

Subgrupos e grupos cíclicos

AULA

14

Meta da aula

Apresentar os conceitos de subgrupo e de subgrupo cíclico.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as propriedades que caracterizam um subgrupo.
- Apresentar exemplos de subgrupos.
- Identificar as propriedades que caracterizam um grupo cíclico.
- Apresentar exemplos de subgrupos cíclicos.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I e nas Aulas 12 e 13.

INTRODUÇÃO

Nas duas aulas anteriores, desenvolvemos o conceito de grupo e estudamos vários exemplos. Você deve ter notado que vimos alguns exemplos de grupos contidos em outro grupo maior. Por exemplo, o grupo $(\mathbf{Z}, +)$, dos números inteiros com a operação de adição, está contido no grupo $(\mathbf{Q}, +)$ dos números racionais com a operação de adição. Da mesma forma, $(\mathbf{Q}, +)$ está contido em $(\mathbf{R}, +)$ que, por sua vez, está contido em $(\mathbf{C}, +)$. Esta é a importante noção de subgrupo.

É relevante observar que, quando dizemos que o grupo $(\mathbf{Z}, +)$ está contido no grupo $(\mathbf{Q}, +)$, queremos dizer não só que um conjunto é subconjunto do outro, $\mathbf{Z} \subset \mathbf{Q}$, mas também que a operação de adição $(+)$ entre dois números inteiros, a e b , produz o mesmo resultado $a + b$ que na situação em que a e b são vistos como elementos do grupo $(\mathbf{Q}, +)$. Assim, não podemos dizer que o grupo multiplicativo (\mathbf{Q}^*, \cdot) está contido no grupo aditivo $(\mathbf{R}, +)$, pois, apesar de $\mathbf{Q}^* \subset \mathbf{R}$, as operações $a \cdot b$ em (\mathbf{Q}^*, \cdot) e $a + b$ em $(\mathbf{R}, +)$ dão resultados diferentes para os mesmos $a, b \in \mathbf{Q}$. Por exemplo, $1 \cdot 1 = 1$ e $1 + 1 = 2$. Portanto, para que um grupo seja um subgrupo de outro grupo, vamos exigir não só que um conjunto esteja contido no outro mas, também, que suas operações coincidam nos elementos que são comuns aos dois conjuntos.

DEFINIÇÃO 1 (SUBGRUPO)

Sejam (G, \cdot) um grupo e H um subconjunto não-vazio de G . Dizemos que H é um subgrupo de G se H , munido da operação \cdot do grupo G , for um grupo, ou seja, se (H, \cdot) for um grupo.

Veja que a operação \cdot já é associativa em G , logo, ela já satisfaz a propriedade associativa para os elementos de H . Portanto, as propriedades a serem satisfeitas para que H seja um subgrupo de G são dadas pelos seguintes axiomas.

SG1. H é fechado pela operação de G , isto é, $a \cdot b \in H$ para todo $a, b \in H$.

SG2. $e_G \in H$.

SG3. Se $a \in H$ então $a^{-1} \in H$.

Se H é subgrupo de G , então denotamos $H < G$ e, caso contrário, denotamos $H \not< G$.

Observação

Dado o grupo G , então $\{e_G\}$ e G são subgrupos de G , chamados *subgrupos triviais* de G . Se H é um subgrupo de G , diferente de $\{e_G\}$ e G , então dizemos que H é um subgrupo próprio de G .

Exemplo 1

Pelas nossas observações iniciais, temos a seguinte seqüência de subgrupos:

$$(\mathbf{Z}, +) < (\mathbf{Q}, +) < (\mathbf{R}, +) < (\mathbf{C}, +).$$

No entanto, (\mathbf{Q}^*, \cdot) não é subgrupo de $(\mathbf{R}, +)$, já que a operação de (\mathbf{Q}^*, \cdot) não é a mesma que a de $(\mathbf{R}, +)$. Mas é verdade que

$$(\mathbf{Q}^*, \cdot) < (\mathbf{R}^*, \cdot) < (\mathbf{C}^*, \cdot).$$

Assim como temos critérios que facilitam verificar se um subconjunto de um espaço vetorial é um subespaço vetorial ou se um subconjunto de um anel é um subanel, temos, também, um critério que facilita verificar se um subconjunto de um grupo é um subgrupo. É o que vamos fazer a seguir.

