PARTE D

TEORIA DOS AUTÔMATOS FINITOS

CAPÍTULO I

RELAÇÕES, FUNÇÕES E MONÓIDES

Neste capítulo apresentamos as definições de alguns conceitos básicos, bem como algumas de suas propriedades. No texto omitimos a maioria das demonstrações. Em particular, as afirmações seguidas de um ponto de exclamação são enunciados de propriedades cuja demonstração fica a cargo do leitor.

1. Relações e funções

Dados conjuntos A e B, uma *relação* r de A para B é um subconjunto do produto cartesiano $A \times B$. Os conjuntos A e B são ditos *domínio* e *co-domínio* da relação r. Para um subconjunto S de A, definimos a *imagem* de S por r:

$$Sr = \{b \in B \mid (a, b) \in r \text{ para algum } a \in S\}.$$

Convencionamos nesta parte do livro denotar um subconjunto unitário $\{a\}$ de A pelo seu único elemento a. Assim, $ar = b$ significa que (a, b) é o único par ordenado em r cujo primeiro elemento é a. Note que

$$(a, b) \in r \quad \text{e} \quad b \in ar$$

são notações equivalentes. Além disso, uma relação r é completamente determinada pelos conjuntos ar, no seguinte sentido: Duas relações $r, s \subseteq A \times B$ são iguais sse para todo $a \in A$ $ar = as$!

A *inversa* da relação $r \subseteq A \times B$ é a relação $r^{-1} \subseteq B \times A$, definida por:

$$r^{-1} = \{(b, a) \in B \times A \mid (a, b) \in r\}.$$

Para toda relação $r \subseteq A \times B$,

$$(r^{-1})^{-1} = r!$$

A *composição* da relação $r \subseteq A \times B$ com a relação $s \subseteq B \times C$ é a relação $rs \subseteq A \times C$, definida por:

$$rs = \{(a, c) \in A \times C \mid (a, b) \in r \quad \text{e} \quad (b, c) \in s \text{ para algum } b \in B\}.$$

Dada outra relação $t \subseteq C \times D$, resulta que

$$(rs)t = r(st)!$$

Isto é, a composição de relações é uma operação associativa, não havendo necessidade de utilizar parêntesis ao escrevermos rst. Analogamente, para $S \subseteq A$, Srs é uma expressão bem definida, pois

$$(Sr)s = S(rs)!$$

No caso de r ser uma relação de A para A, diremos também que r é uma relação *sobre* A.

Funções são casos particulares muito importantes de relações. Assim, uma *função* f de A para B, escreve-se $f : A \to B$, é uma relação $f \subseteq A \times B$, tal que, para todo a em A, af é um subconjunto unitário de B. Neste caso, as fórmulas

$$(a, b) \in f, \quad b \in af \text{ e } af = b$$

são todas equivalentes.

Dadas funções $f : A \to B$ e $g : B \to C$, a sua composição fg é uma função $fg : A \to C$! Observe que nesta parte do livro a imagem de a por f é denotada por af em vez da notação mais comum $f(a)$. Além disso a função composta fg consiste em aplicar primeiro f e depois g, ao contrário da notação tradicional.

Uma função $f : A \to B$ é *injetora* se para todo $a_1, a_2 \in A$, $a_1f = a_2f$ implica que $a_1 = a_2$; ela é *sobrejetora* se $Af = B$; e é *bijetora* se ela for injetora e sobrejetora. Nestes casos, podemos dizer também que a função f é, respectivamente, uma *injeção*, *sobrejeção* ou *bijeção*.

A *relação identidade* 1_A sobre A é definida por

$$1_A = \{(a, a) \in A \times A \mid a \in A\},$$

e é uma função bijetora $1_A : A \to A$. Para toda relação $r \subseteq A \times A$,

$$r1_A = 1_Ar = r!$$

Note que a inversa f^{-1} de uma função $f : A \to B$ é uma relação $f^{-1} \subseteq B \times A$ que em geral não é uma função!

A proposição seguinte caracteriza funções injetoras, sobrejetoras e bijetoras.

