# Introdução à teoria de grupos

Gustavo Zambonin

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
INE5601 — Fundamentos Matemáticos da Informática

gustavo.zambonin@posgrad.ufsc.br

# Contexto

- Reticulados como estruturas algébricas
  - Duas operações binárias, encontro $\wedge$ e junção $\vee$
  - Reticulados limitados, complementados, distributivos

# Contexto

- Reticulados como estruturas algébricas
  - Duas operações binárias, encontro $\wedge$ e junção $\vee$
  - Reticulados limitados, complementados, distributivos
- Álgebras Booleanas
  - Reticulado complementado distributivo
  - Encontro, junção, e operação unária de complementação $^{\perp}$

# Contexto

- Reticulados como estruturas algébricas
  - Duas operações binárias, encontro $\wedge$ e junção $\vee$
  - Reticulados limitados, complementados, distributivos
- Álgebras Booleanas
  - Reticulado complementado distributivo
  - Encontro, junção, e operação unária de complementação $^{\perp}$
- Estrutura algébrica geral
  - Conjunto equipado com um número finito de operações de aridade finita

# Exemplos práticos

- Fundamental em muitas áreas da matemática
  - Teoria de números, álgebra linear, geometria, combinatória, criptografia, teoria de códigos etc.

# Exemplos práticos

- Fundamental em muitas áreas da matemática
  - Teoria de números, álgebra linear, geometria, combinatória, criptografia, teoria de códigos etc.
- Física, química, biologia, ciência dos materiais
  - Modelagem de estruturas e leis da natureza, estudo de partículas

# Exemplos práticos

- Fundamental em muitas áreas da matemática
  - Teoria de números, álgebra linear, geometria, combinatória, criptografia, teoria de códigos etc.
- Física, química, biologia, ciência dos materiais
  - Modelagem de estruturas e leis da natureza, estudo de partículas
- Ideia geral: operacionalização de elementos de um conjunto

# Teoria de grupos

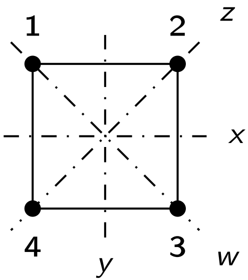
- Estudo de simetrias de um objeto
- Uma simetria é um estado de um objeto que ocupa o mesmo lugar no espaço após um movimento rígido

# Teoria de grupos

- Estudo de simetrias de um objeto
- Uma simetria é um estado de um objeto que ocupa o mesmo lugar no espaço após um movimento rígido
- Podem ser aplicadas repetidamente, desfeitas, ou simplesmente não mudar o objeto
  - Ou seja, as propriedades de composição, elemento inverso e elemento neutro são satisfeitas

# Exemplo

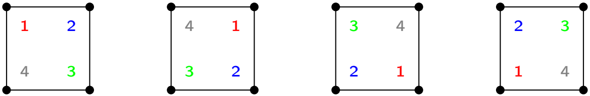
## Teoria de grupos



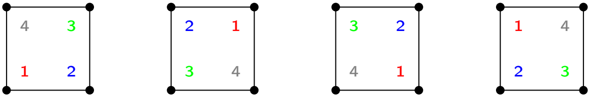

- Um quadrado sobre um plano qualquer tem oito simetrias, que levam de vértice em vértice
- Rotações no sentido horário e reflexões sobre eixos

# Exemplo

## Teoria de grupos




Rotações no sentido horário de 0°, 90°, 180° e 270°, respectivamente ($R_0, R_1, R_2, R_3$).




Reflexões com relação aos eixos $x, y, z$ e $w$, respectivamente ($X, Y, Z, W$).

