Universidade Federal de Goiás – Câmpus Catalão

Aluno: Bruno Castilho Rosa

Orientador: Igor Lima

Seminário Semanal de Álgebra

Notas de aula

1. **Título:** Subgrupos finitos de $\mathbb{C}^*$.

2. Breve descrição da aula

A aula será dividida em duas partes. Inicialmente, introduziremos as noções de grupo, subgrupo, ordem e índice. Em seguida, apresentaremos exemplos de grupos, grupos cíclicos, grupos abelianos e não abelianos, mas nos fixaremos nos conjuntos numéricos que tem estrutura natural de grupo, tais como o grupo dos inteiros, dos racionais e dos complexos.

E, finalmente, relembraremos propriedades dos números complexos C e mostraremos que os subgrupos finitos de C*=C-{0} estão contidos na esfera unitária S = { z em C | |z| =1}.

3. Competência(s) desenvolvida(s)

Compreender algumas noções da teoria dos grupos.

4. Conteúdo(s) desenvolvido(s)

- Definição 1. Seja G um conjunto não vazio, munido de uma operação binária *.

$$GXG \to G$$

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

G é grupo se os axiomas seguintes são satisfeitos:

(i) $a,b \in G \to a * b \in G$

(ii) Associativa: $(a * b) * c = a * (b * c) \forall\ a,b,c \in G$

(iii) Elemento Neutro: $\exists\ e \in G |\ a * e = e * a = a, \forall a \in \forall G$

(iv)Elemento Inverso: $\exists\ a^{-1} \in G |\ a * a^{-1} = a^{-1} * a = e, \forall a \in G$

Observação: Se, $a * b = b * a, \forall a,b \in\ G$, então G é abeliano.

- Exemplos de grupos:

$G = (\mathbb{Z}, +)$; $G = (\mathbb{Q}, +)$ $G = (\mathbb{R}, +)$; $G = (\mathbb{Q}^*, .)$ $G = (\mathbb{R}^*, .)$ $G = (\mathbb{Z}_m, +)$
$G = (\mathbb{C}, +), G = (\mathbb{C}^*, .)$

Vamos primeiramente demonstrar que

$G = (\mathbb{Z}, +)$ é um grupo.

Demonstração: $G \neq \phi$, pois $1 \in G$. Sejam a, b e c $\in \mathbb{Z}$. Temos que
$(a + b) \in \mathbb{Z}$, $\forall\, a, b \in \mathbb{Z}$. Logo $\mathbb{Z}$ é fechado.
Em $G = (\mathbb{Z}, +)$ vale a associativa: $(a, +b) + c = a + (b + c), \forall\, a, b\ e\ c \in \mathbb{Z}$.
Elemento Neutro. $a + e = e + a = a, \forall a \in \mathbb{Z}$.
O conjunto $\mathbb{Z}$ possui o elemento neutro e da adição. Tome $e = 0$.
Elemento inverso: $a + a^{-1} = a^{-1} + a = e, \forall a \in \mathbb{Z}$
O conjunto $\mathbb{Z}$ possui inverso aditivo a^{-1}. Tome $a^{-1} = -a$.

Portanto o conjunto $G = (\mathbb{Z}, +)$ é grupo.

$G = (\mathbb{Q}, +)$ é um grupo.

Demonstração: $G \neq \phi$, pois $1 \in G$. Sejam x, $y \in \mathbb{Q}$, mostraremos que $\mathbb{Q}$ é fechado para a soma.
$x = \frac{a_1}{b_1}, y = \frac{a_2}{b_2}$, com $a_i, b_i \in \mathbb{Z}$ e $b_1, b_2 \neq 0$. então $x + y = \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{b_2 a_1 + b_1 a_2}{b_1 b_2} \in \mathbb{Q}$
Associativa: $(x + y) + z = x + (y + z)$, onde $x = \frac{a_1}{b_1}, y = \frac{a_2}{b_2}$ e $z = \frac{a_3}{b_3}$ tal que
$a_i, b_i \in \mathbb{Z}$ e $b_i \neq 0$.