PROPOSIÇÃO 1. *Seja $g : A \to B$ uma função com domínio não vazio. Então,*

(i) *g é injetora sse existe uma função $h : B \to A$, tal que $gh = 1_A$;*

(ii) *g é sobrejetora sse existe uma função $f : B \to A$, tal que $fg = 1_B$;*
(iii) *g é bijetora sse a relação g^{-1} é uma função $g^{-1} : B \to A$, tal que $gg^{-1} = 1_A$ e $g^{-1}g = 1_B$.*

Demonstração. (i) Suponhamos que $h : B \to A$ seja uma função, tal que $gh = 1_A$. Sejam $a_1, a_2 \in A$, tais que $a_1g = a_2g$. Então $a_1gh = a_2gh$. Como $gh = 1_A$, resulta que $a_1gh = a_1$ e $a_2gh = a_2$; logo $a_1 = a_2$. Isto é, a função g é injetora.

Reciprocamente, suponhamos que a função g seja injetora. Consideramos inicialmente a relação $g^{-1} \subseteq B \times A$, e mostramos que para cada b em B, bg^{-1} é vazio ou é um subconjunto unitário de A. De fato, suponha que $a_1, a_2 \in bg^{-1}$, então $a_1g = a_2g$, logo $a_1 = a_2$ pois g é injetora. Como $A \neq \emptyset$, podemos escolher um elemento a_0 em A e definir uma função h como segue:

$$bh = \begin{cases} a_0 & \text{se } bg^{-1} = \emptyset \\ bg^{-1} & \text{caso contrário} \end{cases} \qquad (b \in B).$$

Resta demonstrar que $gh = 1_A$. De fato, seja $a \in A$, e seja $ag = b$. Então $a \in bg^{-1}$, e pela construção $bh = a$. Logo, $agh = bh = a$, resultando que $gh = 1_A$.

(ii) Suponhamos que $f : B \to A$ seja uma função, tal que $fg = 1_B$. Está claro que $Bf \subseteq A$, logo $Bfg \subseteq Ag$. Por outro lado $Bfg = B1_B = B$, isto é, $B \subseteq Ag$. Como $Ag \subseteq B$, resulta que $Ag = B$, isto é, g é sobrejetora.

Reciprocamente, suponhamos que a função g seja sobrejetora. Consideremos inicialmente a relação $g^{-1} \subseteq B \times A$. Para todo b em B, bg^{-1} é não vazio. De fato, como g é sobrejetora, $Ag = B$ e para todo b em B existe a em A, tal que $ag = b$, isto é $a \in bg^{-1}$. Nestas condições, para cada b em B, escolhemos um elemento a em bg^{-1} e colocamos $bf = a$. Assim, $bfg = ag = b$. Como $bfg = b$ para todo b em B, resulta que $fg = 1_B$.(1)

(iii) Suponhamos que a relação g^{-1} seja uma função $g^{-1} : B \to A$, tal que $gg^{-1} = 1_A$ e $g^{-1}g = 1_B$. Por (i) e (ii), g é injetora e sobrejetora, logo a função g é bijetora.

---

(1) Observe que nesta demonstração estamos usando (implicitamente) o axioma da escolha. Na verdade demonstra-se que a afirmação (ii) é equivalente a este axioma.

Reciprocamente, suponhamos que a função g seja bijetora. Por (i) e (ii), existem funções $f, h : B \to A$, tais que $gh = 1_A$ e $fg = 1_B$. Inicialmente mostramos que $f = h$. De fato,

$$f = f1_A = f(gh) = (fg)h = 1_Bh = h.$$

Por outro lado, $fg = 1_B$ implica que $f \subseteq g^{-1}$. De fato, se $(b, a) \in f$, isto é, $bf = a$, então $bfg = ag$. Como $fg = 1_B$, resulta que $ag = b$, isto é $(b, a) \in g^{-1}$. Analogamente, $gh = 1_A$ implica que $g \subseteq h^{-1}$, logo $g^{-1} \subseteq (h^{-1})^{-1} = h$. Assim, $f \subseteq g^{-1} \subseteq h$; mas como $f = h$, resulta que $f = g^{-1} = h$. Portanto g^{-1} é uma função, $gg^{-1} = 1_A$ e $g^{-1}g = 1_B$. ■

Dadas funções $f : A \to B$ e $f' : A' \to B'$, dizemos que f é uma *restrição* de f' se $A \subseteq A'$, $B \subseteq B'$ e $f \subseteq f'$, isto é, para todo a em A $af = af'$. Neste caso dizemos também que f' é uma *extensão* de f.

