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 Semigrupos

- Modos de obter novos semigrupos a partir de outros existentes.

- **Teorema:** Se $(S, *)$ e $(T, *')$ são semigrupos, então:
  - $(S \times T , *'')$ é um semigrupo
  - com $*''$ dado por: $(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2 , t_1 *' t_2)$

- **Prova:** ??

PRODUTOS E QUOCIENTES DE SEMIGRUPOS

- Modos de obter novos semigrupos a partir de outros existentes.

- **Teorema:** Se $(S, *)$ e $(T, *')$ são semigrupos, então:
  - $(\ S \times T\ ,\ *''\ )$ é um semigrupo
  - com $*''$ dado por: $(s_1, t_1)\ *''\ (s_2, t_2)\ =\ (s_1 * s_2\ ,\ t_1 *' t_2)$

- **Prova:** ??

- **Corolário:** se S e T são monóides com identidades e_S e e_T:
  - $S \times T$ é um monóide com identidade (e_S, e_T)

Relações de Equivalência sobre Semigrupos

- Como um semigrupo não é simplesmente um conjunto:
  - certas relações de equivalência sobre um semigrupo ajudam a conhecer a sua estrutura.

Relações de Equivalência sobre Semigrupos

- Como um semigrupo não é simplesmente um conjunto:
  - certas relações de equivalência sobre um semigrupo ajudam a conhecer a sua estrutura.

- Uma relação de equivalência R sobre um semigrupo $(S, *)$ é chamada de **Relação de congruência** se:

$$a \, R \, a' \quad \text{e} \quad b \, R \, b' \qquad \Longrightarrow \qquad (a * b) \, R \, (a' * b')$$

Relações de Equivalência sobre Semigrupos

- **Exemplo 1/3 (1/2):** Seja o semigrupo $(\mathbb{Z}, +)$,
  - e seja a relação de equivalência $\boldsymbol{R}$ sobre $\mathbb{Z}$:
    - $\boldsymbol{a\,R\,b}$ se e somente se $\mathbf{2}$ divide $\boldsymbol{a - b}$

      ou: $\boldsymbol{a \equiv b\ (mod\ 2)}$

RELAÇÕES DE EQUIVALÊNCIA SOBRE SEMIGRUPOS

- **Exemplo 1/3 (1/2):** Seja o semigrupo $(\mathbb{Z}, +)$,
  - e seja a relação de equivalência R sobre $\mathbb{Z}$:
    - $a\,R\,b$ se e somente se 2 divide $a - b$

    ou: $a \equiv b\ (mod\ 2)$
  - sejam: $a \equiv b\ (mod\ 2)$ e $c \equiv d\ (mod\ 2)$
  - então 2 divide tanto $a - b$ como $c - d$, de modo que:

    $a - b = 2m$ e $c - d = 2n$

Relações de Equivalência sobre Semigrupos

- **Exemplo 1/3 (1/2):** Seja o semigrupo $(\mathbb{Z}, +)$,
  - e seja a relação de equivalência R sobre $\mathbb{Z}$:
    - $a \, R \, b$ se e somente se 2 divide $a - b$

    ou: $a \equiv b \ (mod \ 2)$
  - sejam: $a \equiv b \ (mod \ 2)$ e $c \equiv d \ (mod \ 2)$
  - então 2 divide tanto $a - b$ como $c - d$, de modo que:

    $$a - b = 2m \quad \text{e} \quad c - d = 2n$$

    $$\Rightarrow (a - b) + (c - d) = 2m + 2n$$

    $$\Rightarrow (a + c) - (b + d) = 2(m + n)$$

    $$\Rightarrow a + c \equiv b + d \ (mod \ 2)$$
  - logo: R é uma relação de congruência. $\square$

Relações de Equivalência sobre Semigrupos

- **Exemplo 2/3 (1/2):** Seja $A = \{0, 1\}$,
  - considere o semigrupo livre $(A^*\ ,\ \cdot\ )$ gerado por A
  - e seja a seguinte relação sobre A^*:
    - $\alpha\ R\ \beta$ sse α e β possuem o mesmo nro de 1s

RELAÇÕES DE EQUIVALÊNCIA SOBRE SEMIGRUPOS

- **Exemplo 2/3 (1/2):** Seja $A = \{0, 1\}$,
  - considere o semigrupo livre $(A^*\ ,\ \cdot\ )$ gerado por A
  - e seja a seguinte relação sobre A^*:
    - $\alpha\ R\ \beta$ sse α e β possuem o mesmo nro de 1s
  - R é uma relação de equivalência:

1. $\alpha\ R\ \alpha,\ \ \forall\alpha \in A^*$
2. se $\alpha\ R\ \beta$, α e β têm o mesmo nro de 1s, logo: $\beta\ R\ \alpha$
3. se $\alpha\ R\ \beta$ e $\beta\ R\ \gamma$, tanto α e β como β e γ têm mesmo nro de 1s, logo: α e γ têm mesmo nro de 1s e $\alpha R \gamma$

Relações de Equivalência sobre Semigrupos

- **Exemplo 2/3 (1/2):** Seja $A = \{0, 1\}$,
  - considere o semigrupo livre $(A^*\ ,\ \cdot\ )$ gerado por A
  - e a relação: $\alpha\, R\, \beta$ sse α e β possuem o mesmo nro de 1s

Relações de Equivalência sobre Semigrupos

- **Exemplo 2/3 (1/2):** Seja $A = \{0, 1\}$,
  - considere o semigrupo livre $(A^*\ ,\ \cdot\ )$ gerado por A
  - e a relação: $\alpha\, R\, \beta$ sse α e β possuem o mesmo nro de 1s
  - R também é uma relação de congruência:
    - suponha que temos: $\alpha\, R\, \alpha'$ e $\beta\, R\, \beta'$
    - então α e α' E β e β' possuem mesmo nro de 1s
    - "nro de 1s em $\alpha \cdot \beta$" = "nro de 1s em α" + "nro de 1s em β"

      $\Rightarrow$ "nro de 1s em $\alpha \cdot \beta$" = "número de 1s em $\alpha' \cdot \beta'$ "
    - logo: $(\alpha \cdot \beta)\ R\ (\alpha' \cdot \beta')$ $\square$

Relações de Equivalência sobre Semigrupos

- **Exemplo 3/3 (1/2):** Seja o semigrupo $(\mathbb{Z}, +)$,
  - seja: $f(x) = x^2 - x - 2$
  - e seja a relação sobre $\mathbb{Z}$:
    - $a\,R\,b$ se e somente se $f(a) = f(b)$
  - fácil notar que R é uma relação de equivalência sobre $\mathbb{Z}$

Relações de Equivalência sobre Semigrupos

- **Exemplo 3/3 (1/2):** Seja o semigrupo $(\mathbb{Z}, +)$,
  - seja: $f(x) = x^2 - x - 2$
  - e seja a relação sobre $\mathbb{Z}$:
    - $a \; R \; b$ se e somente se $f(a) = f(b)$
  - fácil notar que R é uma relação de equivalência sobre $\mathbb{Z}$
  - no entanto, R não é uma relação de congruência sobre $\mathbb{Z}$, pois:
    - $-1 \; R \; 2 \quad (\, f(-1) = f(2) = 0 \,)$
    - $-2 \; R \; 3 \quad (\, f(-2) = f(3) = 4 \,)$
    - mas: $-3 \; \not{R} \; 5$
      - pois: $f(-3) = 10$ e $f(5) = 18$ $\square$

SEMIGRUPOS QUOCIENTES

- **Relembrando**:
  - a relação de equivalência R sobre o semigrupo $(S, *)$ determina uma partição de S
  - $[a] = R(a)$ é a classe de equivalência que contém a
  - S/R denota o conjunto de todas as classes de equivalência

SEMIGRUPOS QUOCIENTES

- **Teorema:**
  - Seja R uma relação de congruência sobre o semigrupo $(S, *)$.
  - E seja a relação $\circledast$, de $S/R \times S/R$ para S/R, dada por:

    $([a]\ ,\ [b])$ está relacionado com $[a * b]$ $\quad (a, b \in S)$
  - Então:

SEMIGRUPOS QUOCIENTES

- **Teorema:**
  - Seja R uma relação de congruência sobre o semigrupo $(S, *)$.
  - E seja a relação $\circledast$, de $S/R \times S/R$ para S/R, dada por:

    $([a]\ ,\ [b])$ está relacionado com $[a * b]$ $\quad (a, b \in S)$
  - Então:
    - $\circledast$ é uma função de $S/R \times S/R$ para S/R
      - usual: "$\circledast([a], [b])$" denotado por "$[a] \circledast [b]$"
      - ou seja: $[a] \circledast [b] = [a * b]$

