Subgrupos Cíclicos

Prof. Márcio Nascimento

marcio@matematicauva.org

Universidade Estadual Vale do Acaraú
Centro de Ciências Exatas e Tecnologia
Curso de Licenciatura em Matemática
Disciplina: Estruturas Algébricas II - 2014.2

11 de março de 2015

Sumário

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;
- Deve ser fechado para a operação. Isto é, $\overline{3} + \overline{3} = \overline{6} \in H$;

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;
- Deve ser fechado para a operação. Isto é, $\overline{3} + \overline{3} = \overline{6} \in H$;
- Pelo mesmo motivo, $\overline{3} + \overline{6} = \overline{9} \in H$;

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;
- Deve ser fechado para a operação. Isto é, $\overline{3} + \overline{3} = \overline{6} \in H$;
- Pelo mesmo motivo, $\overline{3} + \overline{6} = \overline{9} \in H$;
- Dentre os elementos $\overline{0}, \overline{3}, \overline{6}$ e $\overline{9}$, a soma sempre resultará em um desses elementos!

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;
- Deve ser fechado para a operação. Isto é, $\overline{3} + \overline{3} = \overline{6} \in H$;
- Pelo mesmo motivo, $\overline{3} + \overline{6} = \overline{9} \in H$;
- Dentre os elementos $\overline{0}, \overline{3}, \overline{6}$ e $\overline{9}$, a soma sempre resultará em um desses elementos!
- Os inversos: $(\overline{0})^{-1} = \overline{0}$, $(\overline{3})^{-1} = \overline{9}$, $(\overline{6})^{-1} = \overline{6}$, $(\overline{9})^{-1} = \overline{3}$.

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;
- Deve ser fechado para a operação. Isto é, $\overline{3} + \overline{3} = \overline{6} \in H$;
- Pelo mesmo motivo, $\overline{3} + \overline{6} = \overline{9} \in H$;
- Dentre os elementos $\overline{0}, \overline{3}, \overline{6}$ e $\overline{9}$, a soma sempre resultará em um desses elementos!
- Os inversos: $(\overline{0})^{-1} = \overline{0}$, $(\overline{3})^{-1} = \overline{9}$, $(\overline{6})^{-1} = \overline{6}$, $(\overline{9})^{-1} = \overline{3}$.
- Conclusão: $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ é um subgrupo de $(\mathbb{Z}_{12}, +)$. Na verdade, é o **menor subgrupo** de $\mathbb{Z}_{12}$ contendo $\overline{3}$.

Subgrupos Cíclicos

Considere o grupo $\mathbb{Z}_{12}$ com a operação $+$. Como seria um subgrupo H de $\mathbb{Z}_{12}$ contendo o elemento $\overline{3}$?

- Sendo um subgrupo, deve conter o elemento neutro $\overline{0}$;
- Deve ser fechado para a operação. Isto é, $\overline{3} + \overline{3} = \overline{6} \in H$;
- Pelo mesmo motivo, $\overline{3} + \overline{6} = \overline{9} \in H$;
- Dentre os elementos $\overline{0}, \overline{3}, \overline{6}$ e $\overline{9}$, a soma sempre resultará em um desses elementos!
- Os inversos: $(\overline{0})^{-1} = \overline{0}$, $(\overline{3})^{-1} = \overline{9}$, $(\overline{6})^{-1} = \overline{6}$, $(\overline{9})^{-1} = \overline{3}$.
- Conclusão: $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ é um subgrupo de $(\mathbb{Z}_{12}, +)$. Na verdade, é o **menor subgrupo** de $\mathbb{Z}_{12}$ contendo $\overline{3}$.
- Veja que $H = \{(\overline{3})^0, (\overline{3})^1, (\overline{3})^2, (\overline{3})^3\}$, pois $(\overline{3})^4 = (\overline{3})^0$.

Subgrupos Cíclicos

Exemplo

Descreva o menor subgrupo de $\mathbb{Z}_{12}$ que contém $\overline{4}$.

Subgrupos Cíclicos

Exemplo

Descreva o menor subgrupo de $\mathbb{Z}_{12}$ que contém $\overline{4}$.

