Centro Paula Souza	CENTRO PAULA SOUZA	18/08/2022 29/08/2022
	MAG004 — ÁLGEBRA LINEAR MAT006 — MATEMÁTICA DISCRETA	HENRIQUE FURIA SILVA

Aula 02 Grupos, Anéis e Corpos

I — Grupos algébricos

[1] Definição: Seja $(\mathbb{G})$ um conjunto não vazio e $(*)$ uma operação binária em $(\mathbb{G})$:

$*:$	$\mathbb{G}\times\mathbb{G}$	$\longrightarrow$	$\mathbb{G}$
	(a,b)	$\longmapsto$	$*\,(a,b) \overset{\text{def}}{=} a*b$

Observe que uma operação binária é simplesmente uma função de duas variáveis em que cada elemento na entrada está no conjunto $(\mathbb{G})$, e o resultado da operação também está no conjunto.

O par $(\mathbb{G},*)$ é denominado um grupo se para cada para cada $\{a;b;c\}\subset\mathbb{G}$, a operação $(*)$ satisfizer os axiomas:

$(G1)$	Associatividade	$a*(b*c)=(a*b)*c$		
$(G2)$	Existência do elemento neutro $(e_{\mathbb{G}})$	$e_{\mathbb{G}}*a=a$	&	$a*e_{\mathbb{G}}=a$
$(G3)$	Existência do elemento inverso (h_a)	$a*h_a=e_{\mathbb{G}}$	&	$h_a*a=e_{\mathbb{G}}$

[2] Definição: Um grupo é dito ser **abeliano** se for comutativo, isto é:

$(G4)$	Comutatividade	$a*b=b*a$	

[3] Observação: Grupos abelianos são representados por $(\mathbb{G},+)$, seu elemento neutro é representado por $(0_{\mathbb{G}})$, o elemento inverso de cada $(a\in\mathbb{G})$ é representado por $(-a)$ e a sua operação $(+)$ satisfaz às propriedades:

$(A1)$	Associatividade da soma	$a+(b+c)=(a+b)+c$		
$(A2)$	Existência do elemento neutro $(0_{\mathbb{G}})$	$0_{\mathbb{G}}+a=a$	&	$a+0_{\mathbb{G}}=a$
$(A3)$	Existência do elemento oposto $(-a)$	$a+(-a)=0_{\mathbb{G}}$	&	$(-a)+a=0_{\mathbb{G}}$
$(A4)$	Comutatividade da soma	$a+b=b+a$		

II — Anéis algébricos

Seja $(\mathbb{A})$ um conjunto não vazio, munido de duas operações binárias $(+,-)$:

Adição			soma		Multiplicação			produto
$+:$	$\mathbb{A}\times\mathbb{A}$	$\longrightarrow$	$\mathbb{A}$		$\cdot:$	$\mathbb{A}\times\mathbb{A}$	$\longrightarrow$	$\mathbb{A}$
	(a,b)	$\longmapsto$	$+(a,b)\overset{\text{def}}{=}a+b$			(a,b)	$\longmapsto$	$\cdot\,(a,b)\overset{\text{def}}{=}a\cdot b$

Isto significa que ao grupo comutativo $(\mathbb{A},+)$ acrescenta-se outra operação denotada por $(\cdot)$, obtendo-se a dupla $\big((\mathbb{A},+),\cdot\big)$ usualmente representada pela tripla $(\mathbb{A},+,\cdot)$.

[4] Definição: A tripla $(\mathbb{A},+,\cdot)$ é denominada um **anel** se para cada para cada $\{a;b;c\}\subset\mathbb{A}$, a operação $(+)$ satisfizer os axiomas de grupos comutativos e se as operações $\{+,\cdot\}$ satisfizerem os seguintes axiomas:

$(A5)$	Associatividade do produto	$a\cdot(b\cdot c)=(a\cdot b)\cdot c$	
$(A6)$	Distributiva à esquerda	$a\cdot(b+c)=a\cdot b+a\cdot c$	
$(A7)$	Distributiva à direita	$(a+b)\cdot c=a\cdot c+b\cdot c$	

Assim, um anel $(\mathbb{A},+,\cdot)$ é um conjunto não vazio que satisfaz os (7) axiomas anteriormente apresentados.