Dado um conjunto A, uma relação $r \subseteq A \times A$ é de *equivalência* sobre A sse

$$1_A \subseteq r, \; r \subseteq r^{-1} \quad \text{e} \quad rr \subseteq r,$$

isto é, r é *reflexiva*, *simétrica* e *transitiva*, respectivamente. Escrevendo $a \sim b$ ao invés de $(a, b) \in r$, as propriedades acima tomam sua forma habitual! É bem conhecido que para $a_1, a_2 \in A$, a_1r e a_2r são conjuntos não vazios que são disjuntos ou são iguais! Eles são iguais sse $(a_1, a_2) \in r$! Para $a \in A$, ar é a *classe de equivalência* contendo a, e o *conjunto quociente* de A por r é

$$A/r = \{ar \mid a \in A\}.$$

A *projeção canônica* de A em A/r é a função

$$p : A \to A/r$$

que associa a cada elemento a de A a classe de equivalência ar. A projeção canônica é sobrejetora e $pp^{-1} = r$!

Dada uma função $f : A \to B$, a relação $ff^{-1} \subseteq A \times A$ é uma relação de equivalência sobre A! Observe que para a_1, a_2 em A, $(a_1, a_2) \in ff^{-1}$ sse $a_1f = a_2f$! Assim, para cada a em A, a classe de equivalência aff^{-1} que contém a é dada por:

$$aff^{-1} = \{b \in A \mid bf = af\}!$$

PROPOSIÇÃO 2. *Seja $g : A \to B$ uma função sobrejetora e seja $f : A \to C$ uma função. Se $gg^{-1} \subseteq ff^{-1}$ então existe* *uma única função $h : B \to C$, tal que $f = gh$. Ademais, h é sobrejetora sse f é sobrejotora; e h é injetora sse $gg^{-1} = ff^{-1}$.*

As funções f, g e h no enunciado da proposição acima podem ser representadas como no diagrama da Figura 1. Costuma-se dizer que este diagrama é comutativo para expressar o fato de que $f = gh$.

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f"'] & B \arrow[dl, dashed, "h"] \\ C & \end{tikzcd}$$

Figura 1 — Diagrama para a Proposição 2.

Demonstração. Se A for vazio, então B é vazio também, pois a função g é sobrejetora. Assim, $f = g = \varnothing$, e a função $h = \varnothing$ satisfaz trivialmente a proposição! Caso contrário, A, B e C são todos não-vazios! Pela Proposição 1 (ii), existe uma função $g_e : B \to A$, tal que

$$g_e g = 1_B. \tag{1}$$

Colocamos então

$$h = g_e f. \tag{2}$$

Para provar que $f = gh$, observamos inicialmente que $g = g1_B = gg_eg$. Seja a em A, então $ag = agg_eg$, logo $(a, agg_e) \in gg^{-1}$. Como $gg^{-1} \subseteq ff^{-1}$ por hipótese, resulta que $(a, agg_e) \in ff^{-1}$, isto é, $af = agg_ef$. Como o raciocínio acima vale para todo a em A, concluimos que $f = gg_ef$. Finalmente, como $g_ef = h$, resulta que

$$f = gh. \tag{3}$$

Para provar a unicidade de h, suponhamos que $h' : B \to C$ seja outra função tal que $f = gh'$. Usando (2) e (1), vem que $h = g_ef = g_egh' = h'$, isto é $h = h'$.

Suponhamos agora que h seja sobrejetora. Pela Proposição 1 (ii), existe uma função $h_e : C \to B$, tal que $h_eh = 1_C$. Usando (1) e (3), vem que $1_C = h_eh = h_e1_Bh = h_eg_egh = h_eg_ef$, isto é, $(h_eg_e)f = 1_C$. A função f é sobrejetora pela Proposição 1 (ii). Reciprocamente, suponhamos que f é sobrejetora. Pela Proposição 1 (ii), existe uma função

$f_e : C \to A$, tal que $f_e f = 1_C$. Resulta de (3) que $(f_e g)h = 1_C$, logo a função h é sobrejetora pela Proposição 1 (ii).

