Estruturas Discretas

Estruturas Algébricas

Profa. Helena Caseli
helenacaseli@dc.ufscar.br

Estruturas Algébricas

- **Conceitualização**
  - Englobam conjuntos de objetos e as operações que podem ser realizadas com esses objetos
    - Tratam das propriedades de operações binárias definidas sobre um conjunto específico
    - Por exemplo, a adição de inteiros
    - Combinam conteúdo visto anteriormente neste curso:
      - Teoria dos Conjuntos
      - Funções
      - Teoria dos Números

Estruturas Algébricas

- **Estrutura Algébrica**
  - Operação
  - Propriedades das operações
  - Grupo
  - Grupo comutativo
  - Semigrupo
  - Monoide
  - Subgrupo
  - Isomorfismo de grupo
  - Anel
  - Corpo

Estruturas Algébricas

- **Operação**
  - Até aqui
    - Aprendemos operações como:
      - adição e divisão de números inteiros;
      - $\oplus$ e $\otimes$ no conjunto Z_n

Estruturas Algébricas

- **Operação**
  - Até aqui
    - Aprendemos operações como:
      - adição e divisão de números inteiros;
      - $\oplus$ e $\otimes$ no conjunto Z_n
  - Neste curso
    - Estudaremos com maior profundidade, e de forma genérica, operações definidas sobre conjuntos e suas propriedades algébricas

Estruturas Algébricas

- **Operação**
  - Definição
    - Seja A um conjunto. Uma **operação** em A é uma função cujo domínio contém $A \times A$
      - Assim, uma operação é uma função cuja entrada é um par de elementos de A

Estruturas Algébricas

- **Operação**
  - Definição
    - Seja A um conjunto. Uma **operação** em A é uma função cujo domínio contém $A \times A$
      - Assim, uma operação é uma função cuja entrada é um par de elementos de A
  - ➔ Essa definição implica:
    1.
    2.
    3.

Estruturas Algébricas

- **Operação**
  - Definição
    - Seja A um conjunto. Uma **operação** em A é uma função cujo domínio contém $A \times A$
      - Assim, uma operação é uma função cuja entrada é um par de elementos de A

  → Essa definição implica:

  1. A operação está definida para todo par de elementos de A (caso contrário, não seria função)
  2.
  3.

Estruturas Algébricas

- **Operação**
  - Definição
    - Seja A um conjunto. Uma **operação** em A é uma função cujo domínio contém $A \times A$
      - Assim, uma operação é uma função cuja entrada é um par de elementos de A

  → Essa definição implica:

  1. A operação está definida para todo par de elementos de A (caso contrário, não seria função)
  2. O resultado da operação é único para cada entrada (caso contrário não seria função)
  3.

Estruturas Algébricas

- **Operação**
  - Definição
    - Seja A um conjunto. Uma **operação** em A é uma função cujo domínio contém $A \times A$
      - Assim, uma operação é uma função cuja entrada é um par de elementos de A

  → Essa definição implica:

  1. A operação está definida para todo par de elementos de A (caso contrário, não seria função)
  2. O resultado da operação é único para cada entrada (caso contrário não seria função)
  3. O resultado não está necessariamente em A. Se estiver, dizemos que a operação tem uma propriedade particular de fechamento

Estruturas Algébricas

1. A operação está definida para todo par de elementos de A
2. O resultado da operação é único para cada entrada

- **Operação**
  - Exemplos
    - Quais das operações +, -, ×, ÷ são operações em $\mathbb{N}$?
      - Adição?

Estruturas Algébricas

1. A operação está definida para todo par de elementos de A
2. O resultado da operação é único para cada entrada

- **Operação**
  - Exemplos
    - Quais das operações +, -, ×, ÷ são operações em ℕ?
      - Adição: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Multiplicação?

Estruturas Algébricas

1. A operação está definida para todo par de elementos de A
2. O resultado da operação é único para cada entrada

- **Operação**
  - Exemplos
    - Quais das operações +, -, ×, ÷ são operações em $\mathbb{N}$?
      - Adição: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Multiplicação: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Subtração?

Estruturas Algébricas

1. A operação está definida para todo par de elementos de A
2. O resultado da operação é único para cada entrada

- **Operação**
  - Exemplos
    - Quais das operações +, -, ×, ÷ são operações em ℕ?
      - Adição: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Multiplicação: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Subtração: SIM

        Porém o resultado pode não ser um elemento de ℕ
      - Divisão?

