# INE5403

# FUNDAMENTOS DE MATEMÁTICA DISCRETA PARA A COMPUTAÇÃO

PROF. DANIEL S. FREITAS

UFSC - CTC - INE

# 7 - ESTRUTURAS ALGÉBRICAS

7.1) Operações Binárias

7.2) Semigrupos

7.3) Produtos e Quocientes de Semigrupos

7.4) Grupos

7.5) Produtos e Quocientes de Grupos

# PRODUTOS E QUOCIENTES DE GRUPOS

- Recursos que permitem obter novos grupos a partir de outros já conhecidos.

- **Nota:** Um grupo tem mais estrutura do que um semigrupo:
  - resultados mais profundos do que os análogos para semigrupos

- **Teorema 1:** Se $G_1$ e $G_2$ são grupos,então $G = G_1 \times G_2$ é um grupo com uma operação definida por:

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$$

# PRODUTOS E QUOCIENTES DE GRUPOS

- **Exemplo:** Sejam $G_1$ e $G_2$ o grupo $\mathbb{Z}_2$.
  - Nota: $\overline{0}$ e $\overline{1}$ em vez de $[0]$ e $[1]$
  - Tabela de multiplicação de $G = G_1 \times G_2$:

| | $(\overline{0},\overline{0})$ | $(\overline{1},\overline{0})$ | $(\overline{0},\overline{1})$ | $(\overline{1},\overline{1})$ |
|---|---|---|---|---|
| $(\overline{0},\overline{0})$ | $(\overline{0},\overline{0})$ | $(\overline{1},\overline{0})$ | $(\overline{0},\overline{1})$ | $(\overline{1},\overline{1})$ |
| $(\overline{1},\overline{0})$ | $(\overline{1},\overline{0})$ | $(\overline{0},\overline{0})$ | $(\overline{1},\overline{1})$ | $(\overline{0},\overline{1})$ |
| $(\overline{0},\overline{1})$ | $(\overline{0},\overline{1})$ | $(\overline{1},\overline{1})$ | $(\overline{0},\overline{0})$ | $(\overline{1},\overline{0})$ |
| $(\overline{1},\overline{1})$ | $(\overline{1},\overline{1})$ | $(\overline{0},\overline{1})$ | $(\overline{1},\overline{0})$ | $(\overline{0},\overline{0})$ |

  - $G$ é um grupo de ordem 4 $\Rightarrow$ deve ser isomórfico a $V$ ou a $\mathbb{Z}_4$
  - Vemos ($\Rightarrow$) que o isomorfismo é a $f : V \to \mathbb{Z}_2 \times \mathbb{Z}_2$ dada por:

$$f(e) = (\overline{0},\overline{0}) \qquad f(a) = (\overline{1},\overline{0}) \qquad f(b) = (\overline{0},\overline{1}) \qquad f(c) = (1,1)$$

□

# (GRUPOS DE ORDEM 4)

- Tabelas de multiplicação para grupo de ordem 4:

| | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

(1)

| | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | a | e |
| c | c | b | e | a |

(2)

| | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

(3)

| | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | c | e | b |
| b | b | e | c | a |
| c | c | b | a | e |

(4)

- Grupos das tabelas (2), (3) e (4) são isomórfi cos.
- De fato, existem exatamente 2 grupos não-isomórifi cos de ordem 4:
  - o grupo da tab. (1) é chamado de “grupo Klein 4” (denotado por $V$)
  - o grupo da tab. (2) é denotado por $\mathbb{Z}_4$
    - (re-rotulando os elementos de $\mathbb{Z}_4$ resulta nesta tabela.) □

# PRODUTOS E QUOCIENTES DE GRUPOS

- Se repetirmos o exemplo com $\mathbb{Z}_2$ e $\mathbb{Z}_3$, concluiremos que:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$$

- Pode-se mostrar que, em geral:

$$\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn} \quad \text{se e somente se} \quad \text{GCD}(m, n) = 1$$

# PRODUTOS E QUOCIENTES DE GRUPOS

- O Teorema 1 pode ser estendido para:
  - Se $G_1, G_2, \ldots, G_n$ são grupos, então

    $G = G_1 \times G_2 \times \cdots G_n$ também é um grupo.

# PRODUTOS E QUOCIENTES DE GRUPOS

- **Exemplo:** Seja $B = \{0, 1\}$ o grupo com operação (já) definida por:

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

- Então $B^n = B \times B \times \cdots \times B$ é um grupo.
- Com operação $\bigoplus$ defi nida por:

  $(x_1, x_2, \ldots, x_n) \bigoplus (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$
- A identidade de $B^n$ é $(0, 0, \ldots, 0)$.
- Cada elemento é a sua própria inversa.
- Este grupo é, essencialmente, o mesmo que a Álgebra Booleana $B_n$
  - só que a operação binária é bem diferente de $\wedge$ e $\vee$.