Proposição 1 (Critério do Subgrupo)

Seja H um subconjunto não-vazio de um grupo G . Então, H é um subgrupo de G se, e somente se, $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

Demonstração

(\Rightarrow) Vamos supor, inicialmente, que H é um subgrupo de G . Queremos provar que $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

Assim, sejam $a, b \in H$. Temos

$$\begin{aligned} a, b \in H &\Rightarrow b^{-1} \in H \quad \text{pela propriedade SG3 de subgrupo} \\ &\Rightarrow a \cdot b^{-1} \in H \quad \text{pela propriedade SG1 de subgrupo,} \end{aligned}$$

e, assim, provamos o que queríamos, ou seja, que $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

(\Leftrightarrow) Nossa hipótese, agora, é que $a \cdot b^{-1} \in H$ para todo $a, b \in H$. Queremos provar que H é subgrupo de G , ou seja, que H satisfaz as propriedades SG1 a SG3. Vamos provar primeiro a validade de SG2, depois SG3 e, por fim, SG1.

SG2. Como $H \neq \emptyset$, existe um elemento $a \in H$. Daí, temos

$$a \in H \Rightarrow e_G = a \cdot a^{-1} \in H \quad \text{pela hipótese com } b = a.$$

SG3. Seja $x \in H$. Como já sabemos que $e_G \in H$, então,

$$x, e_G \in H \Rightarrow x^{-1} = e_G \cdot x^{-1} \in H \quad \text{pela hipótese com } a = e_G \text{ e } b = x.$$

SG1. Sejam $x, y \in H$. Pela propriedade SG3, sabemos que $y^{-1} \in H$. Portanto, temos

$$x, y^{-1} \in H \Rightarrow x \cdot y = x \cdot (y^{-1})^{-1} \in H \quad \text{pela hipótese com } a = x \text{ e } b = y^{-1}.$$

Concluimos, assim, que H é um subgrupo de G .

Observação

Quando G for um grupo aditivo, $(G, +)$, e H um subconjunto não-vazio de G , a condição $a \cdot b^{-1} \in H$ se transformará em

$$a - b \in H,$$

já que $-b$ é o elemento inverso de b . Assim, nesse caso, temos

$$H < G \quad \Leftrightarrow \quad a - b \in H \quad \text{para todo } a, b \in H.$$

**ATIVIDADE**

1. Dado o grupo aditivo $(\mathbf{Z}, +)$, mostre que $n\mathbf{Z} = \{kn \mid k \in \mathbf{Z}\}$ é um subgrupo de \mathbf{Z} para todo inteiro $n > 1$.

Exemplo 2

Seja $D_3 = \{I, R, R^2, F, FR, FR^2\}$ o grupo das simetrias do triângulo eqüilátero visto na Aula 18. Então

$$H_1 = \{I, R, R^2\} \text{ e } H_2 = \{I, F\}$$

são subgrupos de D_3 . Isso é imediato pela aplicação do critério do subgrupo.

Exemplo 3

Considere o grupo $(\mathbf{Z}_4, +)$. Vamos mostrar que $H = \{\bar{0}, \bar{2}\}$ é o único subgrupo próprio de \mathbf{Z}_4 . Se H for outro subgrupo próprio de $\mathbf{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, então, teremos $\bar{1} \in H$ ou $\bar{3} \in H$. Caso seja $\bar{1} \in H$, então, aplicando SG1, teremos

$$\bar{2} = \bar{1} + \bar{1} \in H; \quad \bar{3} = \bar{2} + \bar{1} \in H \quad \text{e} \quad \bar{0} = \bar{3} + \bar{1} \in H,$$

e, portanto, teríamos $H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbf{Z}_4$, o que é uma contradição, já que H é subgrupo próprio de \mathbf{Z}_4 .

Caso seja $\bar{3} \in H$, então, aplicando SG3, teremos

$$\bar{1} = -\bar{3} \in H,$$

e, pelo argumento anterior, teríamos novamente que $H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbf{Z}_4$, que é a mesma contradição. A conclusão, portanto, é que $H = \{\bar{0}, \bar{2}\}$ é o único subgrupo próprio de \mathbf{Z}_4 .