Suponhamos finalmente que h seja injetora. Como $gg^{-1} \subseteq ff^{-1}$, basta demonstrar que $ff^{-1} \subseteq gg^{-1}$. De fato, seja $(a_1, a_2) \in ff^{-1}$, isto é, $a_1 f = a_2 f$. De (3), $f = gh$, logo $a_1 gh = a_2 gh$. Como h é injetora, resulta que $a_1 g = a_2 g$, isto é, $(a_1, a_2) \in gg^{-1}$. Reciprocamente, suponhamos que $gg^{-1} = ff^{-1}$. Para demonstrar que h é injetora, sejam b_1 e b_2 em B, tais que $b_1 h = b_2 h$; basta provar então que $b_1 = b_2$. De fato, como $h = g_e f$ por (2), resulta que $b_1 g_e f = b_2 g_e f$, isto é, $(b_1 g_e, b_2 g_e) \in ff^{-1}$. Segue da hipótese que $(b_1 g_e, b_2 g_e) \in gg^{-1}$, isto é $b_1 g_e g = b_2 g_e g$. Porém, $g_e g = 1_B$, por (1), logo $b_1 = b_2$. ■

Talvez seja interessante examinar a Proposição 2 de outro ângulo. Vimos que gg^{-1} e ff^{-1} são relações de equivalência sobre o conjunto A. Seja agora b um elemento de B. Como g é sobrejetora, bg^{-1} é uma classe de equivalência de gg^{-1}. A condição $gg^{-1} \subseteq ff^{-1}$ garante que cada classe de equivalência de gg^{-1} está contida numa classe de equivalência de ff^{-1}. Logo, existe um único c em C, tal que $bg^{-1} \subseteq cf^{-1}$ Nestas condições $bh = c$.

Descrevemos a seguir uma aplicação importante da Proposição 2. Dada uma função $f : A \to B$, vimos que ff^{-1} é uma relação de equivalência sobre A. Seja $p : A \to A/ff^{-1}$ a projeção canônica de ff^{-1}; então p é sobrejetora e $pp^{-1} = ff^{-1}$. Segue da Proposição 2 que existe uma única função $h : A/ff^{-1} \to B$, tal que $f = ph$. Ademais, pela mesma proposição, h é injetora. Observe que h é bijetora sse f é sobrejetora.

$$\begin{tikzcd}
A \arrow[r, "p"] \arrow[d, "f"'] & A/ff^{-1} \arrow[dl, "h"] \\
B &
\end{tikzcd}$$

Figura 2 — Funções e relações de equivalência.

Terminamos esta seção com duas notações relativas à teoria dos conjuntos. O *conjunto potência* de um conjunto A será denotado por $\mathfrak{p}(A)$, isto é

$$\mathfrak{p}(A) = \{B \mid B \subseteq A\}.$$

A *cardinalidade* de um conjunto finito A será denotada (nesta parte do livro) por *card* A.

2. Monóides

Um *monóide* consiste de um conjunto M, munido de uma operação binária associativa (escrita multiplicativamente), e que contém um *elemento identidade* $1 \in M$. Isto é, para todo $m_1, m_2, m_3 \in M$,

$$(m_1m_2)m_3 = m_1(m_2m_3) \quad \text{e} \quad m_1 1 = 1m_1 = m_1.$$

Assim, dado um conjunto A, o conjunto das relações (funções) de A para A, com a operação de composição, é um monóide cuja identidade é 1_A, e que será denotado por *Rel* A (*Fun* A). Analogamente, $\mathfrak{p}(A)$ com a operação de união é um monóide cuja identidade é o conjunto vazio $\varnothing$.

Dados subconjuntos A e B de um monóide M, definimos o seu *produto* por:

$$AB = \{m_1m_2 \in M \mid m_1 \in A \quad \text{e} \quad m_2 \in B\}.$$

Com esta multiplicação de subconjuntos, $\mathfrak{p}(M)$ transforma-se num monóide, com identidade 1. Note que para subconjuntos de M, o produto distribui sobre a união, isto é, para $A, B, C \subseteq M$,

$$A(B \cup C) = AB \cup AC \quad \text{e} \quad (A \cup B)C = AC \cup BC!$$

Para um natural n e um subconjunto A de M, definimos A^n indutivamente, por:

$$A^0 = 1 \quad \text{e} \quad A^{n+1} = A^nA.$$

Um subconjunto T de M é um *submonóide* de M sse

$$1 \in T \quad \text{e} \quad T^2 \subseteq T.$$

Em outras palavras, T é um submonóide de M sse T contém a identidade de M e é fechado sob a operação binária de M.

