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

SEMIGRUPOS

- **Semigrupo:** conjunto S + oper. binária associativa definida sobre S.
  - Sistema algébrico simples.
  - Muitas aplicações importantes.
    - Ex.: máquinas de estados finitos
- Denotado por $(S, *)$.
  - Ou simplesmente por S (quando fica claro o que é "$*$").
- Também nos referimos a $a * b$ como o **produto** de a e b.
- $(S, *)$ é chamado de **comutativo** se $*$ é uma operação comutativa.

EXEMPLOS DE SEMIGRUPOS

- **Exemplo:** $(\mathbb{Z}, +)$ é um semigrupo comutativo.

- **Exemplo:** $(P(S), \cup)$ é um semigrupo comutativo.

- **Exemplo:** $(\mathbb{Z}, -)$ não é um semigrupo
  - pois a subtração não é associativa.

EXEMPLOS DE SEMIGRUPOS

- **Exemplo:** Seja S um conjunto fixo não-vazio.
  - E seja S^S o conjunto de todas as funções $f : S \to S$
  - Então, sejam f e g dois elementos de S^S:
    - definimos $f * g$ como $f \circ g$ (função composta)
  - $*$ é uma operação binária associativa sobre S^S
  - Portanto, $(S^S, *)$ é um semigrupo (não-comutativo). $\square$

Exemplos de Semigrupos

- **Exemplo:** Seja $(L, \leq)$ um reticulado.
  - Definição: $a * b = a \vee b$
  - Então, L é um semigrupo. $\square$

Exemplos de Semigrupos

- **Exemplo:** Seja $A = \{a_1, a_2, \ldots, a_n\}$.
  - Sejam α e β dois elementos de A^*.
  - Note que concatenação $(\cdot)$ é uma operação binaria sobre A^*.
    - É associativa: se α, β e γ são elementos quaisquer de A^*:

$$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

    - Logo, $(A^*, \cdot)$ é um semigrupo.
      - (é o chamado “semigrupo livre gerado por A”)

Associatividade em Semigrupos

- Em um semigrupo $(S, *)$ a propriedade associativa pode ser generalizada:

- **Teorema:** O produto dos elementos $a_1, a_2, \ldots, a_n \quad (n \geq 3)$, de um semigrupo, não depende da inserção de parênteses.
  - Ou seja, este produto pode ser escrito como: $a_1 * a_2 * \cdots * a_n$

- **Exemplo:** São iguais os produtos:
  - $((a_1 * a_2) * a_3) * a_4$
  - $a_1 * (a_2 * (a_3 * a_4))$
  - $(a_1 * (a_2 * a_3)) * a_4$

IDENTIDADES EM SEMIGRUPOS

- Um **elemento identidade** de um semigrupo satisfaz a:

$$e * a = a * e = a \quad , \qquad \forall a \in S$$

- **Exemplo:** O número 0 é uma identidade do semigrupo $(\mathbb{Z}, +)$.

- **Teorema:** Se um semigrupo $(S, *)$ tem uma identidade, ela é única.

- **Prova:**
  - Suponha que e e e' são identidades em S.
  - Como e é uma identidade: $e * e' = e'$
  - Também, como e' é uma identidade: $e * e' = e$
  - Portanto: $e = e'$ $\square$

MONÓIDES

- **Monóide:** semigrupo que tem identidade.

- **Exemplo:** O semigrupo $(P(S), \cup)$ é um monóide.
  - A identidade é o elemento $\emptyset$, pois:

$$\emptyset * A \;=\; \emptyset \cup A \;=\; A \;=\; A \cup \emptyset \;=\; A * \emptyset \;, \quad \forall A \in P(S)$$

- **Exemplo:** O semigrupo $(A^*, \cdot)$ é um monóide.
  - A identidade é o elemento Λ, pois:

$$\alpha \cdot \Lambda \;=\; \Lambda \cdot \alpha = \alpha \;, \quad \forall \alpha \in A^*$$

- **Exemplo:** O conjunto de todas as relações sobre um conjunto A é um monóide sob a operação de composição.
  - A identidade é a relação de igualdade Δ.