Vamos desenvolver, agora, um importante tipo de subgrupos, que são os subgrupos gerados por um único elemento.

DEFINIÇÃO 2 (SUBGRUPO GERADO POR UM ELEMENTO)

Sejam (G, \cdot) um grupo e $a \in G$. Definimos as *potências* de a :

$$\begin{aligned} a^0 &= e_G \\ a^n &= a^{n-1} \cdot a \quad \text{se } n \in \mathbf{Z}, n \geq 1 \\ a^n &= (a^{-1})^{-n} \quad \text{se } n \in \mathbf{Z}, n < 0. \end{aligned}$$

Denotamos por $\langle a \rangle$ o conjunto de todas as potências de a , ou seja,

$$\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$$

Veremos, a seguir, que este conjunto é um subgrupo de G , chamado *subgrupo gerado* por a . Dizemos, também, que a é um gerador de $\langle a \rangle$.

Quando G for um grupo aditivo, $(G, +)$, então as potências de a serão, na verdade, os múltiplos de a :

$$\begin{cases} 0a = 0_G \\ na = (n-1)a + a \quad \text{se } n \in \mathbf{Z}, n \geq 1 \\ na = (-n)(-a) \quad \text{se } n \in \mathbf{Z}, n < 0, \end{cases}$$

e o subgrupo gerado por a se escreve como

$$\langle a \rangle = \{na \mid n \in \mathbf{Z}\}$$

Proposição 2 (O subgrupo gerado por a)

Sejam (G, \cdot) um grupo e $a \in G$. Então $\langle a \rangle$ é um subgrupo de G .

Demonstração

Vamos aplicar o critério do subgrupo. Sejam $a^n, a^k \in \langle a \rangle$ dois elementos, então

$$a^n \cdot (a^k)^{-1} = a^n \cdot a^{-k} = a^{n-k} \in \langle a \rangle$$

o que prova que $\langle a \rangle$ é um subgrupo de G .

Exemplo 4

Dado o grupo $(\mathbb{Z}, +)$, então $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z} = \langle n \rangle\}$. Em particular, $2\mathbb{Z} = \langle 2 \rangle$. Veja, também, que $\mathbb{Z} = \langle 1 \rangle$.

Exemplo 5

Considere o grupo $(\mathbb{Z}_4, +)$ do Exemplo 3. Então $H = \{\bar{0}, \bar{2}\} = \langle \bar{2} \rangle$. Veja aqui, também, que $\mathbb{Z}_4 = \langle \bar{1} \rangle$.

Grupos, como \mathbb{Z} ou \mathbb{Z}_n , que são gerados por apenas um elemento, são muito importantes e têm uma nomenclatura especial.

DEFINIÇÃO 3 (GRUPO CÍCLICO)

Um grupo G é chamado grupo cíclico se $G = \langle a \rangle$ para algum $a \in G$, ou seja, G é gerado por um elemento. Neste caso, dizemos que a é um gerador de G .

Observação

Se G é um grupo cíclico, então o gerador de G , isto é, o elemento $a \in G$ tal que $G = \langle a \rangle$, em geral, não é único. Por exemplo, $\mathbb{Z}_4 = \langle \bar{1} \rangle$ e $\mathbb{Z}_4 = \langle \bar{3} \rangle$.

Exemplo 6

Considere o grupo $(\mathbb{Z}_n, +)$, onde $n > 1$ é um inteiro. Então $\mathbb{Z}_n = \langle \bar{1} \rangle$, e, portanto, \mathbb{Z}_n é um grupo cíclico.



ATIVIDADE

2. Determine se os grupos multiplicativos (\mathbb{Z}_5^*, \cdot) e (\mathbb{Z}_8^*, \cdot) são grupos cíclicos. Caso algum deles seja um grupo cíclico, determine seus geradores.

Para terminar esta aula, vamos enunciar um resultado que diz, no fundo, que todo grupo cíclico é uma cópia de $(\mathbb{Z}, +)$ ou uma cópia de algum $(\mathbb{Z}_n, +)$. Para isso precisamos definir o conceito de ordem de um elemento.