$$(x + y) + z = \left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) + \frac{a_3}{b_3} = \frac{b_3(b_2 a_1 + b_1 a_2) + b_1 b_2 a_3}{b_1 b_2 a_3}$$
$$= \frac{b_3 b_2 a_1 + b_3 b_1 a_2 + b_1 b_2 a_3}{b_1 b_2 a_3} = \frac{b_3 b_2 a_1 + b_1(b_3 a_2 + b_2 a_3)}{b_1 b_2 a_3}$$
$$= \frac{a_1}{b_1} + \frac{(b_3 a_2 + b_2 a_3)}{b_2 b_3} = \frac{a_1}{b_1} + \left(\frac{a_2}{b_2} + \frac{a_3}{b_3}\right) = x + (y + z)$$

Elemento Neutro: $x + e = e + x = x, \forall x \in \mathbb{Q}$
Tome $e = 0$, assim $x + 0 = 0 + x = x$
Elemento inverso: Verificaremos que dado $x \in \mathbb{Q}\ \exists\, x^{-1} \in \mathbb{Q} |\ x + x^{-1} = x^{-1} + x = 0$
$\frac{a_1}{b_1} + x^{-1} = 0$, tome $x^{-1} = \left(\frac{-a_1}{b_1}\right)$. Assim $\frac{a_1}{b_1} + x^{-1} = x^{-1} + \frac{a_1}{b_1} = 0$

Portanto $G = (\mathbb{Q}, +)$ é um grupo.

$G = (\mathbb{R}, +)$ é um grupo.

Demonstração: $G \neq \phi$, pois $1 \in \mathbb{R}$. Sejam x, $y \in \mathbb{R}$, temos que x+y$\in \mathbb{R}$.

Em $G = (\mathbb{R}, +)$ vale a associativa: $(x + y) + z = x + (y + z), \forall\, x, y\ e\ z \in \mathbb{R}$.
Elemento neutro: O elemento neutro em $\mathbb{R}$ é 0, pois $x + 0 = 0 + x = x$: $\forall x \in \mathbb{R}$.
Elemento inverso; Dado $x \in \mathbb{R}$, existe y $\in \mathbb{R}$, $y = -x$, tal que
$x + (-x) = (-x) + x = 0$
Portanto $G = (\mathbb{R}, +)$ é um grupo.

$G = (\mathbb{R}^*, .)$ é um grupo

Demonstração: $G \neq \phi$, pois $1 \in \mathbb{R}^*$. Sejam x, $y \in \mathbb{R}^*$, temos que x.y $\in \mathbb{R}^*$, $\forall x, y \in \mathbb{R}^*$.
Em $G = (\mathbb{R}^*, .)$ também vale a associativa: $(x.y).z = x.(y.z), \forall\, x, y\ e\ z \in \mathbb{R}^*$.
Elemento neutro: O elemento neutro em $\mathbb{R}^*$ é 1, pois
$x.1 = 1.x = \forall x \in \mathbb{R}^*$.
Elemento inverso: Dado $x \in \mathbb{R}^*$ existe y $\in \mathbb{R}^*$, $y = \frac{1}{x}$, tal que:

$$x.y = x\frac{1}{x} = 1.$$

Portanto $G = (\mathbb{R}^*, .)$ é um grupo.

$G = (\mathbb{Z}_m, +)$ é grupo, conhecido por grupo aditivo das classes dos restos, onde
$\mathbb{Z}_m = \{\overline{1}, \overline{2}, \overline{3}, \ldots \overline{m-1}, \}$ e a soma é definida por:
$\bar{a} + \bar{b} = \overline{a + b}, \forall \bar{a}, \bar{b} \in \mathbb{Z}_m$.

