

PROF. MAURÍCIO ZAHN

wp.ufpel.edu.br/zahn

O plano de ensino, bem como datas das provas e materiais extras estarão disponíveis na pág. de disciplina.

Nesta disciplina estudaremos grupos, subgrupos e homomorfismos de grupos.

OPERAÇÕES:

Def.: Seja G um conjunto não vazio. Chama-se operação em G toda função

$$\varphi: G \times G \rightarrow G.$$

$$(a, b) \mapsto \varphi(a, b) = a * b$$

↑
ESTE SÍMBOLO
DENOTA A
OPERAÇÃO
EM G

EXEMPLOS:

(a) Tome $G = \mathbb{N} := \{1, 2, 3, 4, \dots\}$ e defina a operação:

$$\varphi: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$(a, b) \mapsto a + b,$$

ou seja, dado, $a, b \in \mathbb{N}$, $\varphi(a, b) = a + b$

denota a soma dos números naturais a e b .
(chamada de operação de adição)

(b) $G = \mathbb{N}$ e tome a operação

$$\rho: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N},$$

definida por:

$$\rho(a, b) = a^b,$$

que chamamos de operação de potenciação.

(c) $G = \{f: \mathbb{R} \rightarrow \mathbb{R} ; f \text{ é uma função}\}$ o conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$.

Defina em G a operação:

$$\varphi: G \times G \rightarrow G.$$

$$\varphi(f, g) = f \circ g, \quad ,$$

chamada de operação de composição de funções,

ou seja: $\forall x \in \mathbb{R}$; dados $f, g \in G$; então:

$$(f \circ g)(x) = f(g(x))$$

(d) $G = M_n(\mathbb{R})$ o conjunto de matrizes

quadradas $n \times n$. Defina a operação

$$\varphi: G \times G \rightarrow G \quad \text{por}.$$

$$\varphi(A, B) = A \cdot B, \quad ,$$

ou seja, a operação de produto de matrizes.

Def.: Seja G um conjunto não vazio e $*$ uma operação ^(*) em G . Dizemos que a operação $*$ é associativa em G se, $\forall a, b, c \in G$,
$$a * (b * c) = (a * b) * c$$

Exemplos: 01) Em $\mathbb{Z}$, a operação de adição
$$+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$$
$$(x, y) \mapsto x + y$$

é associativa:

$$a + (b + c) = (a + b) + c.$$

02) Sendo $G = M_m(\mathbb{R})$ a operação de produto de matrizes é associativa; ou seja, dados as matrizes $A, B, C \in G$, tem-se que
$$A \cdot (B \cdot C) = (A \cdot B) \cdot C.$$

(*) ou seja, $* : G \times G \rightarrow G$
$$(a, b) \mapsto a * b$$

03) $G = \mathbb{N}$ a operação de potência
 $p(a,b) = a^b$ é associativa?

Não, pois, por exemplo:

$$(2^3)^2 = 8^2 = 64 ; \text{ mas:}$$

$$2^{(3^2)} = 2^9 = 512$$

$$\Rightarrow (2^3)^2 \neq 2^{(3^2)}$$

Def. 1: Seja G um conjunto não vazio e $*$ uma operação em G . Dizemos que um elemento $e \in G$ é o neutro à esquerda se, $\forall x \in G$;

$$e * x = x.$$

Do mesmo modo, dizemos que um elemento $\tilde{e}$ é um neutro à direita em G se, $\forall x \in G$,

$$x * \tilde{e} = x$$

Quando o neutro à esquerda e à direita forem o mesmo, chamemos simplesmente de neutro para a operação $*$ em G :

$$\forall x \in G;$$
$$e * x = x * e = x.$$

Exemplos:

01) Em $\mathbb{Z}$, temos que 0 é o neutro para a operação de adição, pois, $\forall x \in \mathbb{Z}$:

$$0 + x = x + 0 = x.$$

chamado de neutro aditivo.

02) Em $M_n(\mathbb{R})$, temos que a matriz identidade I_n é o neutro para a operação de produto entre matrizes; ou seja, $\forall A \in M_n(\mathbb{R})$

$$I_n \cdot A = A = A \cdot I_n$$

03) $G = \{ f: \mathbb{R} \rightarrow \mathbb{R} \}$ contém a função identidade $\text{id}: \mathbb{R} \rightarrow \mathbb{R}$

$$\text{id}(x) = x,$$

e é o elemento neutro para a operação de composição de funções, ou seja; $\forall f \in G$, tem-se:

$$\text{id} \circ f = f \quad \text{e} \quad f \circ \text{id} = f.$$


$$\forall x \in \mathbb{R} \quad \underline{(\text{id} \circ f)(x)} = \text{id}(f(x)) = \underline{f(x)}$$


$$\forall x \in \mathbb{R} : \underline{(f \circ \text{id})(x)} = f(\underline{\text{id}(x)}) = \underline{f(x)}$$

Proposição: Seja G um conjunto não vazio equipado com uma operação $*$. O elemento neutro para esta operação em G , se existir, é único.