DEFINIÇÃO 4 (ORDEM DE UM ELEMENTO)

Seja G um grupo e seja $a \in G$. Se o subgrupo $\langle a \rangle$ for finito, então dizemos que a *ordem de a* , denotada por $\text{ord}(a)$, é o número de elementos de $\langle a \rangle$, ou seja, é igual à ordem de $\langle a \rangle$. Agora, se $\langle a \rangle$ for um grupo infinito, então dizemos que a *ordem de a* é *infinita*.

Observação

1. Para o elemento neutro e de um grupo G , temos $\langle e \rangle = \{e\}$ e, portanto, $\text{ord}(e) = 1$. Para qualquer outro elemento $a \in G$ ($a \neq e$), temos $\text{ord}(a) = > 1$.
2. Se G é um grupo cíclico com gerador a , $G = \langle a \rangle$, então $\text{ord}(a) = |G|$.

Exemplo 7

Considere o grupo aditivo $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Pela observação anterior, já sabemos que $\text{ord}(\bar{0}) = 1$. Agora,

$$\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4; \quad \langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}; \quad \langle \bar{3} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4,$$

de onde concluímos que

$$\text{ord}(\bar{1}) = 4; \quad \text{ord}(\bar{2}) = 2 \quad \text{ord}(\bar{3}) = 4$$

**ATIVIDADE**

3. Determine a ordem dos elementos dos grupos multiplicativos (\mathbf{Z}_5^*, \cdot) e (\mathbf{Z}_8^*, \cdot) .

Podemos enunciar, agora, o resultado mais importante deste capítulo.

TEOREMA 1

Seja G um grupo e seja $a \in G$.

1. Se a for um elemento de ordem finita n , então n será o menor inteiro positivo que satisfaz $a^n = e_G$. Mais ainda, $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.
2. Se a for um elemento de ordem infinita, então $a^n \neq e_G$ para todo inteiro $n \neq 0$. Mais ainda, $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$ e todas as potências de a serão distintas.

CARACTERIZAÇÃO DOS GRUPOS CÍCLICOS

Futuramente vamos definir o conceito de isomorfismo de grupos de modo muito semelhante ao que foi feito para os isomorfismos de espaços vetoriais e para os isomorfismos de anéis. Isso significa que dois grupos serão isomórficos quando um for uma cópia algébrica do outro.

Assim, se G for um grupo cíclico com gerador a , ou seja, $G = \langle a \rangle$, então o teorema anterior diz que teremos dois casos a considerar:

1. Se a for um elemento de ordem finita n , então $G = \{e, a, a^2, \dots, a^{n-1}\}$ e G será isomórfico a \mathbf{Z}_n .
2. Se a for um elemento de ordem infinita, então $G = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$, com todas as potências de a distintas, e G será isomórfico a \mathbf{Z} .

Observação

Como conseqüência da caracterização dos grupos cíclicos, temos que todo grupo cíclico é abeliano.

No entanto, a recíproca é falsa, ou seja, nem todo grupo abeliano é um grupo cíclico. Por exemplo, o grupo multiplicativo \mathbf{Z}_8^* , é abeliano, mas, como você provou na Atividade 2, ele não é um grupo cíclico.

ATIVIDADES FINAIS

1. Determine se o grupo multiplicativo $\mathbf{Z}_7^* = \{\bar{a} \in \mathbf{Z}_7 \mid \text{mdc}(a, 7) = 1\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ é cíclico. Caso seja, determine seus geradores.

2. Determine se o grupo S_3 , das permutações de 3 objetos, é cíclico. Caso seja, determine seus geradores.

RESUMO

Nesta aula, vimos o conceito de subgrupo. Vimos que um subconjunto não-vazio H de um grupo G é um subgrupo de G se satisfizer os seguintes axiomas:

SG1. H é fechado pela operação de G , isto é, $a \cdot b \in H$ para todo $a, b \in H$.

SG2. $e_G \in H$.

SG3. Se $a \in H$ então $a^{-1} \in H$.

