Grupos - Introdução

José Antônio O. Freitas

MAT-UnB

19 de outubro de 2020

Definição

Seja $G \neq \emptyset$

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$

Definição

Seja $G \neq \emptyset$ um conjunto no qual está definida uma operação binária $*$ tal que:

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x, y, $z \in G$:

Definição

Seja $G \neq \emptyset$ um conjunto no qual está definida uma operação binária $*$ tal que:

i) Para todos x, y, $z \in G$:

$$(x * y) * z$$

Definição

Seja $G \neq \emptyset$ um conjunto no qual está definida uma operação binária $*$ tal que:

i) *Para todos x, y, $z \in G$:*

$$(x * y) * z = x * (y * z).$$

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos $x,\ y,\ z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$

Definição

Seja $G \neq \emptyset$ um conjunto no qual está definida uma operação binária $*$ tal que:

i) Para todos x, y, $z \in G$:

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ tal que

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x, y, $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e$$

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x*,* y*,* $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e = x =$$

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x*,* y*,* $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e = x = e * x$$

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x, y, $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e = x = e * x$$

para todo $x \in G$.

Definição

Seja $G \neq \emptyset$ um conjunto no qual está definida uma operação binária $*$ tal que:

i) Para todos x, y, $z \in G$:

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ tal que

$$x * e = x = e * x$$

para todo $x \in G$. Tal elemento e

Definição

Seja $G \neq \emptyset$ um conjunto no qual está definida uma operação binária $*$ tal que:

i) Para todos x, y, $z \in G$:

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ tal que

$$x * e = x = e * x$$

*para todo $x \in G$. Tal elemento e é chamado de **elemento neutro***

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x*,* y*,* $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e = x = e * x$$

para todo $x \in G$*. Tal elemento* e *é chamado de* ***elemento neutro*** *ou* ***unidade***

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x*,* y*,* $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e = x = e * x$$

para todo $x \in G$*. Tal elemento* e *é chamado de* ***elemento neutro*** *ou* ***unidade*** *de* G*.*

Definição

Seja $G \neq \emptyset$ *um conjunto no qual está definida uma operação binária* $*$ *tal que:*

i) Para todos x*,* y*,* $z \in G$*:*

$$(x * y) * z = x * (y * z).$$

ii) Existe $e \in G$ *tal que*

$$x * e = x = e * x$$

para todo $x \in G$*. Tal elemento* e *é chamado de* ***elemento neutro*** *ou* ***unidade*** *de* G*.*

Definição

iii) Para cada $x \in G$,

Definição

iii) Para cada $x \in G$*, existe* $y \in G$

Definição

iii) Para cada $x \in G$*, existe* $y \in G$ *tal que*

Definição

iii) Para cada $x \in G$*, existe* $y \in G$ *tal que*

$$x * y$$

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e =$$

Definição

iii) Para cada $x \in G$*, existe* $y \in G$ *tal que*

$$x * y = e = y * x.$$

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

O elemento y

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

O elemento y é chamado de ***inverso***

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

*O elemento y é chamado de **inverso** ou **oposto***

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

*O elemento y é chamado de **inverso** ou **oposto** de x.*

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

O elemento y é chamado de ***inverso*** *ou* ***oposto*** *de x.*

Nesse caso dizemos que o par $(G, *)$

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

*O elemento y é chamado de **inverso** ou **oposto** de x.*

*Nesse caso dizemos que o par $(G, *)$ é um **grupo**.*

Definição

iii) Para cada $x \in G$, existe $y \in G$ tal que

$$x * y = e = y * x.$$

*O elemento y é chamado de **inverso** ou **oposto** de x.*

*Nesse caso dizemos que o par $(G, *)$ é um **grupo**.*

Observação:

Quando $*$ *é uma "soma",*

Observação:

*Quando $*$ é uma "soma", dizemos que $(G, *)$ é um **grupo aditivo**.*

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação",

Observação:

*Quando $*$ é uma "soma", dizemos que $(G, *)$ é um **grupo aditivo**.*

*Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um **grupo multiplicativo**.*

Observação:

*Quando $*$ é uma "soma", dizemos que $(G, *)$ é um **grupo aditivo**.*

*Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um **grupo multiplicativo**.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo***.

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo***.