SEMIGRUPOS QUOCIENTES

- **Teorema:**
  - Seja R uma relação de congruência sobre o semigrupo $(S, *)$.
  - E seja a relação $\circledast$, de $S/R \times S/R$ para S/R, dada por:

    $([a]\ ,\ [b])$ está relacionado com $[a * b]$ $\quad (a, b \in S)$
  - Então:
    - $\circledast$ é uma função de $S/R \times S/R$ para S/R
      - · usual: "$\circledast([a], [b])$" denotado por "$[a] \circledast [b]$"
      - · ou seja: $[a] \circledast [b] = [a * b]$
    - $(S/R\ ,\ \circledast)$ é um semigrupo.
- **Prova:** $\Rightarrow$

SEMIGRUPOS QUOCIENTES

- **Prova (1/2):**
  - suponha que $([a],[b]) = ([a'],[b'])$
  - então $a\ R\ a'$ e $b\ R\ b'$, de modo que:

    $a * b\ R\ a' * b'$ (pois R é relação de congruência)
  - portanto $[a * b] = [a' * b']$
    - ou seja, $\circledast$ é uma função
    - ou seja, $\circledast$ é uma operação binária sobre S/R

Semigrupos Quocientes

- **Prova (2/2):**
  - além disto, $\circledast$ é associativa:

$$
\begin{aligned}
[a] \circledast ([b] \circledast [c]) &= [a] \circledast [b * c] \\
&= [a * (b * c)] \\
&= [(a * b) * c)] \qquad \text{(associatividade de } * \text{ em } S\text{)}
\end{aligned}
$$

- **Prova (2/2):**
  - além disto, $\circledast$ é associativa:

$$
\begin{aligned}
[a] \circledast ([b] \circledast [c]) &= [a] \circledast [b * c] \\
&= [a * (b * c)] \\
&= [(a * b) * c)] \qquad \text{(associatividade de } * \text{ em } S) \\
&= [a * b] \circledast [c] \\
&= ([a] \circledast [b]) \circledast [c]
\end{aligned}
$$

  - portanto, S/R é um semigrupo $\square$

SEMIGRUPOS QUOCIENTES

- S/R: **Semigrupo Quociente** ou **Semigrupo Fator**.
- Note que $\circledast$ é uma espécie de "relação binária quociente" sobre S/R
  - construída a partir da relação binária original $*$ sobre S
  - pela relação de congruência R

SEMIGRUPOS QUOCIENTES

- S/R: **Semigrupo Quociente** ou **Semigrupo Fator**.
- Note que $\circledast$ é uma espécie de "relação binária quociente" sobre S/R
  - construída a partir da relação binária original $*$ sobre S
  - pela relação de congruência R
- **Corolário:**
  - Seja R uma relação de congruência sobre o monóide $(S, *)$.
  - Defina a operação $\circledast$ em S/R por $[a] * [b] = [a * b]$.
  - Então $(S/R, \circledast)$ é um monóide.
- **Prova:** Se e é a identidade em $(S, *)$:
  - $[e]$ é a identidade em $(S/R, \circledast)$. $\square$

- **Exemplo:**
  - Considere o exemplo já visto:
    - monóide $(A^*, \cdot)$ gerado por $A = \{0, 1\}$
    - R sobre A^*: $\alpha \; R \; \beta$ sse α e β com mesmo # 1s

SEMIGRUPOS QUOCIENTES

- **Exemplo:**
  - Considere o exemplo já visto:
    - monóide $(A^*, \cdot)$ gerado por $A = \{0, 1\}$
    - R sobre A^*: $\alpha \; R \; \beta$ sse α e β com mesmo # 1s
  - Como R é de congruência sobre $S = (A^*, \cdot)$:
    - concluímos que $(S/R, \odot)$ é um monóide, aonde:

$$[\alpha] \odot [\beta] = [\alpha \cdot \beta] \qquad \square$$

SEMIGRUPOS QUOCIENTES

- **Exemplo(1/2):**
  - Relação s/ o semigrupo $(\mathbb{Z}, +)$: $a\,R\,b$ sse $n \mid (a-b)$

- **Exemplo(1/2):**
  - Relação s/ o semigrupo $(\mathbb{Z}, +)$: $a\ R\ b$ sse $n \mid (a - b)$
  - R é de equivalência e é escrita como "$\equiv (mod\ n)$":