SUBSEMIGRUPOS & SUBMONÓIDES

- Sejam $(S, *)$ um semigrupo e T um subconjunto de S:
  - $(T, *)$ é um **subsemigrupo** de $(S, *)$ se T for fechado sob $*$
    - (fechado: $a * b \in T$ sempre que $a, b \in T$)

Similarmente:

- Seja $(S, *)$ um monóide (com identidade e) e seja T um subconjunto de S.
  - $(T, *)$ é um **submonóide** de $(S, *)$ se T for fechado sob $*$ e se $e \in T$.

SUBSEMIGRUPOS & SUBMONÓIDES

- Note que a associatividade vale em qualquer subconjunto de um semigrupo.
- Deste modo, um subsemigrupo $(T, *)$ de um semigrupo $(S, *)$ é por si mesmo um semigrupo.
- Da mesma forma: um submonóide de um monóide é ele próprio um monóide.

SUBSEMIGRUPOS & SUBMONÓIDES

- **Exemplo:**
  - Seja $(S, *)$ um semigrupo. Então:
    - $(S, *)$ é um subsemigrupo de $(S, *)$
  - Seja $(S, *)$ um monóide. Então:
    - $(S, *)$ é um submonóide de $(S, *)$
    - $(\{e\}, *)$ também é um submonóide de $(S, *)$

$\square$

Potências em semigrupos

- Seja a um elemento de um semigrupo $(S, *)$
- Para $n \in \mathbb{Z}^+$, definimos recursivamente as potências a^n:
  - $a^1 = a$
  - $a^n = a^{n-1} * a, \qquad n \geq 2$
- Além disto:
  - se $(S, *)$ é um monóide, definimos: $\quad a^0 = e$
  - se m e n são inteiros não-negativos: $\quad a^m * a^n = a^{m+n}$

POTÊNCIAS EM SEMIGRUPOS

- **Exemplo:**
  - Se $(S, *)$ é um semigrupo e:
    - $a \in S$
    - $T = \{a^i \mid i \in \mathbb{Z}^+\}$
  - Então $(T, *)$ é um subsemigrupo de $(S, *)$. $\square$

- **Exemplo:**
  - Se $(S, *)$ é um monóide e:
    - $a \in S$
    - $T = \{a^i \mid i \in \mathbb{Z}^+ \text{ ou } i = 0\}$
  - Então $(T, *)$ é um submonóide de $(S, *)$. $\square$

Potências em semigrupos

- **Exemplo:** Seja T o conjunto de todos os inteiros pares.
  - Então $(T, \times)$ é um subsemigrupo do monóide $(\mathbb{Z}, \times)$.
  - Mas não é um submonóide:
    - a identidade de $\mathbb{Z}$ (o número 1), não pertence a T. $\square$

ISOMORFISMOS

- Sejam $(S, *)$ e $(T, *')$ dois semigrupos.
  - Uma $f : S \to T$ é um **isomorfismo** de $(S, *)$ para $(T, *')$ se:
    - ela for uma bijeção de S para T
    - $f(a * b) = f(a) *' f(b), \qquad \forall a, b \in S$

Isomorfismos

- Já que f é uma bijeção de S para T:
  - f^{-1} existe e é uma correspondência um-para-um de T para S.
- **Proposição:** f^{-1} é um isomorfismo de $(T, *')$ para $(S, *)$.
- **Prova:**
  - sejam a' e b' elementos de T
  - já que f é sobrejetiva:
    - devem existir a e b em S tais que $f(a) = a'$ e $f(b) = b'$
    - então: $a = f^{-1}(a')$ e $b = f^{-1}(b')$
  - daí:

$$\begin{aligned} f^{-1}(a' *' b') &= f^{-1}(f(a) *' f(b)) \\ &= f^{-1}(f(a * b)) \\ &= (f^{-1} \circ f)(a * b) \\ &= a * b \\ &= f^{-1}(a') * f^{-1}(b') \qquad \square \end{aligned}$$

ISOMORFISMOS

- Se $(S, *)$ e $(T, *')$ são isomórficos, escrevemos: $S \simeq T$

- Procedimento para mostrar que $(S, *)$ e $(T, *')$ são isomórficos:
  1. Defina uma função $f : S \to T$ com $Dom(f) = S$.
  2. Mostre que f é um-para-um (injetiva).
  3. Mostre que f é sobrejetiva.
  4. Mostre que $f(a * b) = f(a) *' f(b)$.