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo****.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

Um grupo $(G, *)$

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo****.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

Um grupo $(G, *)$ é chamado de ***grupo comutativo***

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo****.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

Um grupo $(G, *)$ é chamado de ***grupo comutativo*** *ou* ***abeliano***

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo****.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

Um grupo $(G, *)$ é chamado de ***grupo comutativo*** *ou* ***abeliano*** *quando $*$ é comutativa,*

Observação:

Quando $*$ é uma "soma", dizemos que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo****.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

Um grupo $(G, *)$ é chamado de ***grupo comutativo*** *ou* ***abeliano*** *quando $*$ é comutativa, ou seja, quando*

Observação:

*Quando $*$ é uma "soma", dizem que $(G, *)$ é um **grupo aditivo**.*

*Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um **grupo multiplicativo**.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

*Um grupo $(G, *)$ é chamado de **grupo comutativo** ou **abeliano** quando $*$ é comutativa, ou seja, quando*

$$x * y =$$

Observação:

Quando $*$ é uma "soma", dizem que $(G, *)$ é um ***grupo aditivo****.*

Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um ***grupo multiplicativo****.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

Um grupo $(G, *)$ é chamado de ***grupo comutativo*** *ou* ***abeliano*** *quando $*$ é comutativa, ou seja, quando*

$$x * y = y * x$$

Observação:

*Quando $*$ é uma "soma", dizemos que $(G, *)$ é um **grupo aditivo**.*

*Se $*$ é uma "multiplicação", dizemos que $(G, *)$ é um **grupo multiplicativo**.*

Além disso, quando não houver chance de confusão com relação à operação do grupo $(G, *)$ vamos dizer simplesmente que G é um grupo.

Definição

*Um grupo $(G, *)$ é chamado de **grupo comutativo** ou **abeliano** quando $*$ é comutativa, ou seja, quando*

$$x * y = y * x$$

para todos x, $y \in G$.

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

2) $(\mathbb{Z}, \cdot)$ *não é grupo.*

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

2) $(\mathbb{Z}, \cdot)$ *não é grupo.*

3) $(\mathbb{Q}, +)$ *é um grupo abeliano.*

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

2) $(\mathbb{Z}, \cdot)$ *não é grupo.*

3) $(\mathbb{Q}, +)$ *é um grupo abeliano.*

4) $(\mathbb{Q}^*, \cdot)$ *é um grupo abeliano.*

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

2) $(\mathbb{Z}, \cdot)$ *não é grupo.*

3) $(\mathbb{Q}, +)$ *é um grupo abeliano.*

4) $(\mathbb{Q}^*, \cdot)$ *é um grupo abeliano.*

5) $(\mathbb{R}, +)$ *é um grupo abeliano.*

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

2) $(\mathbb{Z}, \cdot)$ *não é grupo.*

3) $(\mathbb{Q}, +)$ *é um grupo abeliano.*

4) $(\mathbb{Q}^*, \cdot)$ *é um grupo abeliano.*

5) $(\mathbb{R}, +)$ *é um grupo abeliano.*

6) $(\mathbb{R}^*, \cdot)$ *é um grupo abeliano.*

Exemplos

1) $(\mathbb{Z}, +)$ *é um grupo abeliano.*

2) $(\mathbb{Z}, \cdot)$ *não é grupo.*

3) $(\mathbb{Q}, +)$ *é um grupo abeliano.*

4) $(\mathbb{Q}^*, \cdot)$ *é um grupo abeliano.*

5) $(\mathbb{R}, +)$ *é um grupo abeliano.*

6) $(\mathbb{R}^*, \cdot)$ *é um grupo abeliano.*

7) $(\mathbb{C}, +)$ *é um grupo abeliano.*

Exemplos

1) $(\mathbb{Z},+)$ *é um grupo abeliano.*

2) $(\mathbb{Z},\cdot)$ *não é grupo.*

3) $(\mathbb{Q},+)$ *é um grupo abeliano.*

4) $(\mathbb{Q}^*,\cdot)$ *é um grupo abeliano.*

5) $(\mathbb{R},+)$ *é um grupo abeliano.*

6) $(\mathbb{R}^*,\cdot)$ *é um grupo abeliano.*

7) $(\mathbb{C},+)$ *é um grupo abeliano.*

8) $(\mathbb{C}^*,\cdot)$ *é um grupo abeliano.*

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) Considere o conjunto dos números reais $\mathbb{R}$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y =$$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$.