Estruturas Algébricas

1. A operação está definida para todo par de elementos de A
2. O resultado da operação é único para cada entrada

- **Operação**
  - Exemplos
    - Quais das operações +, -, ×, ÷ são operações em ℕ?
      - Adição: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Multiplicação: SIM

        Função cujo domínio inclui qualquer par de números naturais
      - Subtração: SIM

        Porém o resultado pode não ser um elemento de ℕ
      - Divisão: NÃO

        Divisão por zero não é definida

Estruturas Algébricas

- **Operação**
  - Exemplo
    - Seja f: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $f(a, b) = |a - b|$
      - A função f dá a distância entre a e b
      - Dizemos que f é uma operação em $\mathbb{Z}$
    - Notação
      - A notação f(a,b) está correta, mas geralmente escrevemos um símbolo da operação entre os dois elementos:

$$a \; f \; b$$

Símbolo para denotar uma operação genérica é *

Assim, ao invés de $f(a, b) = |a - b|$

Podemos escrever $a * b = |a - b|$

Estruturas Algébricas

- **Propriedades das operações**

Estruturas Algébricas

- **Propriedades das operações**
  - **Propriedade Comutativa**
    - Seja * uma operação sobre um conjunto *A*. Dizemos que * é **comutativa** sobre *A* se e somente se

$$\forall\, a, b \in A, a * b = b * a$$

Estruturas Algébricas

- **Propriedades das operações**
  - **Propriedade Comutativa**
    - Seja * uma operação sobre um conjunto *A*. Dizemos que * é **comutativa** sobre *A* se e somente se

$$\forall a, b \in A, a * b = b * a$$

  - **Propriedade de Fechamento**
    - Seja * uma operação sobre um conjunto A. Dizemos que * é **fechada** em A se e somente se

$$\forall a, b \in A, a * b \in A$$

Obs.: A subtração não é fechada em $\mathbb{N}$, mas é fechada em $\mathbb{Z}$

Estruturas Algébricas

- **Propriedades das operações**
  - **Propriedade Associativa**
    - Seja * uma operação sobre um conjunto *A*. Dizemos que * é **associativa** em *A* se e somente se

$$\forall\, a, b, c \in A, (a * b) * c = a * (b * c)$$

Estruturas Algébricas

- **Propriedades das operações**
  - **Propriedade Associativa**
    - Seja * uma operação sobre um conjunto *A*. Dizemos que * é **associativa** em *A* se e somente se

$$\forall\, a, b, c \in A, (a * b)*c = a*(b * c)$$

Obs.: As operações + e × são associativas mas a subtração não

- Exemplo
  - Considere a operação de subtração sobre $\mathbb{Z}$

    $(2 – 5) – 4 = -7$

    Mas $2 – (5 – 4) = 1$

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Seja * uma operação sobre um conjunto *A*. Um elemento $e \in A$ é chamado **elemento identidade** (ou simplesmente **identidade**) para * desde que

$$\forall\, a \in A,\ a * e = e * a = a$$

Obs.: Os elementos identidades devem "funcionar" em ambos os lados da operação

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Seja * uma operação sobre um conjunto *A*. Um elemento $e \in A$ é chamado **elemento identidade** (ou simplesmente **identidade**) para * desde que

$$\forall\, a \in A,\ a * e = e * a = a$$

Obs.: Os elementos identidades devem "funcionar" em ambos os lados da operação

    - Exemplos
      - Considere o conjunto $\mathbb{Z}$

        O elemento identidade para + é ?

        O elemento identidade para $\times$ é ?

        O elemento identidade para – é ?

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Seja * uma operação sobre um conjunto *A*. Um elemento $e \in A$ é chamado **elemento identidade** (ou simplesmente **identidade**) para * desde que

$$\forall\, a \in A,\ a * e = e * a = a$$

Obs.: Os elementos identidades devem "funcionar" em ambos os lados da operação

    - Exemplos
      - Considere o conjunto $\mathbb{Z}$

        O elemento identidade para + é 0

        O elemento identidade para $\times$ é 1

        O elemento identidade para – é … a subtração de inteiros não tem elemento identidade!

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Proposição
      - Seja * uma operação definida em um conjunto *A*
      - Então, * pode ter no máximo um elemento identidade

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Proposição
      - Seja * uma operação definida em um conjunto *A*
      - Então, * pode ter no máximo um elemento identidade

Prova:
Seja * uma operação definida em um conjunto A. Vamos mostrar que * pode ter no máximo um elemento identidade.

Logo, só há um elemento identidade para * em A. ■

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Proposição
      - Seja * uma operação definida em um conjunto *A*
      - Então, * pode ter no máximo um elemento identidade

Prova:
Seja * uma operação definida em um conjunto A. Vamos mostrar que * pode ter no máximo um elemento identidade.
Suponha, por contradição que haja dois elementos identidade **e** e **e'** em A, com **e** ≠ **e'.**

Logo, só há um elemento identidade para * em A. ■

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Proposição
      - Seja * uma operação definida em um conjunto *A*
      - Então, * pode ter no máximo um elemento identidade

Prova:
Seja * uma operação definida em um conjunto A. Vamos mostrar que * pode ter no máximo um elemento identidade.
Suponha, por contradição que haja dois elementos identidade **e** e **e'** em A, com **e** ≠ **e'.**
Considere e * e'.