    $2 \equiv 6\ (mod\ 4)$, pois: $4 \mid (2 - 6)$

Semigrupos Quocientes

- **Exemplo(1/2):**
  - Relação s/ o semigrupo $(\mathbb{Z}, +)$: $\boldsymbol{a\ R\ b}$ sse $\boldsymbol{n \mid (a - b)}$
  - $\boldsymbol{R}$ é de equivalência e é escrita como "$\equiv (mod\ n)$":

    $\mathbf{2} \equiv \mathbf{6}\ (mod\ 4)$, pois: $\mathbf{4} \mid (\mathbf{2} - \mathbf{6})$
  - Classes de equiv. determinadas por "$\equiv (mod\ 4)$" sobre $\mathbb{Z}$:

$$[0] = \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\} = [4] = [8] = \cdots$$

$$[1] = \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\} = [5] = [9] = \cdots$$

$$[2] = \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\} = [6] = [10] = \cdots$$

$$[3] = \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\} = [7] = [11] = \cdots$$

SEMIGRUPOS QUOCIENTES

- **Exemplo(1/2):**
  - Relação s/ o semigrupo $(\mathbb{Z}, +)$: $\boldsymbol{a \; R \; b}$ sse $\boldsymbol{n \mid (a-b)}$
  - $\boldsymbol{R}$ é de equivalência e é escrita como "$\equiv (\boldsymbol{mod}\ \boldsymbol{n})$":

    $\mathbf{2 \equiv 6}\ (\boldsymbol{mod}\ \mathbf{4})$, pois: $\mathbf{4 \mid (2-6)}$
  - Classes de equiv. determinadas por "$\equiv (\boldsymbol{mod}\ \mathbf{4})$" sobre $\mathbb{Z}$:

$$[\mathbf{0}] = \{\ldots, \mathbf{-8, -4, 0, 4, 8, 12}, \ldots\} = [\mathbf{4}] = [\mathbf{8}] = \cdots$$
$$[\mathbf{1}] = \{\ldots, \mathbf{-7, -3, 1, 5, 9, 13}, \ldots\} = [\mathbf{5}] = [\mathbf{9}] = \cdots$$
$$[\mathbf{2}] = \{\ldots, \mathbf{-6, -2, 2, 6, 10, 14}, \ldots\} = [\mathbf{6}] = [\mathbf{10}] = \cdots$$
$$[\mathbf{3}] = \{\ldots, \mathbf{-5, -1, 3, 7, 11, 15}, \ldots\} = [\mathbf{7}] = [\mathbf{11}] = \cdots$$

  - Estas são todas as classes do "conj. quociente" $\mathbb{Z}/\equiv (\boldsymbol{mod}\ \mathbf{4})$.
    - $\mathbb{Z}/\equiv (\boldsymbol{mod}\ \boldsymbol{n})$ é denotado por $\mathbb{Z}_{\boldsymbol{n}}$
    - $\mathbb{Z}_{\boldsymbol{n}}$ é um monóide com operação $\bigoplus$ e identidade $[\mathbf{0}]$

SEMIGRUPOS QUOCIENTES

- **Exemplo(2/2):**
  - Tabela de adição para o semigrupo $\mathbb{Z}_4$ com operação $\bigoplus$:

$\bigoplus$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

- **Exemplo(2/2):**
  - Tabela de adição para o semigrupo $\mathbb{Z}_4$ com operação $\bigoplus$:

$\bigoplus$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

  - Elementos da tabela obtidos de: $[a] \bigoplus [b] = [a+b]$
    - exemplo: $[2] \bigoplus [3] = [2+3] = [5] = [1]$

Semigrupos Quocientes

- **Exemplo(2/2):**
  - Tabela de adição para o semigrupo $\mathbb{Z}_4$ com operação $\bigoplus$:

$\bigoplus$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

  - Elementos da tabela obtidos de: $[a] \bigoplus [b] = [a + b]$
    - exemplo: $[2] \bigoplus [3] = [2 + 3] = [5] = [1]$
  - Em geral:
    - $\mathbb{Z}_n$ tem n classes de equivalência: $[0], [1], [2], \ldots, [n - 1]$

SEMIGRUPOS QUOCIENTES & HOMOMORFISMOS

- Há uma conexão entre as estruturas do semigrupo $(S, *)$ e do semigrupo quociente $(S/R, \circledast)$.