# PRODUTOS E QUOCIENTES DE GRUPOS

- Sob uma relação de congruência, o grupo é visto como um semigrupo.
- A seguir, veremos estruturas quocientes determinadas por uma relação de congruência sobre um grupo.

# PRODUTOS E QUOCIENTES DE GRUPOS

- **Teorema 2:**
  - Seja $R$ uma relação de congruência sobre o grupo $(G, *)$.
  - Então o semigrupo $(G/R, \circledast)$ é um grupo.
    - A operação $\circledast$ é definida sobre $G/R$ como:

$$[a] \circledast [b] = [a \circledast b]$$

- **Prova:**
  - $G$ é um grupo $\Rightarrow$ $G$ é um monóide $\Rightarrow$ $G/R$ é um monóide
  - Só falta provar que cada elemento de $G/R$ tem uma inversa:
    - como $[a] \in G/R$, então $[a^{-1}] \in G/R$ *(pois $a^{-1} \in G$)*
    - daí: $[a] \circledast [a^{-1}] = [a \circledast a^{-1}] = [e]$
    - de modo que: $[a]^{-1} = [a^{-1}]$
    - portanto: $(G/R, \circledast)$ é um grupo $\square$

# HOMOMORFISMOS E ISOMORFISMOS

- **Nota:** As definições de homomorfismo, isomorfismo e congruência para grupos envolvem apenas as suas estruturas de semigrupos e monóides.

- A seguir, uma conseqüência imediata dos resultados para semigrupos...

# PRODUTOS E QUOCIENTES DE GRUPOS

- **Corolário 1(a):**
  - Se $R$ é uma relação de congruência sobre $G$, então:
    - a função $f_R : G \to G/R$, dada por: $f_R(a) = [a]$

      é um homomorfismo de grupo.

- **Corolário 1(b):**
  - Se $f : G \to G'$ é um homomorfismo e:
    - se $R$ é definida por: "$a\ R\ b$ sse $f(a) = f(b)$"
  - então:
    - $R$ é uma relação de congruência
    - a função $\overline{f} : G/R \to G'$, dada por: $\overline{f}([a]) = f(a)$

      é um isomorfismo do grupo $(G/R, \circledast)$ sobre o grupo $(G', *')$.

# SUBGRUPOS E COSETS

- Têm uma forma muito especial...
- Seja $H$ um subgrupo de um grupo $G$ e seja $a \in G$:
  - o **coset à esquerda** de $H$ em $G$ determinado por $a$ é o conjunto:

    $$aH = \{ah \mid h \in H\}$$

  - o **coset à direita** de $H$ em $G$, determinado por $a$, é o conjunto:

    $$Ha = \{ha \mid h \in H\}$$

  - dizemos que um subgrupo $H$ de $G$ é **normal** se:

    $$aH = Ha, \qquad \forall a \in G$$

- **Nota:** "$Ha = aH$" não é o mesmo que "$ha = ah$"
  - só se sabe que $ha = ah'$ aonde $h'$ é algum elemento em $H$

# SUBGRUPOS E COSETS

- Computando todos os cosets à esquerda de um subgrupo $H$ em $G$:
  - Suponha que $a \in H$:
    - então $aH \subseteq H$, pois $H$ é subgrupo (de $G$)
    - além disto:
      - se $h \in H$, então $h = ah'$, aonde: $h' = a^{-1}h \in H$
      - de modo que: $H \subseteq aH$.
    - logo: se $a \in H$, então $aH = H$.
  - Conclusão: quando computando todos os cosets de $H$, não é preciso computar $aH$ para $a \in H$
    - (pois será sempre $H$)

# SUBGRUPOS E COSETS

- **Exemplo 1(/3):** Seja $G$ o grupo de simetrias $S_3$ já visto (=>).
  - O subconjunto $H = \{f_1, g_2\}$ é um subgrupo de $G$.
  - Computando todos os cosets à esquerda de $H$ em $G$:
    - se $a \in H$ então: $aH = H$
    - portanto: $f_1 H = g_2 H = H$
    - além disto:

$$f_2 H = \{f_2, g_1\}$$
$$f_3 H = \{f_3, g_3\}$$
$$g_1 H = \{g_1, f_2\} = f_2 H$$
$$g_3 H = \{g_3, f_3\} = f_3 H$$

  - Portanto, todos os cosets à esquerda de $H$ em $G$ que são distintos são:

$$H, \ f_2 H \ \text{ e } \ f_3 H \qquad \square$$

# (EXEMPLOS DE GRUPOS)

- **Exemplo (relembrando):**

$$S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$$
$$= \{\{1,2,3\},\{2,3,1\},\{3,1,2\},\{1,3,2\},\{3,2,1\},\{2,1,3\}\}$$