# Operações binárias

- Tome $G$ como um conjunto qualquer. Uma **operação binária** sobre $G$ é uma função $* : G \times G \to G$

# Operações binárias

- Tome $G$ como um conjunto qualquer. Uma **operação binária** sobre $G$ é uma função $* : G \times G \to G$
- $*$ é definida para todo par $(a, b)$ de elementos, e associa-os unicamente
  - A aplicação $*(a, b)$ será denotada como $a * b$

# Operações binárias

- Tome $G$ como um conjunto qualquer. Uma **operação binária** sobre $G$ é uma função $* : G \times G \to G$
- $*$ é definida para todo par $(a, b)$ de elementos, e associa-os unicamente
  - A aplicação $*(a, b)$ será denotada como $a * b$
- Definição pode ser estendida para operações $n$-árias
  - Teoria de grupos trabalha geralmente com operações entre dois elementos

# Operações binárias

- Definição implica que a operação é fechada
  - Imagem da função sempre estará no conjunto base
  - Descrição mais genérica pode ignorar essa limitação

# Operações binárias

- Definição implica que a operação é fechada
  - Imagem da função sempre estará no conjunto base
  - Descrição mais genérica pode ignorar essa limitação
- Se existe um elemento neutro para qualquer operação $*$ sobre um conjunto $G$, ele é único

# Operações binárias

- Definição implica que a operação é fechada
  - Imagem da função sempre estará no conjunto base
  - Descrição mais genérica pode ignorar essa limitação
- Se existe um elemento neutro para qualquer operação $*$ sobre um conjunto $G$, ele é único
- Pode ser associativa, comutativa, distributiva

| $*$ | $R_0$ | $R_1$ | $R_2$ | $R_3$ | $X$ | $Y$ | $Z$ | $W$ |
|---|---|---|---|---|---|---|---|---|
| $R_0$ | $R_0$ | $R_1$ | $R_2$ | $R_3$ | $X$ | $Y$ | $Z$ | $W$ |
| $R_1$ | $R_1$ | $R_2$ | $R_3$ | $R_0$ | $Z$ | $W$ | $Y$ | $X$ |
| $R_2$ | $R_2$ | $R_3$ | $R_0$ | $R_1$ | $Y$ | $X$ | $W$ | $Z$ |
| $R_3$ | $R_3$ | $R_0$ | $R_1$ | $R_2$ | $W$ | $Z$ | $X$ | $Y$ |
| $X$ | $X$ | $Z$ | $Y$ | $W$ | $R_0$ | $R_2$ | $R_1$ | $R_3$ |
| $Y$ | $Y$ | $W$ | $X$ | $Z$ | $R_2$ | $R_0$ | $R_3$ | $R_1$ |
| $Z$ | $Z$ | $Y$ | $W$ | $X$ | $R_3$ | $R_1$ | $R_0$ | $R_2$ |
| $W$ | $W$ | $X$ | $Z$ | $Y$ | $R_1$ | $R_3$ | $R_2$ | $R_0$ |

Tabela de operações para as simetrias do quadrado.

# Exemplos

## Operações binárias

- Operações comutativas

- Operações não comutativas

- Operações não associativas e não comutativas

# Exemplos

## Operações binárias

- Operações comutativas
  - $+$, a adição usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

- Operações não comutativas

- Operações não associativas e não comutativas

# Exemplos

## Operações binárias

- Operações comutativas
  - $+$, a adição usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Operações não comutativas
- Operações não associativas e não comutativas

# Exemplos

## Operações binárias

- Operações comutativas
  - $+$, a adição usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Operações não comutativas
  - $-$, subtração usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Operações não associativas e não comutativas

# Exemplos

## Operações binárias

- Operações comutativas
  - $+$, a adição usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Operações não comutativas
  - $-$, subtração usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação de matrizes de mesma dimensão
- Operações não associativas e não comutativas

# Exemplos

## Operações binárias

- Operações comutativas
  - $+$, a adição usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Operações não comutativas
  - $-$, subtração usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação de matrizes de mesma dimensão
- Operações não associativas e não comutativas
  - $\div$, a divisão usual em $\mathbb{Q}, \mathbb{R}$