Demonstração: $\mathbb{Z}_m \neq \phi$, pois $\overline{1} \in \mathbb{Z}_m$.
$\mathbb{Z}_m$ é fechado, pois: $\bar{a} + \bar{b} = \overline{a + b} \in \mathbb{Z}_m$.
Associativa: $(\bar{a} + \bar{b}) + \bar{c} = (\overline{a + b}) + \bar{c} = \overline{a + b + c} = \bar{a} + \overline{b + c} = \bar{a} + (\overline{b + c}) =$
$\bar{a} + (\bar{b} + \bar{c})$.
Elemento neutro: O elemento neutro em $(\mathbb{Z}_m, +)$ é $\bar{0}$, pois:
$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}, \forall \bar{a} \in \mathbb{Z}_m$.
Elemento inverso: Dado $\bar{a} \in \mathbb{Z}_m$ existe $\bar{b} \in \mathbb{R}^*$, $\bar{b} = \overline{m - a}$, tal que:
$\bar{a} + \bar{b} = \bar{a} + \overline{m - a} = \overline{a + m - a} = \bar{m} = \bar{0}$.

Portanto $G = (\mathbb{Z}_m, +)$ é grupo.

G=($\mathbb{C}^*$, .) é um grupo.

Demonstração: Temos que $G \neq \phi$, pois $1 \in G$. Agora sejam $z_1, z_2, z_3 \in G$ tal que,
$z_1 = a_1 + b_1 i\,;\ z_2 = a_2 + b_2 i;\ z_3 = a_3 + b_3 i$, com $a_i,\ b_i \in \mathbb{Z}\ e\ a_i \neq b_i$
simultaneamente. Assim $z_1.\ z_2 = (a_1 + b_1 i)(a_2 + b_2 i) =$
$(a_1 a_2 + a_1 b_2 i + b_1 a_2 i - b_1 b_2) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)$i $\in G$. Logo
G é fechado.
Associativa: $(z_1.\ z_2).\ z_3 = z_1.(z_2.\ z_3)$
$[(a_1 + b_1 i)(a_2 + b_2 i)](a_3 + b_3 i)$
$= [(a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)\text{i}]\ (a_3 + b_3 i)$
=
$\{[(a_1 a_2 - b_1 b_2)\ a_3 - (a_1 b_2 + b_1 a_2)(b_3)] +$
$i[(a_1 a_2 - b_1 b_2)\ b_3 + (a_1 b_2 + b_1 a_2)\ a_3]\}$
$= (a_1 + b_1 i)[(a_2 + b_2 i)(a_3 + b_3 i)]$
Elemento Neutro: $z_1.\ e = e.\ z_1 = z_1$

Basta tomar e = $1+0i$, pois: $(a_1+b_1i)(1+0i)=(1+0i)(a_1+b_1i)=(a_1+b_1i)$
Elemento Inverso: $z_1 z_1^{-1} = z_1^{-1} z_1 = 1+0i$
Basta tomar $z_1^{-1} = \frac{\overline{z_1}}{|z_1|}$
Portanto, G=($\mathbb{C}^*$, .) é um grupo.

- Subgrupos.

Definição 2. Seja $(G,*)$ um grupo. Se $\phi \neq H \subseteq G$, com a operação* é um grupo, então H é um subgrupo de G.

Notação: $H \leq G$.

- Ordem e índice de um grupo.

A ordem de um grupo G, é a quantidade de elementos de G.

Notação: $|G|$

- Definição 3. Sejam G um grupo, $H \leq G$. Definimos como classe lateral à esquerda de H em G, o seguinte subconjunto $a*H$ de G|a$\in G$.

$a*H = \{a*h | h \in H\}$

De modo análogo, definimos,

$H*a = \{h*a | h \in H\}$, onde a$\in G$, como classe lateral à direita de H em G.

Seja G/H o conjunto das classes laterais, então o número de elementos distintos de G/H é chamado índice de H em G.

- Definição 4. Seja G um grupo. Dizemos que G é cíclico se existe $a \in G$, tal que $G = \{a^n | n \in \mathbb{Z}\}$.