DEMONSTRAÇÃO: sejam e e $\tilde{e}$ neutros para a operação $*$ em G . Então:

$$\underbrace{e}_{\text{pois } \tilde{e} \text{ é neutro}} = \tilde{e} * e = \underbrace{\tilde{e}}_{\text{pois } e \text{ é neutro}} \Rightarrow e = \tilde{e}$$

□

Def.: Dizemos que uma operação $*$ em um conjunto não vazio G é comutativa se, $\forall a, b \in G$,
 $a * b = b * a$.

Ex.: 01) $G = M_n(\mathbb{R})$, a operação " $\cdot$ " é produto de matrizes, não é comutativa, pois,
 $\forall A, B \in G$, tem-se, em geral, que
 $A \cdot B \neq B \cdot A$.

02) Em $G = \{f: \mathbb{R} \rightarrow \mathbb{R}\}$, a operação " $\circ$ " é composição de funções, em geral, não é

comutativa, ou seja; $\forall f, g \in G$:
 $f \circ g \neq g \circ f$.

03) $G = \mathbb{N}$ e "+" a operação de adição em $\mathbb{N}$, temos que, $\forall a, b \in \mathbb{N}$;

$$a + b = b + a$$

ou seja, a adição em $\mathbb{N}$ é comutativa.

Def.1 Seja $*$ uma operação definida em um conjunto não vazio G . Diremos que um elemento $x \in G$ é simetrizável se $\exists y \in G$

tal que $x * y = e$ e $y * x = e$;
onde e denota o elemento neutro de para a operação $*$ em G .

Exemplos:

01) $G = \mathbb{Z}$ equipado com a operação de adição em $\mathbb{Z}$. Então, $\forall x \in \mathbb{Z}, \exists -x \in \mathbb{Z}$

$$\text{tal que } x + (-x) = 0;$$

onde 0 é o elemento neutro para a adição em $\mathbb{Z}$.

Conclusão: em $\mathbb{Z}$, com a adição, todo elemento é simetrizável.

02) $G = \mathbb{Z}$, equipado com a operação de multiplicação em $\mathbb{Z}$. $(a, b) \mapsto a \cdot b$

Neste caso, o neutro multiplicativo é 1.

$$\text{Iremos, em } \mathbb{Z}, \quad x \cdot y = 1 \Leftrightarrow \begin{cases} x = y = 1 \\ \text{ou} \\ x = y = -1. \end{cases}$$

Outro seja, em $\mathbb{Z}$, equipado com o produto, apenas 1 e -1 são simetrizáveis; onde o simétrico de 1 é ele próprio, pois

$$1 \cdot 1 = 1 \quad ;$$

e o simétrico de -1 é ele próprio, pois
 $(-1) \cdot (-1) = 1$.

NOTAÇÃO: Quando a operação em G for
multiplicativa, o simétrico de x , existindo,
é chamado de inverso e denotado por x^{-1} .

Assim, usa-se a notação:

$$x \cdot x^{-1} = 1 \quad \text{e} \quad x^{-1} \cdot x = 1.$$

PROPOSIÇÃO: Seja G um conjunto não vazio, equi-
pado por uma operação $*$, associativa.
Então, se $x \in G$ for simetrizável, o seu simétrico é
único.

DEMONSTR.: Seja $x \in G$ simetrizável.

Considere $\alpha, \beta \in G$ simétricos para $x \in G$.

Vamos mostrar que $\alpha = \beta$.

Como α é simétrico para x , então

$$\alpha * x = e \quad \text{e} \quad \underline{x * \alpha = e},$$

onde e denota o neutro para $*$ em G .

Do mesmo modo, como β é simétrico para α , tem-se que

$$\beta * \alpha = e \quad \text{e} \quad \alpha * \beta = e.$$

Assim, observando que $*$ é associativa, por hipótese, temos que:

$$\alpha = \underline{e * \alpha} = (\underbrace{\beta * \alpha}_e) * \alpha = \beta * (\underbrace{\alpha * \alpha}_e) = \beta * e = \beta;$$

↑
pois $*$ é associativa.

ou seja, acabamos de mostrar que $\alpha = \beta$, como desejávamos. □

REPRESENTAÇÃO DE OPERAÇÕES EM TÁBUAS

Quando o conjunto G for finito (e com poucos elementos) é possível montar uma tabela com a operação dada como segue: seja

$G = \{g_1, g_2, \dots, g_k\}$, equipado com uma

operação $*$. Disponibilizamos os k elementos de G em uma linha e em uma coluna, e os "cruzamentos" com a operação $*$.