Logo, só há um elemento identidade para * em A. ■

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Proposição
      - Seja * uma operação definida em um conjunto *A*
      - Então, * pode ter no máximo um elemento identidade

Prova:
Seja * uma operação definida em um conjunto A. Vamos mostrar que * pode ter no máximo um elemento identidade.
Suponha, por contradição que haja dois elementos identidade **e** e **e'** em A, com **e ≠ e'.**
Considere e * e'.
Como e é um elemento identidade, e * e' = e'.
Como e' é um elemento identidade, e * e' = e.

Logo, só há um elemento identidade para * em A. ■

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento identidade**
    - Proposição
      - Seja * uma operação definida em um conjunto *A*
      - Então, * pode ter no máximo um elemento identidade

Prova:
Seja * uma operação definida em um conjunto A. Vamos mostrar que * pode ter no máximo um elemento identidade.
Suponha, por contradição que haja dois elementos identidade **e** e **e'** em A, com **e ≠ e'.**
Considere e * e'.
Como e é um elemento identidade, e * e' = e'.
Como e' é um elemento identidade, e * e' = e.
Então temos que e' = e * e' = e uma contradição à hipótese e ≠ e'.
Logo, só há um elemento identidade para * em A. ■

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento inverso**
    - Seja * uma operação sobre um conjunto *A* e suponha que *A* tenha o elemento identidade e
    - Seja $a \in A$
      - Dizemos que *b* (ou a^{-1}) é um inverso de *a* se e somente se

$$\boldsymbol{a * b = b * a = e}$$

Obs.: O inverso de um elemento deve "funcionar" em ambos os lados da operação

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento inverso**
    - Exemplos
      - Considere a operação + sobre os inteiros ($\mathbb{Z}$)

        O elemento identidade para + é o 0

        Todo inteiro a tem um inverso:

        a + (-a) = (-a) + a = 0

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento inverso**
    - Exemplos
      - Considere a operação + sobre os inteiros ($\mathbb{Z}$)

        O elemento identidade para + é o 0

        Todo inteiro a tem um inverso:

        a + (-a) = (-a) + a = 0

      - Considere a operação * sobre os racionais (Q)

        O elemento identidade para multiplicação é o 1

        Quase todos os números racionais têm um inverso:

        Se $x \in Q$, então 1/x é o inverso de x, exceto quando x = 0

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento inverso**
    - Para a maioria das operações conhecidas, os elementos têm no máximo um inverso
    - Exemplos:

      Se $a \in \mathbb{Z}$, existe um único b tal que $a+b = 0$

      Se $a \in Q$, existe no máximo um número racional b tal que $ab=1$

      Se a $\in \mathbb{Z}_n$, existe no máximo um b $\in \mathbb{Z}_n$, tal que $a \otimes b = 1$

  - ➔ Mas é possível que um elemento tenha mais que um inverso!

Estruturas Algébricas

- **Propriedades das operações**
  - **Elemento inverso**
    - Não precisa ser único – Exemplo
      - Operação * definida em {*a, b, c, e*}

*	*e*	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*a*	***e***	***e***
b	*b*	***e***	*b*	*e*
c	*c*	***e***	*e*	*c*

      - O elemento ***e*** é um elemento identidade. Tanto ***b*** como ***c*** são inversos de ***a***, pois

a*b = b*a = e **e** ***a*c = c*a = e***

Estruturas Algébricas

- **Grupo**

Estruturas Algébricas

- **Grupo**
  - Seja * uma operação definida em um conjunto *G*
  - Dizemos que o par *(G,*)* é um **grupo** se e somente se:

1.

2.

3.

4.

Estruturas Algébricas

- **Grupo**
  - Seja * uma operação definida em um conjunto *G*
  - Dizemos que o par *(G,*)* é um **grupo** se e somente se:

1. O conjunto *G* é **fechado** sob a operação *, isto é,

$$\forall\, g, h \in G, g*h \in G$$

2.

3.

4.

Estruturas Algébricas

- **Grupo**
  - Seja * uma operação definida em um conjunto *G*
  - Dizemos que o par *(G,*)* é um **grupo** se e somente se:

  1. O conjunto *G* é **fechado** sob a operação *, isto é,

$$\forall\, g, h \in G,\ g*h \in G$$

  2. A operação * é **associativa**, isto é,

$$\forall\, g, h, k \in G,\ (g*h)*k = g*(h*k)$$

  3.

  4.