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x, \ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

11) $(\mathbb{Z}_m - \{\bar{0}\}, \otimes)$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

11) $(\mathbb{Z}_m - \{\bar{0}\}, \otimes)$ *é grupo?*

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

11) $(\mathbb{Z}_m - \{\bar{0}\}, \otimes)$ *é grupo?*

12) $(\mathbb{R}, *)$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

11) $(\mathbb{Z}_m - \{\bar{0}\}, \otimes)$ *é grupo?*

12) $(\mathbb{R}, *)$ *onde* $x * y = y$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

11) $(\mathbb{Z}_m - \{\bar{0}\}, \otimes)$ *é grupo?*

12) $(\mathbb{R}, *)$ *onde* $x * y = y$ *para todos* $x,\ y \in \mathbb{R}$

Exemplos

9) $(\mathbb{Z}_m, \oplus)$ *é grupo abeliano.*

10) *Considere o conjunto dos números reais* $\mathbb{R}$ *com a operação* $*$ *definida por*

$$x * y = x + y - 3$$

para $x,\ y \in \mathbb{R}$. *Então* $(\mathbb{R}, *)$ *é um grupo abeliano.*

11) $(\mathbb{Z}_m - \{\overline{0}\}, \otimes)$ *é grupo?*

12) $(\mathbb{R}, *)$ *onde* $x * y = y$ *para todos* $x,\ y \in \mathbb{R}$ *é grupo?*

Exemplos

13) Denote por $\mathbb{K}$ *um dos conjuntos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *ou* $\mathbb{C}$, *indistintamente. Seja*

$$M_{r\times s}(\mathbb{K}) = \{A \mid A \textit{ é uma matriz de } r \textit{ linhas por } s \textit{ colunas cujas entradas estão em } \mathbb{K}\}.$$

Então $(M_{r\times s}(\mathbb{K}), +)$ *onde* $+$ *é a soma de matrizes é um grupo abeliano.*

14) Denote por $\mathbb{K}$ *um dos conjuntos* $\mathbb{Q}$, $\mathbb{R}$ *ou* $\mathbb{C}$, *indistintamente. Seja*

$$GL_n(\mathbb{K}) = \{A \in M_{n\times n}(\mathbb{K}) \mid \det(A) = 1\}.$$

Então $(GL_n(\mathbb{K}), \cdot)$ *onde* $\cdot$ *é a multiplicação de matrizes é um grupo não abeliano.*

Proposição

Seja $(G, *)$ *um grupo.*

Proposição

Seja $(G, *)$ *um grupo. Então:*

Proposição

Seja $(G, *)$ *um grupo. Então:*

i) O elemento neutro de G é único.

Proposição

Seja $(G, *)$ um grupo. Então:

i) O elemento neutro de G é único.

ii) Existe um único inverso para cada $x \in G$.

Proposição

Seja $(G, *)$ um grupo. Então:

i) O elemento neutro de G é único.

ii) Existe um único inverso para cada $x \in G$.

Proposição

iii) Para todos $x, y \in G$,

Proposição

iii) Para todos $x, y \in G$,

$$(x * y)^{-1}$$

Proposição

iii) Para todos $x, y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Proposição

iii) Para todos $x, y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução,

Proposição

iii) Para todos x, $y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1, x_2, ..., x_{n-1}, x_n \in G$,

Proposição

iii) Para todos $x,\ y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1,\ x_2,\ ...,x_{n-1},\ x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} =$$

Proposição

iii) Para todos x, $y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, x_1, x_2, ...,x_{n-1}, $x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1}$$

Proposição

iii) Para todos $x,\ y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1,\ x_2,\ \ldots, x_{n-1},\ x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1}$$

Proposição

iii) Para todos x, $y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, x_1, x_2, ...,x_{n-1}, $x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots *$$

Proposição

iii) Para todos $x,\ y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1,\ x_2,\ ..., x_{n-1},\ x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_2^{-1}$$

Proposição

iii) Para todos $x, y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1, x_2, \dots, x_{n-1}, x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_2^{-1} * x_1^{-1}$$

Proposição

iii) Para todos $x,\ y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1,\ x_2,\ ...,x_{n-1},\ x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_2^{-1} * x_1^{-1}$$

iv) Para todo $x \in G$,

Proposição

iii) Para todos $x, y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1, x_2, ..., x_{n-1}, x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_2^{-1} * x_1^{-1}$$

iv) Para todo $x \in G$,

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

Proposição

iii) Para todos $x, y \in G$,

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Por indução, $x_1, x_2, ..., x_{n-1}, x_n \in G$,

$$(x_1 * x_2 * \cdots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \cdots * x_2^{-1} * x_1^{-1}$$

iv) Para todo $x \in G$,

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