# Exemplos

## Operações binárias

- Operações comutativas
  - $+$, a adição usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Operações não comutativas
  - $-$, subtração usual em $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
  - $\times$, a multiplicação de matrizes de mesma dimensão
- Operações não associativas e não comutativas
  - $\div$, a divisão usual em $\mathbb{Q}, \mathbb{R}$
  - $\times$, o produto vetorial de dois elementos $\mathbb{R}^3$

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades
- Dado um conjunto $G$ e uma operação binária $*$, um **grupo** é o par ordenado $(G, *)$ onde, $\forall a, b, c \in G$

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades
- Dado um conjunto $G$ e uma operação binária $*$, um **grupo** é o par ordenado $(G, *)$ onde, $\forall a, b, c \in G$
  - $*$ é fechada, ou seja, $a * b \in G$

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades
- Dado um conjunto $G$ e uma operação binária $*$, um **grupo** é o par ordenado $(G, *)$ onde, $\forall a, b, c \in G$
  - $*$ é fechada, ou seja, $a * b \in G$
  - $*$ é associativa, ou seja, $(a * b) * c = a * (b * c)$

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades
- Dado um conjunto $G$ e uma operação binária $*$, um **grupo** é o par ordenado $(G, *)$ onde, $\forall a, b, c \in G$
  - $*$ é fechada, ou seja, $a * b \in G$
  - $*$ é associativa, ou seja, $(a * b) * c = a * (b * c)$
  - $*$ possui a identidade única $e \in G$, ou seja, $a * e = a$

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades
- Dado um conjunto $G$ e uma operação binária $*$, um **grupo** é o par ordenado $(G, *)$ onde, $\forall a, b, c \in G$
  - $*$ é fechada, ou seja, $a * b \in G$
  - $*$ é associativa, ou seja, $(a * b) * c = a * (b * c)$
  - $*$ possui a identidade única $e \in G$, ou seja, $a * e = a$
  - Existe $d \in G$ único tal que $a * d = e = d * a$, chamado de inverso de $a$ ou $a^{-1}$

# Grupos

- Conjunto de elementos munido de uma operação binária que satisfaz certas propriedades
- Dado um conjunto $G$ e uma operação binária $*$, um **grupo** é o par ordenado $(G, *)$ onde, $\forall a, b, c \in G$
  - $*$ é fechada, ou seja, $a * b \in G$
  - $*$ é associativa, ou seja, $(a * b) * c = a * (b * c)$
  - $*$ possui a identidade única $e \in G$, ou seja, $a * e = a$
  - Existe $d \in G$ único tal que $a * d = e = d * a$, chamado de inverso de $a$ ou $a^{-1}$
- Note que $G \neq \emptyset$, visto que $e \in G$

# Exemplos

## Grupos

- Com relação à adição usual, tome $e = 0$ e $a^{-1} = -a$
  - $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ são todos grupos

# Exemplos
## Grupos

- Com relação à adição usual, tome $e = 0$ e $a^{-1} = -a$
  - $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ são todos grupos
- Com relação à multiplicação usual, tome $e = 1$ e $a^{-1} = \frac{1}{a}$
  - $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ são todos grupos

# Exemplos

## Grupos

- Com relação à adição usual, tome $e = 0$ e $a^{-1} = -a$
  - $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ são todos grupos
- Com relação à multiplicação usual, tome $e = 1$ e $a^{-1} = \frac{1}{a}$
  - $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ são todos grupos
- Com relação à adição módulo $n$, tome $e = 0$ e $a + a^{-1} \equiv 0 \pmod{n}$; $\mathbb{Z}_n$ é um grupo