- $H = \{(\overline{4})^0, (\overline{4})^1, (\overline{4})^2\} = \{\overline{0}, \overline{4}, \overline{8}\}$ pois $(\overline{4})^3 = \overline{0}$.

Subgrupos Cíclicos

Teorema

Seja G um grupo e $a \in G$. Então

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

é um subgrupo de G e é o menor subgrupo de G que contém a, isto é, qualquer outro subgrupo de G que contenha a, contém o conjunto H.

Subgrupos Cíclicos

Teorema

Seja G um grupo e $a \in G$. Então

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

é um subgrupo de G e é o menor subgrupo de G que contém a, isto é, qualquer outro subgrupo de G que contenha a, contém o conjunto H.

Prova: Sendo $x, y \in H$, tem-se $x * y^{-1} \in H$?

Subgrupos Cíclicos

Teorema

Seja G um grupo e $a \in G$. Então

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

é um subgrupo de G e é o menor subgrupo de G que contém a, isto é, qualquer outro subgrupo de G que contenha a, contém o conjunto H.

Prova: Sendo $x, y \in H$, tem-se $x * y^{-1} \in H$?

H é o conjunto das potências de a. Então $x = a^r$ e $y = a^s$ onde r, s são inteiros.

Subgrupos Cíclicos

Teorema

Seja G um grupo e $a \in G$. Então

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

é um subgrupo de G e é o menor subgrupo de G que contém a, isto é, qualquer outro subgrupo de G que contenha a, contém o conjunto H.

Prova: Sendo $x, y \in H$, tem-se $x * y^{-1} \in H$?

H é o conjunto das potências de a. Então $x = a^r$ e $y = a^s$ onde r, s são inteiros.

Veja que $a^{-s} \in H$ pois $-s \in \mathbb{Z}$. Além disso, a^{-s}, por definição, é igual a $(a^{-1})^s$. Logo,

Subgrupos Cíclicos

Teorema

Seja G um grupo e $a \in G$. Então

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

é um subgrupo de G e é o menor subgrupo de G que contém a, isto é, qualquer outro subgrupo de G que contenha a, contém o conjunto H.

Prova: Sendo $x, y \in H$, tem-se $x * y^{-1} \in H$?

H é o conjunto das potências de a. Então $x = a^r$ e $y = a^s$ onde r, s são inteiros.

Veja que $a^{-s} \in H$ pois $-s \in \mathbb{Z}$. Além disso, a^{-s}, por definição, é igual a $(a^{-1})^s$. Logo,

$x * y^{-1} = a^r * a^{-s} = a^{r-s} \in H$ pois $r - s \in \mathbb{Z}$.

Subgrupos Cíclicos

Definição (Subgrupo Cíclico)

Seja G um grupo e $a \in G$. O subgrupo as potências de a é chamado **Subgrupo Cíclico de G gerado por** *a. Notação:*

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

Definição (Gerador)

Um elemento $a \in G$ gera G e é chamado **Gerador de** *G se $\langle a \rangle = G$.*

Definição (Grupo Cíclico)

Um grupo G é dito **Cíclico** *se existe algum elemento $a \in G$ que gera G.*

Exemplos

1. $H = \{\overline{0}, \overline{4}, \overline{8}\}$ é um subgrupo cíclico de $\mathbb{Z}_{12}$ pois $\langle \overline{4} \rangle = H$;

Exemplos

1. $H = \{\overline{0}, \overline{4}, \overline{8}\}$ é um subgrupo cíclico de $\mathbb{Z}_{12}$ pois $\langle \overline{4} \rangle = H$;
2. O conjunto dos números pares, é um subgrupo cíclico de $(\mathbb{Z}, +)$?

Exemplos

1. $H = \{\overline{0}, \overline{4}, \overline{8}\}$ é um subgrupo cíclico de $\mathbb{Z}_{12}$ pois $\langle \overline{4} \rangle = H$;
2. O conjunto dos números pares, é um subgrupo cíclico de $(\mathbb{Z}, +)$?
3. Existe gerador para o grupo $(\mathbb{Z}, +)$?