III — Anéis com unidade

[5] Definição: Um anel $(\mathbb{A}, +, -)$ é dito possuir **unidade** se existir um elemento neutro para a multiplicação:

$(A8)$	Existência do elemento neutro $(1_{\mathbb{A}})$	$1_{\mathbb{A}} \cdot a = a$	&	$a \cdot 1_{\mathbb{A}} = a$

IV — Anéis com divisão

Para poder estabelecer as condições para a divisão, é necessário estabelecer-se a seguinte notação:

$$\mathbb{A}^* \stackrel{\text{def}}{=} \mathbb{A} - 0_{\mathbb{A}}$$

Ou seja, representa-se por $(\mathbb{A}^*)$ ao conjunto $(\mathbb{A})$ removendo-se o elemento neutro da adição $(0_{\mathbb{A}})$.

[6] Definição: Um anel $(\mathbb{A}, +, -)$ é dito **possuir divisão** se o par $(\mathbb{A}^*, \cdot)$ é um grupo. Neste caso, para cada elemento $(a \in \mathbb{A})$ com $(a \neq 0_{\mathbb{A}})$, isto é, para cada $(a \in \mathbb{A}^*)$, o seu elemento inverso é representado por (a^{-1}):

$(A5)$	Associatividade do produto	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$		
$(A8)$	Existência do elemento neutro $(1_{\mathbb{A}})$	$1_{\mathbb{A}} \cdot a = a$	&	$a \cdot 1_{\mathbb{A}} = a$
$(A9)$	Para cada $(a \in \mathbb{A} - \{0_{\mathbb{A}}\})$ há a existência do elemento inverso $(a^{-1} \in \mathbb{A}^*)$	$a \cdot a^{-1} = 1_{\mathbb{A}}$	&	$a^{-1} \cdot a = 1_{\mathbb{A}}$

Observe a correspondência dos axiomas da definição [1] de grupo com as propriedades acima.

IV — Corpos algébricos

No caso particular em que o grupo $(\mathbb{A}^*, \cdot)$ for abeliano, acrescenta-se a comutatividade do produto às propriedades do anel $(\mathbb{A}, +, \cdot)$ com divisão.

$(A10)$	Comutatividade do produto	$a + b = b + a$	

[7] Definição: O trio $(\mathbb{A}, +, \cdot)$ formado por conjunto não vazio $(\mathbb{A})$ munido das operações $(+)$ de adição e $(\cdot)$ de multiplicação é um **corpo** se o par $(\mathbb{A}, +)$ é um grupo comutativo e se o par $(\mathbb{A}^*, \cdot)$ for um grupo comutativo.

Isto significa que as operações satisfazem às seguintes propriedades preteritamente apresentadas:

Propriedades da soma:

$(A1)$	Associatividade da soma	$a + (b + c) = (a + b) + c$		
$(A2)$	Existência do elemento neutro $(0_{\mathbb{G}})$	$0_{\mathbb{A}} + a = a$	&	$a + 0_{\mathbb{A}} = a$
$(A3)$	Existência do elemento oposto $(-a)$	$a + (-a) = 0_{\mathbb{A}}$	&	$(-a) + a = 0_{\mathbb{A}}$
$(A4)$	Comutatividade da soma	$a + b = b + a$		

Propriedades do produto:

$(A5)$	Associatividade do produto	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$		
$(A8)$	Existência do elemento neutro $(1_{\mathbb{A}})$	$1_{\mathbb{A}} \cdot a = a$	&	$a \cdot 1_{\mathbb{A}} = a$
$(A9)$	Existência do elemento inverso (a^{-1})	$a \cdot a^{-1} = 1_{\mathbb{A}}$	&	$a^{-1} \cdot a = 1_{\mathbb{A}}$
$(A10)$	Comutatividade do produto	$a \cdot b = b \cdot a$		

Propriedade distributiva, que relaciona as operações de adição e multiplicação.

$(A6)$	Distributiva à esquerda	$a \cdot (b + c) = a \cdot b + a \cdot c$	
$(A7)$	Distributiva à direita	$(a + b) \cdot c = a \cdot c + b \cdot c$	