Depois, vimos o conceito de um subgrupo gerado por um elemento $a \in G$, que o subconjunto $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \subset G$. Vimos que a ordem do elemento $a \in G$ é a ordem do subgrupo $\langle a \rangle$. Em seguida, vimos que um grupo G é um grupo cíclico se existir $a \in G$ tal que $G = \langle a \rangle$. Nesse caso, dizemos que o elemento a é um gerador do grupo G .

Por fim, vimos o importante teorema que diz que se G é um grupo e $a \in G$, então:

1. Se a for um elemento de ordem finita n , então n será o menor inteiro positivo que satisfaz $a^n = e_G$. Mais ainda, $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$;
2. Se a for um elemento de ordem infinita, então $a^n \neq e_G$ para todo inteiro $n \neq 0$. Mais ainda, $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}$ e todas as potências de a serão distintas.



RESPOSTAS COMENTADAS

Atividade 1

Pelo critério do subgrupo, basta verificar que $a - b \in n\mathbb{Z}$ para todo $a, b \in n\mathbb{Z}$. Como $a, b \in n\mathbb{Z}$, então existem $k, m \in \mathbb{Z}$ tais que $a = kn$ e $b = mn$. Assim,

$$a - b = kn - mn = (k - m)n \in n\mathbb{Z},$$

e, portanto, $n\mathbb{Z}$ é um subgrupo de \mathbb{Z} .

Atividade 2

Vamos considerar, inicialmente, $\mathbf{Z}_5^x = \{\bar{a} \in \mathbf{Z}_5 \mid \text{mdc}(a, 5) = 1\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Considerando as potências de $\bar{2} \in \mathbf{Z}_5^x$, temos:

$$(\bar{2})^1 = \bar{2}; (\bar{2})^2 = \bar{4}; (\bar{2})^3 = \bar{3}; (\bar{2})^4 = \bar{1},$$

o que mostra que $\mathbf{Z}_5^x = \langle \bar{2} \rangle$, ou seja, \mathbf{Z}_5^x é um grupo cíclico. Mais ainda, não só o elemento $\bar{2}$ é um gerador de \mathbf{Z}_5^x , o elemento $\bar{3}$ também é, pois

$$(\bar{3})^1 = \bar{3}; (\bar{3})^2 = \bar{4}; (\bar{3})^3 = \bar{2}; (\bar{3})^4 = \bar{1},$$

e, portanto, $\mathbf{Z}_5^x = \langle \bar{3} \rangle$. Mas, $\bar{4}$ não é gerador de \mathbf{Z}_5^x , pois

$$(\bar{4})^1 = \bar{4}; (\bar{4})^2 = \bar{1}; (\bar{4})^3 = \bar{4}; (\bar{4})^4 = \bar{1}; \dots,$$

ou seja, $\langle \bar{4} \rangle = \{\bar{1}, \bar{4}\}$, que é um subgrupo próprio de \mathbf{Z}_5^x .

No caso de $\mathbf{Z}_8^x = \{a \in \mathbf{Z}_8 \mid \text{mdc}(a, 8) = 1\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, temos

$$(\bar{3})^1 = \bar{3}; (\bar{3})^2 = \bar{1}; (\bar{3})^3 = \bar{3}; (\bar{3})^4 = \bar{1}; \dots,$$

$$(\bar{5})^1 = \bar{5}; (\bar{5})^2 = \bar{5}; (\bar{5})^3 = \bar{5}; (\bar{5})^4 = \bar{1}; \dots,$$

e

$$(\bar{7})^1 = \bar{7}; (\bar{7})^2 = \bar{7}; (\bar{7})^3 = \bar{7}; (\bar{7})^4 = \bar{1}; \dots$$

Portanto, temos

$$\langle \bar{3} \rangle = \{\bar{1}, \bar{3}\}, \quad \langle \bar{5} \rangle = \{\bar{1}, \bar{5}\} \text{ e } \langle \bar{7} \rangle = \{\bar{1}, \bar{7}\},$$

ou seja, todos subgrupos próprios de \mathbf{Z}_8^x . Assim, \mathbf{Z}_8^x não é um grupo cíclico.