Semigrupos Quocientes & Homomorfismos

- Há uma conexão entre as estruturas do semigrupo $(S, *)$ e do semigrupo quociente $(S/R, \circledast)$.

- **Teorema:**
  - Sejam:
    - R uma relação de congruência sobre um semigrupo $(S, *)$
    - $(S/R, \circledast)$ o semigrupo quociente correspondente

SEMIGRUPOS QUOCIENTES & HOMOMORFISMOS

- Há uma conexão entre as estruturas do semigrupo $(S, *)$ e do semigrupo quociente $(S/R, \circledast)$.

- **Teorema:**
  - Sejam:
    - R uma relação de congruência sobre um semigrupo $(S, *)$
    - $(S/R, \circledast)$ o semigrupo quociente correspondente
  - Então:
    - $f_R : S \longrightarrow S/R$, definida por $f_R(a) = [a]$, é um homomorfismo sobrejetivo
    - chamado de **homomorfismo natural**

- **Prova:** $\Rightarrow$

- **Prova:**
  - f_R é uma função sobrejetiva:
    - se $[a] \in S/R$, então $f_R(a) = [a]$

- **Prova:**
  - f_R é uma função sobrejetiva:
    - se $[a] \in S/R$, então $f_R(a) = [a]$
  - f_R é um homomorfismo:
    - se a e b são elementos de S, então:

$$\begin{aligned} f_R(a * b) &= [a * b] \\ &= [a] \circledast [b] \\ &= f_R(a) \circledast f_R(b) \qquad \square \end{aligned}$$

- **Teorema (Fundamental do Homomorfismo):**
  - Sejam:
    - $f : S \rightarrow T$ um homomorfismo do semigrupo $(S, *)$ sobre o semigrupo $(T, *')$
    - R a relação sobre S definida por $a\,R\,b$ sse $f(a) = f(b)$
      - *(R definida com base no homomorfismo)*

- **Teorema (Fundamental do Homomorfismo):**
  - Sejam:
    - $f : S \rightarrow T$ um homomorfismo do semigrupo $(S, *)$ sobre o semigrupo $(T, *')$
    - R a relação sobre S definida por $a \, R \, b$ sse $f(a) = f(b)$
      - *(R definida com base no homomorfismo)*
  - Então:

    (a) R é uma relação de congruência

    (b) $(T, *')$ e o semigrupo quociente $(S/R, \circledast)$ são isomórficos

- **Prova:** $\Rightarrow$

- **Prova da parte (a):**

  (i) $\boldsymbol{R}$ é uma relação de equivalência:

  - $\boldsymbol{a \, R \, a}$, $\forall \boldsymbol{a} \in \boldsymbol{S}$, pois $\boldsymbol{f(a) = f(a)}$
  - se $\boldsymbol{a \, R \, b}$, então $\boldsymbol{f(a) = f(b)}$, de modo que $\boldsymbol{b \, R \, a}$
  - se $\boldsymbol{a \, R \, b}$ e $\boldsymbol{b \, R \, c}$:
    - então: $\boldsymbol{f(a) = f(b)}$ e $\boldsymbol{f(b) = f(c)}$
    - de modo que: $\boldsymbol{f(a) = f(c)}$ e, portanto: $\boldsymbol{a \, R \, c}$

- **Prova da parte (a):**

  (i) R é uma relação de equivalência:

  - $a \, R \, a, \; \forall a \in S$, pois $f(a) = f(a)$
  - se $a \, R \, b$, então $f(a) = f(b)$, de modo que $b \, R \, a$
  - se $a \, R \, b$ e $b \, R \, c$:
    - então: $f(a) = f(b)$ e $f(b) = f(c)$
    - de modo que: $f(a) = f(c)$ e, portanto: $a \, R \, c$

  (ii) R é uma relação de congruência:

  - suponha que $a \, R \, a_1$ e $b \, R \, b_1$
  - então: $f(a) = f(a_1)$ e $f(b) = f(b_1)$

    $\Rightarrow f(a) *' f(b) = f(a_1) *' f(b_1)$

    $\Rightarrow f(a * b) = f(a_1 * b_1)$ *(pois f é um homomorfismo)*
  - logo: $(a * b) \, R \, (a_1 * b_1)$ $\square$