Estruturas Algébricas

- **Grupo**
  - Seja * uma operação definida em um conjunto *G*
  - Dizemos que o par *(G,*)* é um **grupo** se e somente se:

1. O conjunto *G* é **fechado** sob a operação *, isto é,

$$\forall\, g, h \in G,\ g*h \in G$$

2. A operação * é **associativa**, isto é,

$$\forall\, g, h, k \in G,\ (g*h)*k = g*(h*k)$$

3. Existe **um único elemento identidade** $e \in G$ para *, isto é,

$$\exists\, e \in G,\ \forall\, g \in G,\ g*e = e*g = g$$

4.

Estruturas Algébricas

- **Grupo**
  - Seja * uma operação definida em um conjunto *G*
  - Dizemos que o par *(G,*)* é um **grupo** se e somente se:

  1. O conjunto *G* é **fechado** sob a operação *, isto é,

$$\forall\, g, h \in G,\ g*h \in G$$

  2. A operação * é **associativa**, isto é,

$$\forall\, g, h, k \in G,\ (g*h)*k = g*(h*k)$$

  3. Existe **um único elemento identidade** $e \in G$ para *, isto é,

$$\exists\, e \in G,\ \forall\, g \in G,\ g*e = e*g = g$$

  4. Para todo elemento $g \in G$ existe **um único elemento inverso** $h \in G$, isto é,

$$\forall\, g \in G,\ \exists\, h \in G,\ g*h = h*g = e$$

Estruturas Algébricas

- **Grupo**
  - Exemplos
    - Grupo
      - $(\mathbb{Z}, +)$ é um grupo referido como “inteiros com adição”
      - (Q,+) racionais com adição
      - $(Q^{+},\times)$ racionais positivos com multiplicação
      - $(Q - \{0\},\times)$ racionais sem o zero com multiplicação

Estruturas Algébricas

- **Grupo**
  - Exemplos
    - Grupo
      - $(\mathbb{Z}, +)$ é um grupo referido como “inteiros com adição”
      - $(Q,+)$ racionais com adição
      - $(Q^+,\times)$ racionais positivos com multiplicação
      - $(Q - \{0\},\times)$ racionais sem o zero com multiplicação
    - Não Grupo
      - O exemplo dado anteriormente - operação * definida em $\{a, b, c, e\}$ não é um grupo, pois o elemento a tem dois inversos
      - $(Q,\times)$ racionais com multiplicação NÃO formam um grupo, pois $0 \in Q$ não tem inverso

Estruturas Algébricas

- **Unicidade de inversos**
  - Em um grupo, todo elemento tem um inverso e esse inverso é único

Estruturas Algébricas

- **Unicidade de inversos**
  - Em um grupo, todo elemento tem um inverso e esse inverso é único
  - **Proposição**
    - Seja (*G*,*) um grupo. Todo elemento de *G* tem um inverso único em *G*

Estruturas Algébricas

- **Unicidade de inversos**
  - Em um grupo, todo elemento tem um inverso e esse inverso é único
  - **Proposição**
    - Seja (*G*,*) um grupo. Todo elemento de *G* tem um inverso único em *G*
    - Prova
      - ➔ Sabemos, por definição, que todo elemento em G tem um inverso. A questão é se é ou não possível um elemento de G ter dois (ou mais) inversos.

Estruturas Algébricas

- **Unicidade de inversos**
  - **Proposição**
    - Seja (*G*,*) um grupo. Todo elemento de *G* tem um inverso único em *G*

Prova:
Seja (G, *) um grupo. Vamos mostrar que todo elemento de G tem um inverso único em G.

Logo, em (G,*) todo elemento tem um inverso e ele é único. ■

Estruturas Algébricas

- **Unicidade de inversos**
  - **Proposição**
    - Seja (G,*) um grupo. Todo elemento de G tem um inverso único em G

Prova:
Seja (G, *) um grupo. Vamos mostrar que todo elemento de G tem um inverso único em G.

Suponhamos, por contradição, que $g \in G$ tenha dois inversos distintos h e k. Isto significa

$$g*h = h*g = g*k = k*g = e$$

onde $e \in G$ é o elemento identidade para *.

Logo, em (G,*) todo elemento tem um inverso e ele é único. ■

Estruturas Algébricas

- **Unicidade de inversos**
  - **Proposição**
    - Seja (G,*) um grupo. Todo elemento de G tem um inverso único em G

Prova:
Seja (G, *) um grupo. Vamos mostrar que todo elemento de G tem um inverso único em G.

Suponhamos, por contradição, que $g \in G$ tenha dois inversos distintos h e k. Isto significa

$$g*h = h*g = g*k = k*g = e$$

onde $e \in G$ é o elemento identidade para *. Pela propriedade associativa,

$$h*(g*k) = (h*g)*k.$$

Logo, em (G,*) todo elemento tem um inverso e ele é único. ■

Estruturas Algébricas

- **Unicidade de inversos**
  - **Proposição**
    - Seja (*G*,*) um grupo. Todo elemento de *G* tem um inverso único em *G*

Prova:
Seja (G, *) um grupo. Vamos mostrar que todo elemento de G tem um inverso único em G.