Dado um subconjunto A do monóide M, consideremos a intersecção A^* de todos os submonóides de M que contêm A, isto é,

$$A^* = \cap T,$$

onde a intersecção se estende sobre todos os submonóides T de M, tais que $A \subseteq T$. Observe que a intersecção de submonóides de M é um submonóide de M! Assim, A^* é um submonóide de M. De fato,

A^* é o único submonóide minimal de M que contém A! Por isso, costuma-se dizer que A^* é o *menor submonóide de M que contém A*, ou que A^* é o *submonóide de M gerado por A*. Ocasionalmente diremos também que A^* é a *estrela* de A. Demonstra-se que

$$A^* = 1 \cup A \cup A^2 \cup \ldots \cup A^n \cup \ldots !$$

Em outras palavras, A^* consiste exatamente daqueles elementos de M que podem ser expressos como o produto de um número finito de fatores que pertencem a A. Note também que

$$A^* = 1 \cup AA^* = 1 \cup A^*A \; !$$

Dados monóides M e M', com identidades 1 e 1′, uma função $f : M \to M'$ é um *morfismo* sse

$$1f = 1' \text{ e } (m_1m_2)f = (m_1f)\,(m_2f) \text{ para todo } m_1, m_2 \in M.$$

A composição de morfismos é um morfismo! Um *monoforfismo*, *epimorfismo*, ou *isomorfismo* é, respectivamente, um morfismo injetor, sobrejetor, ou bijetor.

Seja M um monóide e r uma relação de equivalência sobre M. Dizemos que r é uma *relação de congruência* sobre M sse para todo m_1 e m_2 em M

$$(m_1r)\,(m_2r) \subseteq (m_1m_2)r,$$

isto é, o produto de classes de equivalência (como subconjuntos de M) está contido em uma outra classe de equivalência. Escrevendo $m_1 \sim m_2$, ao invés de $(m_1, m_2) \in r$, é fácil demonstrar que as afirmações seguintes são equivalentes:

(i) r é uma relação de congruência,

(ii) para todo $m, m', m'' \in M$, $m' \sim m''$ implica que $m'm \sim m''m$ e $mm' \sim mm''$,

(iii) para todo $m_1, m_1', m_2, m_2' \in M$, $m_1 \sim m_1'$ e $m_2 \sim m_2'$ implica que $m_1m_2 \sim m_1'm_2'$!

Se r for uma relação de congruência sobre M, podemos definir um produto (indicador por $\cdot$) no conjunto quociente M/r:

$$(m_1r)\cdot(m_2r) = (m_1m_2)r.$$

O conjunto M/r munido deste produto é um monóide com identidade $1r$! Assim, chamamos M/r de *monóide quociente* de M por r. A projeção canônica $p : M \to M/r$ é um epimorfismo neste caso!

Para monóides, a Proposição 2 toma a seguinte forma:

PROPOSIÇÃO 3. *Sejam* M_1, M_2 *e* M_3 *monóides*, $g : M_1 \to M_2$ *um epimorfismo e* $f : M_1 \to M_3$ *um morfismo. Se* $gg^{-1} \subseteq ff^{-1}$ *então existe um único morfismo* $h : M_2 \to M_3$, *tal que* $f = gh$. *Ademais, h é um epimorfismo sse f é um epimorfismo; e h é um monomorfismo sse* $gg^{-1} = ff^{-1}$.

$$\begin{tikzcd} M_1 \arrow[r, "g"] \arrow[d, "f"'] & M_2 \arrow[dl, dashed, "h"] \\ M_3 & \end{tikzcd}$$

Figura 3 — Morfismos na Proposição 3.

Demonstração. Tendo em vista a Proposição 2, é suficiente mostrar que a função h dada por aquela proposição é um morfismo. De fato, sejam m_1, m_2 em M_2. Como g é sobrejetora, existem m'_1, m'_2 em M_1, tais que $m'_i g = m_i$ $(i = 1, 2)$. Como f é um morfismo, $(m'_1 m'_2)f = (m'_1 f)(m'_2 f)$; logo $(m'_1 m'_2)gh = (m'_1 gh)(m'_2 gh)$, já que $f = gh$. Agora, g é um morfismo, logo $[(m'_1 g)(m'_2 g)]h = (m'_1 gh)(m'_2 gh)$. Substituindo $m'_i g$ por m_i $(i = 1, 2)$, obtemos que $(m_1 m_2)h = (m_1 h)(m_2 h)$. Finalmente, denotando por 1_i a identidade de M_i $(i = 1, 2, 3)$, temos que $1_3 = 1_1 f = 1_1 gh = 1_2 h$. Assim, h é um morfismo. ■