# Exemplos

## Grupos

- Com relação à adição usual, tome $e = 0$ e $a^{-1} = -a$
  - $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ são todos grupos
- Com relação à multiplicação usual, tome $e = 1$ e $a^{-1} = \frac{1}{a}$
  - $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ são todos grupos
- Com relação à adição módulo $n$, tome $e = 0$ e $a + a^{-1} \equiv 0 \pmod{n}$; $\mathbb{Z}_n$ é um grupo
- Com relação à multiplicação módulo $n$, tome $e = 1$ e $a \times a^{-1} \equiv 1 \pmod{n}$; $\mathbb{Z}_n^*$ é um grupo

# Grupos

- Grupos respeitam várias propriedades intuitivas

# Grupos

- Grupos respeitam várias propriedades intuitivas
  - A inversa da identidade é ela mesma, ou seja, $e^{-1} = e$

# Grupos

- Grupos respeitam várias propriedades intuitivas
  - A inversa da identidade é ela mesma, ou seja, $e^{-1} = e$
  - A inversa da inversa de um elemento é ele mesmo, ou seja, $(a^{-1})^{-1} = a$

# Grupos

- Grupos respeitam várias propriedades intuitivas
  - A inversa da identidade é ela mesma, ou seja, $e^{-1} = e$
  - A inversa da inversa de um elemento é ele mesmo, ou seja, $(a^{-1})^{-1} = a$
  - $(a * b)^{-1} = b^{-1} * a^{-1}$

# Grupos

- Grupos respeitam várias propriedades intuitivas
  - A inversa da identidade é ela mesma, ou seja, $e^{-1} = e$
  - A inversa da inversa de um elemento é ele mesmo, ou seja, $(a^{-1})^{-1} = a$
  - $(a * b)^{-1} = b^{-1} * a^{-1}$
  - Leis do cancelamento à direita e à esquerda, ou seja, $a * c = b * c \Leftrightarrow a = b$ e $c * a = c * b \Leftrightarrow a = b$

# Grupos

- Grupos respeitam várias propriedades intuitivas
  - A inversa da identidade é ela mesma, ou seja, $e^{-1} = e$
  - A inversa da inversa de um elemento é ele mesmo, ou seja, $(a^{-1})^{-1} = a$
  - $(a * b)^{-1} = b^{-1} * a^{-1}$
  - Leis do cancelamento à direita e à esquerda, ou seja, $a * c = b * c \Leftrightarrow a = b$ e $c * a = c * b \Leftrightarrow a = b$
- $x^n = x * x * \cdots * x$, $n$ vezes; $x^0 = e$

# Grupos

- A ordem de um grupo $(G, *)$, denotada $|G|$, é o número de elementos de $G$
- A ordem de um elemento $g \in G$, denotada $|g|$, é o menor $n \in \mathbb{N}^*$ tal que $g^n = e$

# Grupos

- A ordem de um grupo $(G, *)$, denotada $|G|$, é o número de elementos de $G$
- A ordem de um elemento $g \in G$, denotada $|g|$, é o menor $n \in \mathbb{N}^*$ tal que $g^n = e$
- Se a operação do grupo é comutativa, então este é chamado de grupo **abeliano**

# Grupos

- Um subconjunto $H \subseteq G$ que é fechado sob $*$ e cujas inversas estão em $H$ é chamado de **subgrupo**
  - Os inteiros pares munidos da adição usual são um subgrupo de $(\mathbb{Z}, +)$

# Grupos

- Um subconjunto $H \subseteq G$ que é fechado sob $*$ e cujas inversas estão em $H$ é chamado de **subgrupo**
  - Os inteiros pares munidos da adição usual são um subgrupo de $(\mathbb{Z}, +)$
- Uma função $\varphi$ entre dois grupos que preserva $*$ é chamada de **homomorfismo**
  - Ou seja, dados $(G_1, *), (G_2, *)$, $\varphi : G_1 \to G_2$, então $\forall g_{11}, g_{12} \in G_1,\ g_{11} * g_{12} = \varphi(g_{11}) * \varphi(g_{12})$