- A operação de composição sobre $S_3$ produz a seguinte tabela de multiplicação:

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $g_1$ | $g_2$ | $g_3$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $g_1$ | $g_2$ | $g_3$ |
| $f_2$ | $f_2$ | $f_3$ | $f_1$ | $g_3$ | $g_1$ | $g_2$ |
| $f_3$ | $f_3$ | $f_1$ | $f_2$ | $g_2$ | $g_3$ | $g_1$ |
| $g_1$ | $g_1$ | $g_2$ | $g_3$ | $f_1$ | $f_2$ | $f_3$ |
| $g_2$ | $g_2$ | $g_3$ | $g_1$ | $f_3$ | $f_1$ | $f_2$ |
| $g_3$ | $g_3$ | $g_1$ | $g_2$ | $f_2$ | $f_3$ | $f_1$ |

# SUBGRUPOS E COSETS

- **Exemplo 2(/3):** Sejam $H$ e $G$ como no exemplo anterior:

  $$H = \{f_1, g_2\}$$

  $$G = S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}$$

  $$= \{\{1,2,3\}, \{2,3,1\}, \{3,1,2\}, \{1,3,2\}, \{3,2,1\}, \{2,1,3\}\}$$

  - Considere o seguinte coset à direita:

    $$Hf_2 = \{f_2, g_3\}$$

  - Mas vimos que: $f_2H = \{f_2, g_1\}$.
  - Logo: $H$ não é um subgrupo normal de $G$. □

# SUBGRUPOS E COSETS

- **Exemplo 3(/3):** Mostre que se $G$ é um grupo abeliano, todo subgrupo de $G$ é um subgrupo normal.
  - Sejam:
    - $H$ um subgrupo de $G$
    - $a \in G$
    - $h \in H$
  - Então, como $G$ é abeliano: $ha = ah$
    - de modo que: $Ha = aH$
    - o que implica que $H$ é um subgrupo normal de $G$. □

# SUBGRUPOS NORMAIS E COSETS

- **Teorema 3:**
  - Sejam:
    - $R$ uma relação de congruência sobre um grupo $G$
    - $H = [e]$ (a classe de equivalência que contém $e$),
  - Então:
    - $H$ é um subgrupo normal de $G$
    - para cada $a \in G$, vale:

$$[a] = aH = Ha$$

- **Prova: ($\Rightarrow$)**

# SUBGRUPOS NORMAIS E COSETS

- **Prova:** Sejam $a$ e $b$ elementos quaisquer em $G$.
  - Uma vez que $R$ é uma relação de equivalência:

    $b \in [a]$ se e somente se $[b] = [a]$

  - Também (pelo Teorema 2) $G/R$ é um grupo.

    $\Rightarrow$ $[b] = [a]$ se e somente se $[e] = [a]^{-1}[b] = [a^{-1}b]$

    $\Rightarrow$ $b \in [a]$ se e somente se $H = [e] = [a^{-1}b]$

    $\Rightarrow$ $b \in [a]$ se e somente se $a^{-1}b \in H$ ou: $b \in aH$

    $\Rightarrow$ $[a] = aH$, $\forall a \in G$

  - Pode-se mostrar, da mesma forma, que:

    $b \in [a]$ se e somente se $H = [e] = [b][a]^{-1} = [ba^{-1}]$

    - o que equivale a afirmar que $[a] = Ha$

  - Portanto: $[a] = aH = Ha$ e $H$ é normal. $\square$

# SUBGRUPOS NORMAIS E COSETS

- Combinando o Teorema 3:
  - "Se $R$ é uma relação de congruência sobre um grupo $G$, então: $[a] = a[e]$."
- com o Corolário 1(a):
  - "Se $R$ é uma relação de congruência sobre $G$, então:
    - $f_R : G \to G/R$, dada por $f_R(a) = [a]$, é um homomorfi smo de grupo."
- notamos que, neste caso:
  - $G/R$ consiste dos cosets à esquerda de $N = [e]$
    - (ou seja: ao juntarmos todos os cosets à esquerda de $[e]$, obteremos $G/R$)
  - e a operação em $G/R$ é dada (simplesmente) por:

$$(aN)(bN) = [a] \circledast [b] = [ab] = abN$$

- Frequentemente, escrevemos $G/R$ como $G/N$.