Exemplos

1. $H = \{\overline{0}, \overline{4}, \overline{8}\}$ é um subgrupo cíclico de $\mathbb{Z}_{12}$ pois $\langle \overline{4} \rangle = H$;
2. O conjunto dos números pares, é um subgrupo cíclico de $(\mathbb{Z}, +)$?
3. Existe gerador para o grupo $(\mathbb{Z}, +)$?
4. $(\mathbb{R}, +)$ é um grupo cíclico?

Exemplos

1. $H = \{\overline{0}, \overline{4}, \overline{8}\}$ é um subgrupo cíclico de $\mathbb{Z}_{12}$ pois $\langle \overline{4} \rangle = H$;
2. O conjunto dos números pares, é um subgrupo cíclico de $(\mathbb{Z}, +)$?
3. Existe gerador para o grupo $(\mathbb{Z}, +)$?
4. $(\mathbb{R}, +)$ é um grupo cíclico?
5. Qual o subgrupo cíclico de $(\mathbb{Q}^*, \cdot)$ gerado por $\frac{1}{2}$?

Exercício

Descreva o subgrupo cíclico de $(\mathbb{Z}_{30}, +)$ *gerado por* $\overline{25}$.

Exercício

Descreva o subgrupo cíclico de $(\mathbb{C}^*, \cdot)$ *gerado por* i*.*

Exemplo

Seja G o conjunto das matrizes de ordem 2×2 com relação a soma de matrizes. Descreva o subgrupo de G gerado pelo elemento

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Exemplo

Seja G o conjunto das matrizes de ordem 2×2 com relação a soma de matrizes. Descreva o subgrupo de G gerado pelo elemento

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \mid n \in \mathbb{Z} \right\}$$

Exemplo

Seja G o conjunto das matrizes de ordem 2×2 com relação a soma de matrizes. Descreva o subgrupo de G gerado pelo elemento

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \mid n \in \mathbb{Z} \right\}$$

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} n & n \\ 0 & n \end{bmatrix} \mid n \in \mathbb{Z} \right\}$$

Exercício

Todo grupo cíclico é abeliano.

Prova:

Exercício

Todo grupo cíclico é abeliano.

Prova:

Se G é um grupo cíclico, então existe um gerador para G, isto é, $a \in G$ tal que

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

Exercício

Todo grupo cíclico é abeliano.

Prova:

Se G é um grupo cíclico, então existe um gerador para G, isto é, $a \in G$ tal que

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

Sejam $x, y \in G$. Devemos mostrar: $x * y = y * x$.

Exercício

Todo grupo cíclico é abeliano.

Prova:

Se G é um grupo cíclico, então existe um gerador para G, isto é, $a \in G$ tal que

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

Sejam $x, y \in G$. Devemos mostrar: $x * y = y * x$.

$$x * y = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = y * x$$

Definição (Ordem de um elemento)

Seja G um grupo e $a \in G$. O menor valor de $n \in \mathbb{N}^*$ para o qual $a^n = e$ é chamado **ordem do elemento** *a* **em** *G. Notação: $n = o(a)$. Quando tal n não existir, dizemos que a tem* **ordem infinita**.

Exemplos

1. A ordem de $\overline{3}$ em $(\mathbb{Z}_{12}, +)$ é igual a 4, pois $(\overline{3})^4 = \overline{0}$;

Exemplos

1. A ordem de $\overline{3}$ em $(\mathbb{Z}_{12}, +)$ é igual a 4, pois $(\overline{3})^4 = \overline{0}$;
2. A ordem de i em $(\mathbb{C}^*, \cdot)$ é 4 pois $i^4 = 1$.

Exemplos

1. A ordem de $\overline{3}$ em $(\mathbb{Z}_{12}, +)$ é igual a 4, pois $(\overline{3})^4 = \overline{0}$;
2. A ordem de i em $(\mathbb{C}^*, \cdot)$ é 4 pois $i^4 = 1$.
3. A ordem de 1 em $(\mathbb{Z}, +)$ é infinita pois $n.1 \neq 0$, qualquer que seja $n \in \mathbb{N}^*$.