Atividade 3

Considere \mathbf{Z}_5^x . Já sabemos que $\text{ord}(\bar{1}) = 1$. Agora, dos cálculos feitos na atividade anterior, temos

$$\langle \bar{2} \rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbf{Z}_5^x; \quad \langle \bar{3} \rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbf{Z}_5^x; \quad \langle \bar{4} \rangle = \{\bar{1}, \bar{4}\},$$

de onde concluímos que

$$\text{ord}(\bar{2}) = 4; \quad \text{ord}(\bar{3}) = 4 \quad \text{e} \quad \text{ord}(\bar{4}) = 2.$$

Seja, agora, $\mathbf{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Já sabemos que $\text{ord}(\bar{1}) = 1$. Também, dos cálculos feitos na atividade anterior, temos

$$\langle \bar{3} \rangle = \{\bar{1}, \bar{3}\}, \quad \langle \bar{5} \rangle = \{\bar{1}, \bar{5}\} \text{ e } \langle \bar{7} \rangle = \{\bar{1}, \bar{7}\},$$

de onde concluímos que

$$\text{ord}(\bar{3}) = 2; \quad \text{ord}(\bar{5}) = 2 \quad \text{e} \quad \text{ord}(\bar{7}) = 2.$$

Observe que, como os elementos $\bar{3}$, $\bar{5}$ e $\bar{7}$ são seus próprios inversos em \mathbf{Z}_8^* , então eles são de ordem $\bar{2}$.

Atividade Final 1

Calculando as potências dos elementos de $\mathbf{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ e aplicando o Teorema 1, obtemos

$$(\bar{2})^1 = \bar{2}; \quad (\bar{2})^2 = \bar{4}; \quad (\bar{2})^3 = \bar{1} \quad \Rightarrow \quad \text{ord}(\bar{2}) = 3;$$

$$(\bar{3})^1 = \bar{3}; \quad (\bar{3})^2 = \bar{2}; \quad (\bar{3})^3 = \bar{6}; \quad (\bar{3})^4 = \bar{4}; \quad (\bar{3})^5 = \bar{5}; \quad (\bar{3})^6 = \bar{1} \quad \Rightarrow \quad \text{ord}(\bar{3}) = 6$$

$$(\bar{4})^1 = \bar{4}; \quad (\bar{4})^2 = \bar{2}; \quad (\bar{4})^3 = \bar{1} \quad \Rightarrow \quad \text{ord}(\bar{4}) = 3$$

$$(\bar{5})^1 = \bar{5}; \quad (\bar{5})^2 = \bar{4}; \quad (\bar{5})^3 = \bar{6}; \quad (\bar{5})^4 = \bar{2}; \quad (\bar{5})^5 = \bar{3}; \quad (\bar{5})^6 = \bar{1} \quad \Rightarrow \quad \text{ord}(\bar{5}) = 6$$

e

$$(\bar{6})^1 = \bar{6}; \quad (\bar{6})^2 = \bar{1}; \quad \Rightarrow \quad \text{ord}(\bar{6}) = 2$$

Portanto, como $\mathbf{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ é um grupo de ordem 6 e temos dois elementos também de ordem 6, então segue que \mathbf{Z}_7^* é um grupo cíclico com

$$\mathbf{Z}_7^* = \langle \bar{3} \rangle = \langle \bar{5} \rangle,$$

ou seja, \mathbf{Z}_7^* tem os geradores $\bar{3}$ e $\bar{5}$.

Atividade Final 2

Na Aula 18, vimos que $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ com

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Pelos cálculos, também feitos naquela aula, e aplicando o Teorema 1, temos

$$(\alpha)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad \alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \Rightarrow \text{ord}(\alpha) = 3;$$

$$(\alpha^2)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad (\alpha^2)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad (\alpha^2)^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \Rightarrow \text{ord}(\alpha) = 3;$$

$$(\beta)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad \beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \Rightarrow \text{ord}(\beta) = 2;$$

$$(\beta\alpha)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \quad (\beta\alpha)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \Rightarrow \text{ord}(\beta\alpha) = 2;$$

e

$$(\beta\alpha^2)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad (\beta\alpha^2)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \Rightarrow \text{ord}(\beta\alpha^2) = 2;$$

Como S_3 é um grupo de ordem 6 e todos os seus elementos têm ordem menor que 6, então segue que S_3 não é um grupo cíclico.