Dado um morfismo $f : M_1 \to M_2$, a relação de equivalência ff^{-1} sobre M_1 é uma congruência! Segue da Proposição 3 que existe um monomorfismo $h : M_1/ff^{-1} \to M_2$ tal que $f = ph$, onde p é a projeção canônica $p : M_1 \to M_1/ff^{-1}$! (Vide Figura 4.) O monomorfismo h é um isomorfismo sse f é um epimorfismo!

$$\begin{tikzcd} M_1 \arrow[r, "p"] \arrow[d, "f"'] & M_1/ff^{-1} \arrow[dl, "h"] \\ M_2 & \end{tikzcd}$$

Figura 4 — Morfismos e relações de congruência.

Certos monóides, chamados de monóides livres, tem um papel importante nos capítulos seguintes. Passamos a descrevê-los.

Dado um conjunto Σ, consideremos o conjunto S de seqüências finitas de elementos de Σ:

$$s = (\sigma_1, \sigma_2, \ldots, \sigma_n) \quad (n \geq 0).$$

Definimos um produto em S por *concatenação*, isto é, se

$$t = (\tau_1, \tau_2, \ldots, \tau_m)$$

for outro elemento de S, o produto st de s e t é:

$$st = (\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_m).$$

A concatenação é associativa, logo S, munido deste produto, é um monóide cuja identidade é a seqüência vazia $1 = (\ )$.

Convencionamos denotar a seqüência unitária (σ) de S por σ. Desta forma, utilizando o produto já definido, o elemento s acima de S pode ser escrito (se $n > 0$):

$$s = \sigma_1 \sigma_2 \ldots \sigma_n.$$

Devido a esta notação, chamamos Σ de *alfabeto*, seus elementos de *letras* e os elementos de S de *palavras*. Por outro lado, usando a convenção acima, podemos considerar Σ como um subconjunto de S. Note que o submonóide de S gerado por Σ é o próprio S, isto é, $S = \Sigma^*$. Assim, chamamos S de *monóide livre* gerado por Σ e o denotamos por Σ^*.

Dada a palavra s acima em Σ^*, o natural n é o seu *comprimento* e é denotado por $|s|$. Resulta que

$$|1| = 0 \text{ e } |st| = |s| + |t| \text{ para todo } s, t \text{ em } \Sigma^*.$$

Sejam s, t_1, t_2 e t_3 em Σ^*, tais que $s = t_1 t_2 t_3$. Dizemos que t_2 é um *segmento* de s e que t_1 (t_3) é um *segmento inicial* (*segmento final*) de s.

A propriedade fundamental dos monóides livres é dada por:

PROPOSIÇÃO 4. *Seja M um monóide e seja $f : \Sigma \to M$ uma função. Existe uma única extensão de f a um morfismo $f^* : \Sigma^* \to M$.*

Demonstração. Definimos a função f^* como segue:

$$1f^* = 1,$$

e para uma palavra $\sigma_1\sigma_2 \ldots \sigma_n$ de Σ^*, $n \geq 1$, com σ_i em Σ $(1 \leq i \leq n)$, colocamos

$$(\sigma_1\sigma_2 \ldots \sigma_n)f^* = (\sigma_1 f)(\sigma_2 f) \ldots (\sigma_n f).$$

É imediato verificar que f^* é uma extensão de f e que dadas palavras s e t em Σ^*, $(st)f^* = (sf^*)(tf^*)$. Logo, f^* é um morfismo.