- **Prova da parte (b):** Seja a relação de S/R para T:

$$\overline{f} = \{\ ([a], f(a))\ \mid\ [a] \in S/R\}$$

- **Prova da parte (b):** Seja a relação de S/R para T:

$$\overline{f} = \{ ([a], f(a)) \mid [a] \in S/R \}$$

  - $\overline{f}$ é uma função: suponha que $[a] = [a']$:
    - então: $a\, R\, a'$ e $f(a) = f(a')$
    - logo, $\overline{f}$ é a função $\overline{f} : S/R \longrightarrow T$, aonde: $\overline{f}([a]) = f(a)$

- **Prova da parte (b):** Seja a relação de S/R para T:

$$\overline{f} = \{ ([a], f(a)) \mid [a] \in S/R\}$$

  - $\overline{f}$ é uma função: suponha que $[a] = [a']$:
    - então: $a\,R\,a'$ e $f(a) = f(a')$
    - logo, $\overline{f}$ é a função $\overline{f} : S/R \longrightarrow T$, aonde: $\overline{f}([a]) = f(a)$
  - $\overline{f}$ é injetiva: suponha que $\overline{f}([a]) = \overline{f}([a'])$:
    - então: $f(a) = f(a')$

$$\Rightarrow \; a\,R\,a' \; \Rightarrow \; [a] = [a']$$

Semigrupos Quocientes & Homomorfismos

- **Prova da parte (b):** Seja a relação de S/R para T:

$$\overline{f} = \{ ([a], f(a)) \mid [a] \in S/R\}$$

  - $\overline{f}$ é uma função: suponha que $[a] = [a']$:
    - então: $a\, R\, a'$ e $f(a) = f(a')$
    - logo, $\overline{f}$ é a função $\overline{f} : S/R \longrightarrow T$, aonde: $\overline{f}([a]) = f(a)$
  - $\overline{f}$ é injetiva: suponha que $\overline{f}([a]) = \overline{f}([a'])$:
    - então: $f(a) = f(a')$

$$\Rightarrow \quad a\, R\, a' \quad \Rightarrow \quad [a] = [a']$$

  - $\overline{f}$ é sobrejetiva: suponha que $b \in T$:
    - $f(a) = b$ para algum elemento a em S *(pois f é sobrejetiva)*
    - então: $\overline{f}([a]) = f(a) = b$

Semigrupos Quocientes & Homomorfismos

- **Prova da parte (b):** Seja a relação de S/R para T:

$$\overline{f} = \{ ([a], f(a)) \mid [a] \in S/R\}$$

- $\overline{f}$ é uma função: suponha que $[a] = [a']$:
  - então: $a \, R \, a'$ e $f(a) = f(a')$
  - logo, $\overline{f}$ é a função $\overline{f} : S/R \longrightarrow T$, aonde: $\overline{f}([a]) = f(a)$
- $\overline{f}$ é injetiva: suponha que $\overline{f}([a]) = \overline{f}([a'])$:
  - então: $f(a) = f(a')$

$$\Rightarrow \quad a \, R \, a' \quad \Rightarrow \quad [a] = [a']$$

- $\overline{f}$ é sobrejetiva: suponha que $b \in T$:
  - $f(a) = b$ para algum elemento a em S *(pois f é sobrejetiva)*
  - então: $\overline{f}([a]) = f(a) = b$
- $\overline{f}$ preserva a estrutura das operações $\circledast$ e $*'$:

$$\overline{f}([a] \circledast [b]) = \overline{f}([a * b]) = f(a * b) = f(a) *' f(b) = \overline{f}([a]) *' \overline{f}([b])$$

Semigrupos Quocientes & Homomorfismos

- **Prova da parte (b):** Seja a relação de S/R para T:

$$\overline{f} = \{ ([a], f(a)) \mid [a] \in S/R\}$$

  - $\overline{f}$ é uma função: suponha que $[a] = [a']$:
    - então: $a \, R \, a'$ e $f(a) = f(a')$
    - logo, $\overline{f}$ é a função $\overline{f} : S/R \longrightarrow T$, aonde: $\overline{f}([a]) = f(a)$
  - $\overline{f}$ é injetiva: suponha que $\overline{f}([a]) = \overline{f}([a'])$:
    - então: $f(a) = f(a')$

$$\Rightarrow \quad a \, R \, a' \quad \Rightarrow \quad [a] = [a']$$

  - $\overline{f}$ é sobrejetiva: suponha que $b \in T$:
    - $f(a) = b$ para algum elemento a em S *(pois f é sobrejetiva)*
    - então: $\overline{f}([a]) = f(a) = b$
  - $\overline{f}$ preserva a estrutura das operações $\circledast$ e $*'$:

$$\overline{f}([a] \circledast [b]) = \overline{f}([a * b]) = f(a * b) = f(a) *' f(b) = \overline{f}([a]) *' \overline{f}([b])$$