Notação: $G = < a >$, G é dito, gerado pelo elemento a.

Observação. Se G é aditivo, a potência de base a e expoente n é denotada por na.

- Exemplo 2.1. G= $\{-1, 1, i, -i\}$ é um grupo cíclico, gerado por i.

Demonstração: G é grupo, pois:
$G \neq \phi$, visto que $1 \in G$. Temos que G também é fechado em relação à multiplicação, isto é, $a, b \in G \rightarrow a.b \in G, \forall a, b \in G$.
G é associativa, pois $(a.b).c = a.(b.c) \forall\ a, b, c \in G$
G possui elemento neutro, tome e=1
G possui elemento inverso, isto é, cada elemento de G tem inverso.

$(1)^{-1} = 1$

$(-1)^{-1} = -1$

$(i)^{-1} = -i$

$(-i)^{-1} = i$

Agora tome $i \in G$. Assim,

$i^0 = 1$
$i^1 = i$
$i^2 = -1$.
$i^3 = i^2.i = (-1).i = -i$

Logo G é um grupo cíclico gerado por i.

- Exemplo 2.2. O grupo $(\mathbb{Z}, +)$ é cíclico infinito gerado por 1.
  $\mathbb{Z} =< 1 >=\{n.1 \mid n \in \mathbb{Z}\}$.

- Propriedades dos números complexos.

Sejam $z_1 \; e \; z_2 \in \mathbb{C}^*$.

P1) $z_1\overline{z_1} = |z_1|^2$

P2) $|z_1 z_2| = |z_1||z_2|$

P3) $|{z_1}^k| = |z_1|^k$ com $k \in \mathbb{N}$.

- **Teorema 1.** Seja $H \leq (\mathbb{C}^*, .)$, $|H| < \infty$, com $n = |H| \text{ e } n \in \mathbb{N}$. Então existe $k \leq n$, tal que $z^k = 1, com \; n, k \in \mathbb{N}$.

Demonstração do Teorema 1.

Observe que existe $k \leq n$, tal que $z^k = 1$. De fato, considere o conjunto $\{z, z^2, z^3, \dots, z^{n+1}\}$. Daí existe $i, j \in \{z, z^2, z^3, \dots, z^{n+1}\}$, sem perda de generalidade podemos supor $i < j$. Assim, $z^i = z^j \Rightarrow \frac{z^i}{z^i} = \frac{z^j}{z^i} \Rightarrow 1 = z^{j-i}$. Tome $k = j - i \Rightarrow 1 = z^k$.

- **Proposição 1.** Se $z \in H$, então $|z| = 1$.

Essa Proposição mostra que todos os números complexos pertencentes aos subgrupos finitos de $(\mathbb{C}^*, .)$ estão contidos na esfera unitária.

Demonstração da Proposição 1.

Suponha que $|z| \neq 1$. Daí, $|z| > 1$ ou $|z| < 1$. Por outro lado, existe $k \in \mathbb{N}$, tal que $z^k = 1$. Aplicando a norma em ambos os lados, temos:

$|z^k| = |1| \Rightarrow |z.z \dots .z| = 1 \Rightarrow |z||z| \dots |z| = |z|^k > 1$, o que é um absurdo em ambos os lados, portanto $|z| = 1$.

Em geral, todos os subgrupos finitos de $(\mathbb{C}^*, .)$ que estão contidos na esfera unitária, podem ser descritos da seguinte forma:

$H_n = \{z \in \mathbb{C}^* \; tal \; que \; z = e^{\frac{i2k\pi}{n}} \text{ e } n \in \mathbb{N}$, onde $0 \leq k \leq n-1\}$.

5. Recursos /Materiais Utilizado

Quadro e giz.

6. Bibiografia

VIANA, Ricardo L. Teoria dos grupos. Curitiba. 2010.
GARCIA, Arnaldo e LEQUAIN, Yves. Elementos de Álgebra. IMPA, 6º ed. Rio de Janeiro. 2012.