# SUBGRUPOS NORMAIS E COSETS

- **Teorema 4**:
  - Sejam:
    - $N$ um subgrupo normal de um grupo $G$
    - $R$ a seguinte relação sobre $G$:

      $$a \; R \; b \quad \text{se e somente se} \quad a^{-1}b \in N$$

  - Então:

    (a) $R$ é uma relação de congruência sobre $G$

    (b) $N$ é a classe de equivalência $[e]$ relativa a $R$

    - ("$e$" é a identidade de $G$)

- **Prova: ($\Rightarrow$)**

# SUBGRUPOS NORMAIS E COSETS

- **Prova de (a) (1/2)**: (" a relação $a\,R\,b \Leftrightarrow a^{-1}b \in N$ é de congruência")
  - $R$ é uma relação de equivalência sobre $G$:
    - $R$ é reflexiva: $a\,R\,a$, pois: $a^{-1}a = e \in N$
    - $R$ é simétrica: seja $a\,R\,b$:
      - então: $a^{-1}b \in N$
      - mas: $(a^{-1}b)^{-1} = b^{-1}a \in N$ (pois $N$ é subgrupo)
      - de modo que: $b\,R\,a$
    - $R$ é transitiva: sejam $a\,R\,b$ e $b\,R\,c$:
      - então: $a^{-1}b \in N$ e $b^{-1}c \in N$
        $\Rightarrow \quad (a^{-1}b)(b^{-1}c) = a^{-1}c \in N$
      - de modo que: $a\,R\,c$
- Continuação da prova de (a) $\Rightarrow$

# SUBGRUPOS NORMAIS E COSETS

- **Prova de (a) (2/2)**: (" a relação $a\,R\,b \Leftrightarrow a^{-1}b \in N$ é de congruência")
  - $R$ é uma relação de congruência sobre $G$:
    - suponha que $a\,R\,b$ e $c\,R\,d$:
      - então: $a^{-1}b \in N$ e $c^{-1}d \in N$
      - $N$ é normal: $Nd = dN$ "$(\forall n_1 \in N,\ \exists n_2 \in N \mid n_1 d = d n_2)$"
      - em particular, como $a^{-1}b \in N$, temos:

        $$a^{-1}bd = dn_2, \quad \text{para algum } n_2 \in N$$

      - o que permite escrever:

        $$(ac)^{-1}bd = (c^{-1}a^{-1})(bd) = c^{-1}(a^{-1}b)d = (c^{-1}d)n_2 \in N$$

      - de modo que: $ac\,R\,bd$.
- Prova de (b) $\Rightarrow$

# SUBGRUPOS NORMAIS E COSETS

- **Prova de (b)**: (" se: $a\ R\ b \Leftrightarrow a^{-1}b \in N$, então: $N = [e]$ ")
  - Seja $x \in N$:
    - então $x^{-1}e = x^{-1} \in N$ (pois $N$ é subgrupo)
    - de modo que: $x\ R\ e$ e, portanto: $x \in [e]$
    - logo: $N \subseteq [e]$
  - Conversamente:
    - se $x \in [e]$, então $x\ R\ e$
    - de modo que: $x^{-1}e = x^{-1} \in N$
    - então: $x \in N$ e $[e] \subseteq N$
  - Logo: $N = [e]$ $\square$

# SUBGRUPOS NORMAIS E COSETS

- (Por Teoremas 3+4) Se $G$ é um grupo qualquer:
  - as classes de equivalência relativas a uma relação de congruência sobre $G$ são sempre cosets de algum subgrupo normal de $G$.

- Conversamente:
  - os cosets de todo subgrupo normal de $G$ são apenas classes de equivalência relativas a alguma relação de congruência sobre $G$.

# SUBGRUPOS NORMAIS E COSETS

- O **Corolário 1(b)** pode agora ser escrito como:
  - Sejam:
    - $f$ um homomorfismo de um grupo $(G, *)$ sobre um $(G', *')$.
    - o **kernel** de $f$ dado por: $\ker(f) = \{a \in G \mid f(a) = e'\}$
  - Então:

    (a) $\ker(f)$ é um subgrupo normal de $G$

    (b) o grupo quociente $G/\ker(f)$ é isomórfico a $G'$.

- **Prova:** segue de Corolário 1 + Teorema 3, pois:
  - se $R$ é a relação de congruência sobre $G$ dada por:

    $$a \; R \; b \quad \text{se e somente se} \quad f(a) = f(b)$$

  - pode-se mostrar que: $\ker(f) = [e]$.

# SUBGRUPOS NORMAIS E COSETS

- **Exemplo:** Seja o homomorfismo $f$ de $\mathbb{Z}$ sobre $\mathbb{Z}_n$: $f(m) = [r]$
  - aonde $r$ é o resto quando $m$ é dividido por $n$
  - Neste caso:
    - o inteiro $m$ em $\mathbb{Z}$ pertence a $\ker(f)$ sse $f(m) = [0]$
    - ou seja, sse $m$ é um múltiplo de $n$
    - portanto: $\ker(f) = n\mathbb{Z}$ $\square$

# PRODUTOS E QUOCIENTES DE GRUPOS

- Final deste item.
- **Dica**: fazer exercícios sobre Produtos e Quocientes de Grupos...