  - Logo: $\overline{f}$ é um isomorfismo. $\square$

- **Exemplo:**
  - Considere o semigrupo livre $\boldsymbol{A^*}$ gerado por $\boldsymbol{A = \{0, 1\}}$ sob concatenação
    - note que $\boldsymbol{A^*}$ é um monóide, aonde a identidade é $\boldsymbol{\Lambda}$

- **Exemplo:**
  - Considere o semigrupo livre A^* gerado por $A = \{0, 1\}$ sob concatenação
    - note que A^* é um monóide, aonde a identidade é Λ
  - Seja N o conjunto dos inteiros não-negativos
    - então $(N, +)$ é um semigrupo

- **Exemplo:**
  - Considere o semigrupo livre A^* gerado por $A = \{0, 1\}$ sob concatenação
    - note que A^* é um monóide, aonde a identidade é Λ
  - Seja N o conjunto dos inteiros não-negativos
    - então $(N, +)$ é um semigrupo
  - A seguinte função $f : A^* \longrightarrow N$ é um homomorfismo:

    $f(\alpha) =$ número de 1s em α
  - Seja R a seguinte relação sobre A^*:

    $\alpha \, R \, \beta$ sse $f(\alpha) = f(\beta)$

SEMIGRUPOS QUOCIENTES & HOMOMORFISMOS

- **Exemplo:**
  - Considere o semigrupo livre A^* gerado por $A = \{0, 1\}$ sob concatenação
    - note que A^* é um monóide, aonde a identidade é Λ
  - Seja N o conjunto dos inteiros não-negativos
    - então $(N, +)$ é um semigrupo
  - A seguinte função $f : A^* \longrightarrow N$ é um homomorfismo:

    $f(\alpha) =$ número de 1s em α
  - Seja R a seguinte relação sobre A^*:

    $\alpha\, R\, \beta$ sse $f(\alpha) = f(\beta)$
  - Segundo o Teorema: $A^* / R \simeq N$
    - sob o isomorfismo $\overline{f} : A^* / R \longrightarrow N$ definido por:

      $\overline{f}([\alpha]) = f(\alpha) =$ número de 1s em α $\Box$

SEMIGRUPOS QUOCIENTES & HOMOMORFISMOS

- **Teorema (Fundamental do Homomorfismo):** (relembrando)
  - Sejam:
    - $f : S \longrightarrow T$ um homomorfismo de $(S, *)$ sobre $(T, *')$
    - R a relação sobre S definida por $a\, R\, b$ sse $f(a) = f(b)$
  - Então:

    (a) R é uma relação de congruência

    (b) $(T, *')$ e o semigrupo quociente $(S/R, \circledast)$ são isomórficos

- **Teorema (Fundamental do Homomorfismo):** (relembrando)
  - Sejam:
    - $f : S \longrightarrow T$ um homomorfismo de $(S, *)$ sobre $(T, *')$
    - R a relação sobre S definida por $a \, R \, b$ sse $f(a) = f(b)$
  - Então:

    (a) R é uma relação de congruência

    (b) $(T, *')$ e o semigrupo quociente $(S/R, \circledast)$ são isomórficos

- A parte (b) pode ser descrita pelo diagrama a seguir ($\Rightarrow$)

SEMIGRUPOS QUOCIENTES & HOMOMORFISMOS

$$
\begin{tikzcd}
S \arrow[rr] \arrow[dr, "f_R"'] & & T \\
& S/R \arrow[ur, "\overline{f}"'] &
\end{tikzcd}
$$

- f_R é o homomorfismo natural
- $\overline{f} \circ f_R = f$ pois:

$$
\begin{aligned}
(\overline{f} \circ f_R)(a) &= \overline{f}(f_R(a)) \\
&= \overline{f}([a]) = f(a)
\end{aligned}
$$

Produtos e Quocientes de Semigrupos

- Final deste item.

- Dica: fazer exercícios sobre Produtos e Quocientes de Semigrupos...