $\Rightarrow$ *imediato.* ■

**Proposição.** *1) $m\mathbb{Z} \cap n\mathbb{Z}$ é subgrupo dos inteiros;*

*2) $m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$, em que $l$ é tal que*

*2.1) $m|l, n|l$;*

*2.2) Se $m|l'$ e $n|l'$, então $l|l'$.*
*Definimos $l = mmc(m, n)$ o mínimo múltiplo comum de $m$ e $n$.*

**Prova.** *Fica como exercício.*

**Corolário.** *Se $m$, $n$ são inteiros, então $mn = mmc(m, n) \gcd(m, n)$.*