Exercício

Seja $a \in G$ com $o(a) = n \leq 1$ e $m \in \mathbb{Z}$. Se $a^m = e$, mostre que $n|m$.

Prova:

Exercício

Seja $a \in G$ com $o(a) = n \leq 1$ e $m \in \mathbb{Z}$. Se $a^m = e$, mostre que $n|m$.

Prova:

Suponha, por absurdo, que n não divide m. Então, a divisão de m por n é não exata, isto é, $m = q.n + r$ com $0 < r < n$.

Exercício

Seja $a \in G$ com $o(a) = n \leq 1$ e $m \in \mathbb{Z}$. Se $a^m = e$, mostre que $n|m$.

Prova:

Suponha, por absurdo, que n não divide m. Então, a divisão de m por n é não exata, isto é, $m = q.n + r$ com $0 < r < n$.

Daí, $e = a^m = a^{q.n+r} = a^q n * a^r = (a^n)^q * a^r = e * a^r = a^r$

Exercício

Seja $a \in G$ com $o(a) = n \leq 1$ e $m \in \mathbb{Z}$. Se $a^m = e$, mostre que $n|m$.

Prova:

Suponha, por absurdo, que n não divide m. Então, a divisão de m por n é não exata, isto é, $m = q.n + r$ com $0 < r < n$.

Daí, $e = a^m = a^{q.n+r} = a^q n * a^r = (a^n)^q * a^r = e * a^r = a^r$

Ou seja, $a^r = e$ com $r < n$. Contradição!

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

$$\underbrace{(ab)(ab)...(ab)}_{\text{n vezes}} = e$$

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

$$\underbrace{(ab)(ab)...(ab)}_{\text{n vezes}} = e$$

Sendo G um grupo, existem a^{-1} e b^{-1}. Isto é,

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

$$\underbrace{(ab)(ab)...(ab)}_{\text{n vezes}} = e$$

Sendo G um grupo, existem a^{-1} e b^{-1}. Isto é,

$$a^{-1}(ab)(ab)...(ab)b^{-1} = a^{-1}eb^{-1}$$

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

$$\underbrace{(ab)(ab)...(ab)}_{\text{n vezes}} = e$$

Sendo G um grupo, existem a^{-1} e b^{-1}. Isto é,

$$a^{-1}(ab)(ab)...(ab)b^{-1} = a^{-1}eb^{-1}$$

$$\underbrace{(ba)(ba)...(ba)}_{\text{n-1 vezes}} = a^{-1}b^{-1} = (ba)^{-1}$$

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

$$\underbrace{(ab)(ab)...(ab)}_{\text{n vezes}} = e$$

Sendo G um grupo, existem a^{-1} e b^{-1}. Isto é,

$$a^{-1}(ab)(ab)...(ab)b^{-1} = a^{-1}eb^{-1}$$

$$\underbrace{(ba)(ba)...(ba)}_{\text{n-1 vezes}} = a^{-1}b^{-1} = (ba)^{-1}$$

$$(ba)\underbrace{(ba)(ba)...(ba)}_{\text{n-1 vezes}} = (ba)(ba)^{-1}$$

Exercício

Sejam a, b elementos de um grupo G. Se $a * b$ tem ordem finita, mostre que $b * a$ também tem ordem finita.

Prova:

Hipótese: existe $n \in \mathbb{N}^*$ tal que $(a * b)^n = e$. Ou seja,

$$\underbrace{(ab)(ab)...(ab)}_{\text{n vezes}} = e$$

Sendo G um grupo, existem a^{-1} e b^{-1}. Isto é,

$$a^{-1}(ab)(ab)...(ab)b^{-1} = a^{-1}eb^{-1}$$

$$\underbrace{(ba)(ba)...(ba)}_{\text{n-1 vezes}} = a^{-1}b^{-1} = (ba)^{-1}$$

$$(ba)\underbrace{(ba)(ba)...(ba)}_{\text{n-1 vezes}} = (ba)(ba)^{-1}$$

$$(ba)^n = e$$