ISOMORFISMOS

- **Exemplo:** Seja T os inteiros pares. Mostre que os semigrupos $(\mathbb{Z}, +)$ e $(T, +)$ são isomórficos.
  - Passo 1: a função $f : \mathbb{Z} \to T$ é $f(a) = 2a$
  - Passo 2: mostrando que f é injetiva (um-para-um):
    - suponha que $f(a_1) = f(a_2)$
    - então: $2a_1 = 2a_2 \quad \Longrightarrow \quad a_1 = a_2$
  - Passo 3: mostrando que f é sobrejetiva:
    - seja b qualquer inteiro par
    - então: $b/2 = a \in \mathbb{Z}$
  - Passo 4: f preserva relação entre operações:
    - $f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b) \qquad \square$

Isomorfismos

- Em geral:
  - é fácil verificar se uma $f : S \to T$ é ou não um isomorfismo
  - mas é difícil mostrar que dois semigrupos são isomórficos
- Como no caso dos reticulados:
  - quando dois semigrupos são isomórficos, só podem diferir na natureza dos seus elementos
  - suas estruturas de semigrupos devem ser idênticas
- Se S e T são semigrupos finitos:
  - operações binárias dadas por tabelas de multiplicação
  - S e T serão isomórficos se, rearranjando e renomeando os elementos de S, obtemos a tabela de T.

ISOMORFISMOS

- **Exemplo:** Seja $S = \{a, b, c\}$ e $T = \{x, y, z\}$.
  - Sejam as seguintes tabelas de multiplicação:

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*'$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

  - Fácil verificar que impõem estruturas de semigrupo a S e T.
  - Agora, considere a função: $f(a) = y \quad f(b) = x \quad f(c) = z$
  - Substituindo os elementos de S por suas imagens e rearranjando a tabela, obtemos, exatamente, a tabela de T
    - portanto, S e T são isomórficos. $\square$

Isomorfismos

- **Teorema:**
  - Sejam os monóides:
    - $(S, *)$, com identidade e
    - $(T, *')$, com identidade e'.
  - Então, se $f : S \to T$ é um isomorfismo, $f(e) = e'$.
- **Prova:**
  - Seja b um elemento qualquer de T.
  - Como f é sobrejetiva, há um a em S tal que $f(a) = b$.
  - Então: $b = f(a) = f(a * e) = f(a) *' f(e) = b *' f(e)$
  - Similarmente, como $a = e * a$, temos que: $b = f(e) *' b$.
  - Logo, $\forall b \in T$: $b = b *' f(e) = f(e) *' b$.
  - Ou seja, $f(e)$ é uma identidade para T.
  - Daí, como a identidade tem que ser única: $f(e) = e'$ $\square$

ISOMORFISMOS

- Conseqüência do teorema anterior:
  - Um semigrupo com identidade não pode ser isomórfico a um semigrupo sem identidade.
- **Exemplo:** Seja T o conjunto dos inteiros pares.
  - Então os semigrupos $(\mathbb{Z}, \times)$ e $(T, \times)$ não são isomórficos.
  - Pois $\mathbb{Z}$ tem uma identidade e T não. $\square$

HOMOMORFISMOS

- Agora vamos tirar da definição de isomorfismo de semigrupos as exigências de que ele seja injetivo e sobrejetivo.
  - Obtemos outro importante método para comparar as estruturas algébricas de dois semigrupos:

- Sejam $(S, *)$ e $(T, *')$ dois semigrupos.
  - Uma $f : S \to T$ é um **homomorfismo** de $(S, *)$ para $(T, *')$ se:

$$f(a * b) = f(a) *' f(b), \qquad \forall a, b \in S$$

- Nota: se, por acaso, f também for sobrejetiva, dizemos que T é a **imagem homomórfica** de S.