$*$	g_1	g_2	g_3	$\dots$	g_k
g_1					
g_2					
g_3					
$\vdots$					
g_k					

nesta posição registramos $g_1 * g_2$

nesta posição registramos $g_2 * g_1$

aqui registramos $g_2 * g_3$

Vejaamos um exemplo:

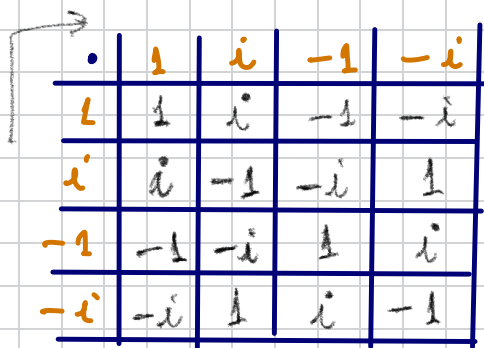
ex.: Tome $i = \sqrt{-1}$ a unidade imaginária e considere $G = \{1, i, -1, -i\}$, equipado com a operação de produto entre números complexos:

$$(a+bi) \cdot (c+di) = (a \cdot c - bd) + (ad + bc)i$$

O que nos interessa nesse produto é:

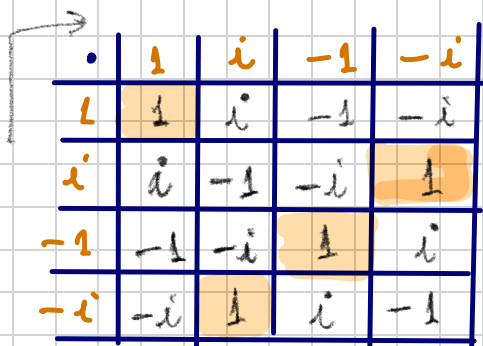
$$i^2 = -1; \quad ; \quad i^0 = 1; \quad ; \quad i^1 = i$$

Montemos a tabela do produto:



•	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Note que, em cada linha dessa tabela consta o neutro multiplicativo 1:



•	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

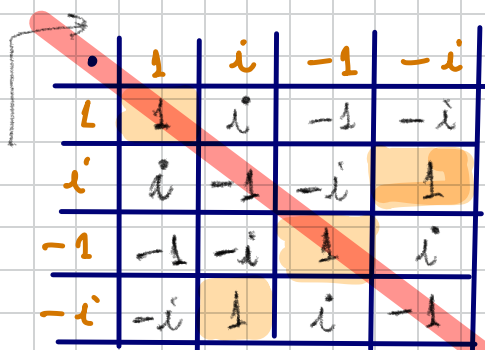
Disto, segue que todo elemento é simétrico.

O simétrico de 1 é 1;
pois $1 \cdot 1 = 1$;

o simétrico de i é -i, pois $i \cdot (-i) = 1$;

o simétrico de -1 é -1, pois $(-1) \cdot (-1) = 1$;

e o simétrico de -i é i pois $(-i) \cdot (-i) = 1$.



•	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Observando a diagonal desta tabela vemos que um lado é o "espelho" do outro, o que mostra que G é COMUTATIVO

ou seja, $\forall a, b \in G$;
 $a \cdot b = b \cdot a$.

GRUPOS:

Def.: Chama-se grupo um conjunto não vazio equipado por uma operação $*$ que é associativa, possui neutro e simétrizável.

Mais precisamente, chama-se grupo G munido da operação $*$, denotado por $(G, *)$,

$$G \times G \longrightarrow G$$

$$(a, b) \mapsto a * b,$$

tal que; $\forall a, b, c \in G$, tem-se:

$$(i) \quad a * (b * c) = (a * b) * c \quad (\text{ASSOCIATIVIDADE})$$

$$(ii) \quad \exists e \in G \text{ tal que } a * e = a = e * a$$

(existência do elemento neutro)

$$(iii) \quad \forall x \in G, \exists x^{-1} \in G \text{ tal que}$$
$$x * x^{-1} = e = x^{-1} * x.$$

(todo elemento é simétrizável)

De além disso, tivermos:

$$(iv) \quad a * b = b * a ;$$

então o grupo é chamado de grupo comutativo ou grupo ABELIANO. Do contrário, é um grupo não-comutativo ou não abeliano.