Suponhamos, por contradição, que $g \in G$ tenha dois inversos distintos h e k. Isto significa

$$g*h = h*g = g*k = k*g = e$$

onde $e \in G$ é o elemento identidade para *. Pela propriedade associativa,

$$h*(g*k) = (h*g)*k.$$

Além disso,

$$h*(g*k) = h*e = h \qquad \text{e} \qquad (h*g)*k = e*k = k.$$

Logo, em (G,*) todo elemento tem um inverso e ele é único. ■

Estruturas Algébricas

- **Unicidade de inversos**
  - **Proposição**
    - Seja (G,*) um grupo. Todo elemento de G tem um inverso único em G

Prova:
Seja (G, *) um grupo. Vamos mostrar que todo elemento de G tem um inverso único em G.

Suponhamos, por contradição, que $g \in G$ tenha dois inversos distintos h e k. Isto significa

$$g*h = h*g = g*k = k*g = e$$

onde $e \in G$ é o elemento identidade para *. Pela propriedade associativa,

$$h*(g*k) = (h*g)*k.$$

Além disso,

$$h*(g*k) = h*e = h \qquad \text{e} \qquad (h*g)*k = e*k = k.$$

Logo, $h=k$, contradizendo o fato que $h \neq k$.

Logo, em (G,*) todo elemento tem um inverso e ele é único. ■

Estruturas Algébricas

- **Grupo**
  - $(\mathbb{Z}_n,\otimes)$ não é um grupo, por que o 0 não tem inverso (não existe b tal que $0\otimes b=1$)
  - Quais elementos precisam ser removidos de $\mathbb{Z}_n$ para que $(\mathbb{Z}_n,\otimes)$ seja um grupo?

Estruturas Algébricas

- **Grupo**
  - $(\mathbb{Z}_n, \otimes)$ não é um grupo, por que o 0 não tem inverso (não existe b tal que $0 \otimes b = 1$)
  - Quais elementos precisam ser removidos de $\mathbb{Z}_n$ para que $(\mathbb{Z}_n, \otimes)$ seja um grupo?
    - Se quisermos eliminar elementos de $\mathbb{Z}_n$ para obter um grupo, o problema não é tão simples: não podemos simplesmente descartar o 0
    - Em $(\mathbb{Z}_{10} - \{0\}, \otimes)$ a operação $\otimes$ não é fechada, pois:

      $$\mathbf{2, 5 \in \mathbb{Z}_{10} - \{0\} \text{ mas } 2 \otimes 5 = 0 \notin Z_{10} - \{0\}}$$

    - Além disso, 2 e 5 não têm inverso

Estruturas Algébricas

- **Grupo**
  - $(\mathbb{Z}_n,\otimes)$ não é um grupo, por que o 0 não tem inverso (não existe b tal que $0\otimes b=1$)
  - Quais elementos precisam ser removidos de $\mathbb{Z}_n$ para que $(\mathbb{Z}_n,\otimes)$ seja um grupo?
    - Assim, para definir um subconjunto X de $\mathbb{Z}_n$ de maneira que $(X,\otimes)$ seja um grupo, devemos eliminar todos os elementos que não tenham inversos
    - Quais são os elementos invertíveis em $\mathbb{Z}_n$?

Estruturas Algébricas

Teorema – Elementos invertíveis em Z_n

- Seja n um inteiro positivo e seja a $\in$ Z_n
- Então, a é invertível se e somente se a e n são relativamente primos

- **Grupo**
  - ($\mathbb{Z}_n$,$\otimes$) não
    (não existe b tal que 0$\otimes$b=1)
  - Quais elementos precisam ser removidos de $\mathbb{Z}_n$ para que ($\mathbb{Z}_n$,$\otimes$) seja um grupo?
    - Assim, para definir um subconjunto X de $\mathbb{Z}_n$ de maneira que (X,$\otimes$) seja um grupo, devemos eliminar todos os elementos que não tenham inversos
    - Quais são os elementos invertíveis em $\mathbb{Z}_n$?

Estruturas Algébricas

Sejam *a* e *b* inteiros. Dizemos que *a* e *b* são **relativamente primos** (ou primos entre si) se e somente se mdc(*a*, *b*) = 1

- **Grupo**
  - $(\mathbb{Z}_n,\otimes)$ não é um grupo, por que o 0 não tem inverso (não existe b tal que $0\otimes b=1$)
  - Quais elementos precisam ser removidos de $\mathbb{Z}_n$ para que $(\mathbb{Z}_n,\otimes)$ seja um grupo?
    - Assim, para definir um subconjunto X de $\mathbb{Z}_n$ de maneira que $(X,\otimes)$ seja um grupo, devemos eliminar todos os elementos que não tenham inversos
    - Ficamos com todos os elementos que são relativamente primos com n e eliminamos os demais
    - Em $\mathbb{Z}_{10}$ ficamos com {1, 3, 7, 9}
    - $(\{1, 3, 7, 9\},\otimes)$ forma um grupo