Suponhamos agora que $g : \Sigma^* \to M$ seja uma outra extensão de f a um morfismo. Mostramos que $sg = sf^*$ para todo s em Σ^*. Para tanto procedemos por indução no comprimento de palavras em Σ^*. Se $|s| = 0$, então $s = 1$, logo $1g = 1$ pois g é um morfismo. Assim, $1g = 1f^*$. Se $|s| > 0$, então existem t em Σ^* e σ em Σ, tais que $s = t\sigma$. Como g é um morfismo, obtemos $sg = (t\sigma)g = (tg)(\sigma g)$. Como $|t| < |s|$, vem pela hipótese da indução que $tg = tf^*$. Por outro lado, $\sigma g = \sigma f = \sigma f^*$, pois g e f^* são ambas extensões de f. Assim, $(tg)(\sigma g) = (tf^*)(\sigma f^*) = (t\sigma)f^* = sf^*$, pois f^* é um morfismo. Segue que $sg = sf^*$. Logo, $g = f^*$. ■

EXERCÍCIOS

1. Prove as afirmações do texto que são seguidas de um ponto de exclamação.
2. Enumere todas as relações de A para A, onde A é o conjunto $\{a, b\}$ de dois elementos. Indique quais são funções, funções injetoras, funções sobrejetoras e funções bijetoras. Indique também o inverso de cada uma das relações.
3. Enumere todas as funções de A para A, onde A é o conjunto $\{a, b, c\}$ de três elementos. Indique as funções bijetoras e o inverso de cada uma destas.
4. Enumere todas as relações de equivalência sobre o conjunto $\{a, b, c\}$ de três elementos.
5. Em cada caso prove ou desprove a afirmação dada:
   (i) Para toda relação $r \subseteq A \times B$, $rr^{-1} \subseteq 1_A$.
   (ii) Para toda relação $r \subseteq A \times B$, $1_A \subseteq rr^{-1}$.
6. Sejam r_1 e r_2 relações de A para B, s_1 e s_2 relações de B para C e P_1 e P_2 subconjuntos de A. Prove que:
   (i) Se $P_1 \subseteq P_2$ e $r_1 \subseteq r_2$ então $P_1r_1 \subseteq P_2r_2$.
   (ii) Se $r_1 \subseteq r_2$ e $s_1 \subseteq s_2$ então $r_1s_1 \subseteq r_2s_2$.
   (iii) $(P_1 \cup P_2)r_1 = P_1r_1 \cup P_2r_1$.

(iv) $(P_1 \cap P_2)r_1 \subseteq P_1r_1 \cap P_2r_1$.
(v) $P_1(r_1 \cup r_2) = P_1r_1 \cup P_1r_2$.
(vi) $P_1(r_1 \cap r_2) \subseteq P_1r_1 \cap P_1r_2$.
(vii) $r_1(s_1 \cup s_2) = r_1s_1 \cup r_1s_2$.
(viii) $(r_1 \cup r_2)s_1 = r_1s_1 \cup r_2s_1$.
(ix) $r_1(s_1 \cap s_2) \subseteq r_1s_1 \cap r_1s_2$.
(x) $(r_1 \cap r_2)s_1 \subseteq r_1s_1 \cap r_2s_1$.
(xi) se $r_1 \subseteq r_2$ então $r_1^{-1} \subseteq r_2^{-1}$.
(xii) $(r_1 \cup r_2)^{-1} = r_1^{-1} \cup r_2^{-1}$.
(xiii) $(r_1 \cap r_2)^{-1} = r_1^{-1} \cap r_2^{-1}$.

7. Prove que as inclusões nos pontos (iv), (vi), (ix) e (x) do exercício anterior não podem, em geral, ser substituídas por igualdades.

8. Sejam $r \subseteq A \times B$ e $s \subseteq B \times C$ relações. Mostre que $(rs)^{-1} = s^{-1}r^{-1}$.

9. Seja $f : A \to B$ uma função. Mostre que se $A = \emptyset$, então $f = \emptyset$ e f é uma função injetora. Neste caso f é sobrejetora sse $B = \emptyset$. Prove que se $B = \emptyset$, então $A = \emptyset$ e f é uma função bijetora.

10. Prove que uma relação $r \subseteq A \times B$ é uma função sse $r^{-1}r \subseteq 1_B$ e $1_A \subseteq rr^{-1}$.

11. Seja $r \subseteq A \times B$ uma relação, onde $B \neq \emptyset$. Prove que as afirmações abaixo são equivalentes:
(i) r é uma função,
(ii) r é maximal com relação à propriedade $r^{-1}r \subseteq 1_B$,
(iii) r é minimal com relação à propriedade $1_A \subseteq rr^{-1}$.