# Grupos

- Um subconjunto $H \subseteq G$ que é fechado sob $*$ e cujas inversas estão em $H$ é chamado de **subgrupo**
  - Os inteiros pares munidos da adição usual são um subgrupo de $(\mathbb{Z}, +)$
- Uma função $\varphi$ entre dois grupos que preserva $*$ é chamada de **homomorfismo**
  - Ou seja, dados $(G_1, *), (G_2, *)$, $\varphi : G_1 \to G_2$, então $\forall g_{11}, g_{12} \in G_1,\ g_{11} * g_{12} = \varphi(g_{11}) * \varphi(g_{12})$
  - Se esta correspondência é bijetora, a função é chamada de isomorfismo

# Grupos cíclicos

- O conjunto gerador de um grupo é um subconjunto cujos elementos, suas potências e inversas geram todos os elementos do grupo

# Grupos cíclicos

- O conjunto gerador de um grupo é um subconjunto cujos elementos, suas potências e inversas geram todos os elementos do grupo
- Um grupo abeliano que é gerado por apenas um elemento é chamado de **cíclico**

# Grupos cíclicos

- O conjunto gerador de um grupo é um subconjunto cujos elementos, suas potências e inversas geram todos os elementos do grupo
- Um grupo abeliano que é gerado por apenas um elemento é chamado de **cíclico**
- Todos os grupos de ordem prima são cíclicos

# Grupos cíclicos

- O conjunto gerador de um grupo é um subconjunto cujos elementos, suas potências e inversas geram todos os elementos do grupo
- Um grupo abeliano que é gerado por apenas um elemento é chamado de **cíclico**
- Todos os grupos de ordem prima são cíclicos
- O grupo $\mathbb{Z}_n$ é cíclico, bem como o grupo das simetrias do quadrado

# Grupos diedrais

- As simetrias do quadrado são definidas como um grupo
- Note que essas funções admitem uma forma de descrição matricial

# Grupos diedrais

- As simetrias do quadrado são definidas como um grupo
- Note que essas funções admitem uma forma de descrição matricial
  - Represente-as como $R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ldots$

# Grupos diedrais

- As simetrias do quadrado são definidas como um grupo
- Note que essas funções admitem uma forma de descrição matricial
  - Represente-as como $R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ldots$
- Então, $G = \{R_0, R_1, R_2, R_3, X, Y, Z, W\}$, munido da operação de composição de funções $\circ$, é um grupo

# Grupos diedrais

- As simetrias do quadrado são definidas como um grupo
- Note que essas funções admitem uma forma de descrição matricial
  - Represente-as como $R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ldots$
- Então, $G = \{R_0, R_1, R_2, R_3, X, Y, Z, W\}$, munido da operação de composição de funções $\circ$, é um grupo
  - Não é abeliano, pois por exemplo, $X \circ R_3 = W \neq Z = R_3 \circ X$

# Grupos diedrais

- Este conceito pode ser generalizado para qualquer polígono regular
  - Grupos dessa forma são chamados de **diedrais** ou $D_n$, onde $n$ é o número de vértices do polígono

# Grupos diedrais

- Este conceito pode ser generalizado para qualquer polígono regular
  - Grupos dessa forma são chamados de **diedrais** ou $D_n$, onde $n$ é o número de vértices do polígono
- Ordem do grupo é sempre $2n$

# Grupos diedrais

- Este conceito pode ser generalizado para qualquer polígono regular
  - Grupos dessa forma são chamados de **diedrais** ou $D_n$, onde $n$ é o número de vértices do polígono
- Ordem do grupo é sempre $2n$
- Exemplo gráfico: o grupo $D_8$

# Material de estudo

Dummit, D. S. and Foote, R. M. (2003).
*Abstract Algebra*.
3rd edition.

- Leitura das páginas 16–32 e resolução dos exercícios 1–10 de cada subseção