Estruturas Algébricas

- **Grupo**
  - $(\mathbb{Z}_n,\otimes)$ não é um grupo, por que o 0 não tem inverso (não existe b tal que $0\otimes b=1$)
  - Quais elementos precisam ser removidos de $\mathbb{Z}_n$ para que $(\mathbb{Z}_n,\otimes)$ seja um grupo?
    - Tabela de operações para o grupo $(\{1, 3, 7, 9\},\otimes)$

$\otimes$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Estruturas Algébricas

- **Grupo**
  - Quais elementos precisam ser removidos de $\mathbb{Z}_8$ para que $(\mathbb{Z}_8, \otimes)$ seja um grupo?

Estruturas Algébricas

- **Grupo**
  - Quais elementos precisam ser removidos de $\mathbb{Z}_8$ para que $(\mathbb{Z}_8,\otimes)$ seja um grupo?
    - Tabela de operações para o grupo $(\{1, 3, 5, 7\},\otimes)$

$\otimes$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Estruturas Algébricas

- **Grupo**
  - Definição ($\mathbb{Z}^*_n$)
    - Seja n um inteiro positivo. Definimos

$$\mathbb{Z}^*_n = \{ a \in \mathbb{Z}_n \mid \text{mdc}(a, n) = 1\}$$

Estruturas Algébricas

- **Grupo**
  - Definição ($\mathbb{Z}^*_n$)
    - Seja n um inteiro positivo. Definimos

$$\mathbb{Z}^*_n = \{ a \in \mathbb{Z}_n \mid \text{mdc}(a, n) = 1\}$$

    - Exemplo
      - $\mathbb{Z}_{14}$ = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13}
      - Quais são os elementos invertíveis em Z_{14}?

Estruturas Algébricas

- **Grupo**
  - Definição ($\mathbb{Z}^*_n$)
    - Seja n um inteiro positivo. Definimos

$$\mathbb{Z}^*_n = \{ a \in \mathbb{Z}_n \mid \text{mdc}(a, n) = 1\}$$

    - Exemplo
      - $\mathbb{Z}_{14}$ = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13}
      - Elementos invertíveis em Z_{14} são: 1, 3, 5, 9, 11, 13

$$\mathbb{Z}^*_{14} = \{1, 3, 5, 9, 11, 13\}$$

      - Inversos

$1^{-1} = 1$ $\quad$ $3^{-1} = 5$ $\quad$ $5^{-1} = 3$

$9^{-1} = 11$ $\quad$ $11^{-1} = 9$ $\quad$ $13^{-1} = 13$

Estruturas Algébricas

- **Grupo**
  - Definição ($\mathbb{Z}^*_n$)
    - Seja n um inteiro positivo. Definimos

$$\mathbb{Z}^*_n = \{ a \in \mathbb{Z}_n \mid \text{mdc}(a, n) = 1\}$$

    - Proposição
      - Seja n um inteiro positivo. Então $(\mathbb{Z}^*_n, \otimes)$ é um grupo

Estruturas Algébricas

- **Grupo**
  - Definição ($\mathbb{Z}^*_n$)
    - Seja n um inteiro positivo. Definimos

$$\mathbb{Z}^*_n = \{ a \in \mathbb{Z}_n \mid \text{mdc}(a, n) = 1\}$$

    - Proposição
      - Seja n um inteiro positivo. Então ($\mathbb{Z}^*_n$,⊗) é um grupo
    - Exemplo:

($\mathbb{Z}^*_{14}$, ⊗)

⊗	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

1. é fechado em $\mathbb{Z}_{14}^*$
2. ⊗ é associativa
3. o elemento identidade é o 1
4. todo elemento de ($\mathbb{Z}_{14}^*$, ⊗) possui inverso (um 1 por linha)

Estruturas Algébricas

- **Grupo comutativo (ou grupo abeliano)**
  - Seja (G,*) um grupo. Dizemos que este grupo é abeliano se * é uma operação comutativa em G, isto é,

$$\forall\, g, h \in G,\ g*h = h*g$$

    - Exemplos
      - $(\mathbb{Z}, +)$ e $(\mathbb{Z}_{10}, \oplus)$ são abelianos

Estruturas Algébricas

- **Semigrupo e Monoide**
  - Seja S um conjunto não vazio com uma operação fechada em S
    - Então, S é dito um **semigrupo** se a operação é associativa
    - Se a operação também tem um elemento identidade, então S é dito um **monoide**
    - Exemplos
      - $(\mathbb{N}^+,+)$ e $(\mathbb{N}^+,\times)$ são semigrupos, pois a adição e multiplicação em $\mathbb{N}^+$ são associativas
      - $(\mathbb{N}^+,\times)$ é um monoide, pois existe o elemento identidade 1

