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

15 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 μ 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 μ.

Utilizaremos a notação 1 para a identidade no caso em que μ 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 μ 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 μ 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 $b coloneqq a^{-1}$.*

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, μ uma operação associativa denotada pelo produto. Então,*

i) Existe no máximo um elemento neutro para S e μ;

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

Definição. *Um grupo é um par (G, μ) é um monoide (G, μ) com a condição extra que todo elemento de G possui inverso. Caso μ 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.*