HOMOMORFISMOS

- **Exemplo:** Seja $A = \{0, 1\}$ e considere os semigrupos:
  - $(A*, \cdot)$, onde $\cdot$ é concatenação
  - $(A, +)$, onde $+$ é definida pela tabela de multiplicação:

+	0	1
0	0	1
1	1	0

  - Agora, seja a função $f : A^* \longrightarrow A$, definida por:

$$f(\alpha) = \begin{cases} 1 & \text{se } \alpha \text{ tem um nro ímpar de 1s} \\ 0 & \text{se } \alpha \text{ tem um nro par de 1s} \end{cases}$$

  - f é um homomorfismo, pois: $f(\alpha \cdot \beta) = f(\alpha) + f(\beta), \quad \forall \alpha, \beta \in A^*$
  - Além disto, f é sobrejetiva, pois: $f(0) = 0$ e $f(1) = 1$
  - Mas f não é um isomorfismo, pois não é um-para-um (injetiva). $\square$

HOMOMORFISMOS

- Diferença: o isomorfismo tem que ser injetivo e sobrejetivo.
- Para ambos: "imagem de um produto" = "produto das imagens"

- **Teorema:** Sejam:
  - $(S, *)$ e $(T, *')$ monóides com respectivas identidades e e e'
  - $f : S \rightarrow T$ um homomorfismo de $(S, *)$ para $(T, *')$

  Então $f(e) = e'$.

- A união deste teorema com os dois a seguir mostra que:
  - se um semigrupo $(T, *')$ é a imagem homomórfica do semigrupo $(S, *)$:
    - $(T, *')$ tem uma forte semelhança algébrica com $(S, *)$.

HOMOMORFISMOS

- **Teorema:**
  - Seja f um homomorfismo de um semigrupo $(S, *)$ para um semigrupo $(T, *')$
  - e seja S' um subsemigrupo de $(S, *)$.
  - Então:

    $$f(S') = \{t \in T \mid t = f(s) \text{ para algum } s \in S'\}$$

    é um subsemigrupo de $(T, *')$

    - ou seja: "a imagem de S' sob f é um subsemigrupo de $(T, *')$"

prova $\longrightarrow$

- **Prova:**
  - se t_1 e t_2 são elementos quaisquer de $f(S')$, então:
    - $t_1 = f(s_1)$ e $t_2 = f(s_2)$ para alguns $s_1, s_2 \in S'$
  - daí:
$$\begin{aligned} t_1 *' t_2 &= f(s_1) *' f(s_2) \\ &= f(s_1 * s_2) \\ &= f(s_3) \end{aligned}$$
    - aonde: $s_3 = s_1 * s_2 \in S'$
  - logo: $t_1 *' t_2 \in f(S')$
    - portanto: $f(S')$ é fechado sob $*'$
  - além disto, já que a associatividade vale em T, ela vale em $f(S')$
  - assim, $f(S')$ é um subsemigrupo de $(T, *')$. $\square$

HOMOMORFISMOS

- **Teorema:** Se f é um homomorfismo de um semigrupo comutativo $(S, *)$ sobre um semigrupo $(T, *')$, então $(T, *')$ também é comutativa.
- **Prova:**
  - sejam t_1 e t_2 elementos quaisquer de T.
  - então: $t_1 = f(s_1)$ e $t_2 = f(s_2)$ para alguns s_1 e s_2 em S
  - logo:
$$\begin{aligned} t_1 *' t_2 &= f(s_1) *' f(s_2) \\ &= f(s_1 * s_2) \\ &= f(s_2 * s_1) \\ &= f(s_2) *' f(s_1) \\ &= t_2 *' t_1 \end{aligned}$$
  - portanto: $(T, *')$ também é comutativa. $\square$

SEMIGRUPOS

- Final deste item.
- Dica: fazer exercícios sobre semigrupos...