Estruturas Algébricas

- **Resumindo**

Propriedade	Grupo comutativo	Grupo	Monoide	Monoide comutativo	Semigrupo
G é fechado sob *	X	X	X	X	X
* é associativa	X	X	X	X	X
Há elemento identidade	X	X	X	X	
Há elemento inverso	X	X			
* é comutativa	X			X	

Estruturas Algébricas

- **Subgrupo**
  - **Informalmente**
    - Um subgrupo é um grupo dentro de um grupo
    - Consideremos o grupo ($\mathbb{Z}$, +) e o conjunto de inteiros pares

$$E = \{x \in \mathbb{Z} : 2|x\}$$

    - O par (E, +) também é um grupo, pois satisfaz as 4 propriedades exigidas
    - Chamamos (E, +) de subgrupo de (Z, +)
  - **Definição**
    - Seja (G, *) um grupo, e seja $H \subseteq G$. Se (H, *) é também um grupo ele é chamado de subgrupo de (G, *)

Estruturas Algébricas

- **Subgrupo**
  - Exemplo
    - Subgrupos de $(\mathbb{Z}_{10}, \oplus)$
      - {0}
      - {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
      - {0, 5}
      - {0, 2, 4, 6, 8}

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Dois grupos são isomorfos se são exatamente o mesmo, a menos dos nomes de seus elementos
    - Considere os grupos G e H definidos como ({1, -1}, *) e ({u,v}, •), respectivamente, representados pelas tabelas abaixo

(G,∗)

*	1	-1
1	1	-1
-1	-1	1

(H,•)

°	u	v
u	u	v
v	v	u

    - Eles são isomorfos?

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Observa-se que, salvo o nome dos elementos e das operações envolvidas, os dois grupos comportam-se como se fosse o mesmo grupo
  - Algebricamente, isso ocorre por causa da bijeção
    - *f*: G → H, onde *f* é uma função que simplesmente troca os "nomes" dos elementos do grupo G
    - 1 ↔ "u" e -1 ↔ "v"
    - *f*(1) = u e *f*(-1) = v

(G,*)

*	1	-1
1	1	-1
-1	-1	1

(H,●)

°	u	v
u	u	v
v	v	u

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Definição
    - Sejam os grupos (G,*) e (H,•), diz-se que uma função f: G → H é um isomorfismo (de grupo) se e somente se:
      - f é bijetora
      - Para quaisquer que sejam x, $y \in G$,

$$f(x*y) = f(x) \bullet f(y)$$

    - Se existe um isomorfismo de G para H, diz-se que G é isomorfo a H e se escreve $G \cong H$

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Dois grupos são isomorfos se são exatamente o mesmo, a menos dos nomes de seus elementos
    - Considere os grupos: $(\mathbb{Z}_4,\oplus)$ e $(\mathbb{Z}_5^*,\otimes)$

$(\mathbb{Z}_4,\oplus)$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}^*_5,\otimes)$

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

    - Eles são isomorfos?

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Os grupos $(\mathbb{Z}_4,\oplus)$ e $(\mathbb{Z}_5^*,\otimes)$ são isomorfos pois

$(\mathbb{Z}_4,\oplus)$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	**0**
2	2	3	**0**	1
3	3	**0**	1	2

$(\mathbb{Z}^*_5, \otimes)$

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	**1**	3
3	3	**1**	4	2
4	4	3	2	**1**

  - São definidos em conjuntos diferentes, mas:
    - 1 e 3 são inversos um do outro em $\mathbb{Z}_4$
    - 2 e 3 são inversos um do outro em $\mathbb{Z}^*_5$
    - Somente 2 é seu próprio inverso em $(\mathbb{Z}_4,\oplus)$
    - Somente 4 é seu próprio inverso em $(\mathbb{Z}^*_5, \otimes)$

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Os grupos $(\mathbb{Z}_4,\oplus)$ e $(\mathbb{Z}_5^*,\otimes)$ são isomorfos pois

$(\mathbb{Z}_4,\oplus)$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	**0**
2	2	3	**0**	1
3	3	**0**	1	2

$(\mathbb{Z}^*_5, \otimes)$

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	**1**	3
3	3	**1**	4	2
4	4	3	2	**1**

  - **Podemos sobrepor as tabelas de operações de modo que elas pareçam a mesma!**

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Os grupos $(\mathbb{Z}_4,\oplus)$ e $(\mathbb{Z}_5^*,\otimes)$ são isomorfos pois

$(\mathbb{Z}_4,\oplus)$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	**0**
2	2	3	**0**	1
3	3	**0**	1	2

$(\mathbb{Z}^*_5, \otimes)$

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	**1**	3
3	3	**1**	4	2
4	4	3	2	**1**

  - **Poder rações de modo**

$(\mathbb{Z}_4,\oplus)$		$(\mathbb{Z}_5^*,\otimes)$
0	$\leftrightarrow$	1
1	$\leftrightarrow$	2
2	$\leftrightarrow$	4
3	$\leftrightarrow$	3

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Mais formalmente, esse emparelhamento pode ser definido por:
    - Seja f: $\mathbb{Z}_4 \rightarrow \mathbb{Z}_5^*$ definida por

$$f(0) = 1 \qquad f(2) = 4$$

$$f(1) = 2 \qquad f(3) = 3$$

    - f é uma bijeção e

$$f(x \oplus y) = f(x) \otimes f(y)$$

    - Os grupos $(\mathbb{Z}_4, \oplus)$ e $(\mathbb{Z}_5^*, \otimes)$ são essencialmente o mesmo grupo e são ditos isomorfos

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - Definição
    - Sejam os grupos $(G,*)$ e $(H, \bullet)$
    - Uma função $f: G \rightarrow H$ é um **isomorfismo** (de grupo) se e somente se f é um a um e sobre e verifica

$$\forall\ g, h \in G,\ f(g*h) = f(g) \bullet f(h).$$

➔ Se existe um isomorfismo de G para H, dizemos que G é isomorfo a H e escrevemos $G \cong H$

Estruturas Algébricas

- **Isomorfismo de Grupo**
  - A relação *isomorfo para grupos* é uma relação de equivalência; isto é
    - Para qualquer grupo G, $G \cong G$, (reflexiva)
    - Para dois grupos quaisquer G e H, se $G \cong H$ então $H \cong G$ (simétrica)
    - Para três grupos quaisquer G, H e K, se $G \cong H$ e $H \cong K$, então $G \cong K$ (transitiva)

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adição é associativa
    2. Existe um elemento identidade para a adição
    3. Todo elemento de R possui um inverso para a adição
    4. A adição é comutativa
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *], se são satisfeitos
    1. A adição é associativa
    2. Existe um elemento identidade para a adição
    3. Todo elemento de R possui um inverso para a adição
    4. A adição é comutativa
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

Para cada $a, b, c \in R$, $(a+b)+c = a+(b+c)$

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adição é fechada em *R*
    2. Existe um elemento identidade para a adição
    3. Todo elemento de R possui um inverso para a adição
    4. A adição é comutativa
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

Existe um elemento $0 \in R$, chamado elemento identidade, tal que $\alpha+0 = 0+\alpha = \alpha$ para todo $\alpha \in R$

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adiç
    2. Existe
    3. Todo elemento de R possui um inverso para a adição
    4. A adição é comutativa
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

Para cada $a \in R$, existe um elemento $-a \in R$ chamado de negativo de a, tal que $a+(-a) = (-a)+a = \alpha$

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adição é associativa
    2. Existe um elemento identidade para a adição
    3. Todo (
    4. A adição é comutativa
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

Para todo $a, b \in R$, $a+b = b+a$

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adição é associativa
    2. Existe um elemento identidade para a adição
    3. Todo elemento de R possui um inverso para a adição
    4. A adiç — Para cada $a, b, c \in R$, temos $(a*b*)c = a*(b*c)$
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adição é associativa
    2. Existe um elemento identidade para a adição
    3. Todo elemento de R possui um inverso para a adição
    4. A adiç
    5. A mul
    6. A multiplicação é distributiva em relação a adição

Para cada $a, b, c \in R$, temos (i) $a*(b+c) = a*b+a*c$ e (ii) $(b+c)*a = b*a + c*a$

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:

R é um grupo comutativo sob +

1. A adição é associativa
2. Existe um elemento identidade para a adição
3. Todo elemento de R possui um inverso para a adição
4. A adição é comutativa

R é semigrupo sob *

5. A multiplicação é associativa
6. A multiplicação é distributiva em relação a adição

Estruturas Algébricas

- **Anel**
  - Seja *R* um conjunto não vazio com duas operações binárias, uma operação de adição (denotada por +) e uma operação de multiplicação (denotada por *)
  - *R* é dito um **anel**, denotado como [*R*, +, *] se são satisfeitos os seguintes axiomas:
    1. A adição é associativa
    2. Existe um elemento identidade para a adição
    3. Todo elemento de R possui um inverso para a adição
    4. A adição é comutativa
    5. A multiplicação é associativa
    6. A multiplicação é distributiva em relação a adição

R é um grupo comutativo sob +

R é semigrupo sob *

  - Exemplo: [$\mathbb{Z}$, +, $\times$] é um anel

Estruturas Algébricas

- **Corpo**
  - Anel comutativo no qual todo elemento diferente de zero possui inverso em relação à multiplicação
  - Exemplo
    - $[\mathbb{R}, +, \times]$ é um corpo