12. Seja $r \subseteq A \times B$ uma relação, onde $B \neq \emptyset$. Prove que:
(i) existe uma função $f : A \to B$, tal que $r \subseteq f$ sse $r^{-1}r \subseteq 1_B$,
(ii) existe uma função $g : A \to B$, tal que $g \subseteq r$ sse $1_B \subseteq rr^{-1}$.

13. Seja $f : A \to B$ uma função. Prove que f é injetora sse $ff^{-1} = 1_A$, e que f é sobrejetora sse $1_B = f^{-1}f$.

14. Sejam $f : A \to B$ e $g : B \to C$ funções. Prove que:
(i) Se f e g forem injetoras então fg é injetora.
(ii) Se f e g forem sobrejetoras então fg é sobrejetora.
(iii) Se fg for injetora então f é injetora.
(iv) Se fg for sobrejetora então g é sobrejetora.

15. Dê exemplos de funções $f : A \to B$ e $g : B \to C$, tais que f é injetora, g é sobrejetora mas fg não é nem injetora nem sobrejetora.

16. Mostre que para toda função $f : A \to B$, $ff^{-1}f = f$.

17. Dada uma função $f : A \to B$, com $A \neq \emptyset$, construa uma outra função $g : B \to A$, tal que $fgf = f$.

18. Sejam $f : A \to B$, $g : B \to C$ e $h : C \to D$ funções e suponha que f e h são bijetoras. Mostre que g é injetora (sobrejetora, bijetora) sse fgh é injetora (sobrejetora, bijetora).

19. Seja $f : A \to B$ uma função. Prove que:
    (i) f é injetora sse para todo subconjunto X e Y de A $(X \cap Y)f = Xf \cap Yf$.
    (ii) f é injetora sse para todo subconjunto X de A $(A \backslash X)f \subseteq B \backslash (Xf)$.
    (iii) f é sobrejetora sse para todo subconjunto X de A $B \backslash (Xf) \subseteq (A \backslash X)f$.

20. Seja $f : A \to B$ uma função, e sejam X e Y subconjuntos de B. Prove que:
    (i) $(X \cup Y)f^{-1} = Xf^{-1} \cup Yf^{-1}$.
    (ii) $(X \cap Y)f^{-1} = Xf^{-1} \cap Yf^{-1}$.
    (iii) $(X \backslash Y)f^{-1} = Xf^{-1} \backslash Yf^{-1}$.

21. Sejam $f \subseteq A \times B$ e $g \subseteq B \times A$ relações, tais que $fg = 1_A$ e $gf = 1_B$. Prove que f e g são funções bijetoras e $f = g^{-1}$.

22. Sejam A e B conjuntos, A não vazio. Mostre que existe uma injeção $f : A \to B$ sse existe uma sobrejeção $g : B \to A$.

23. Seja $g : B \to C$ uma função. Mostre que g é injetora sse para todo conjunto A e funções $f_1, f_2 : A \to B$, se $f_1 g = f_2 g$ então $f_1 = f_2$. Enuncie e prove a caracterização análoga de funções sobrejetoras.

24. Sejam r e s relações simétricas sobre um conjunto A. Prove que se $rs \subseteq sr$, então $rs = sr$.

25. Ache duas relações de equivalência r e s sobre um conjunto A, tais que a relação rs não seja de equivalência.

26. Dê exemplos de relações r, s e t sobre um conjunto A, tais que:
    (i) r é reflexiva e simétrica mas não é transitiva,
    (ii) s é reflexiva e transitiva mas não é simétrica,
    (iii) t é simétrica e transitiva mas não é reflexiva.

27. Mostre que no enunciado da Proposição 2 a hipótese $gg^{-1} \subseteq ff^{-1}$ é necessária, isto é, ache funções $g : A \to B$ e $f : A \to C$, g sobrejetora, tais que não exista função $h : B \to C$, para qual $f = gh$.

28. Seja $f : A \to B$ uma função. Mostre que existem um conjunto C e funções $g : A \to C$ e $h : C \to B$, tais que $f = gh$, g é sobrejetora e h é injetora. Em outras palavras, toda função $f : A \to B$ admite uma fatoração

$$A \xrightarrow{g} C \xrightarrow{h} B,$$

com g sobrejetora e h injetora. Mostre que esta fatoração e "única" no seguinte sentido: se

$$A \xrightarrow{g'} C' \xrightarrow{h'} B$$

for uma outra fatoração de f, com g' sobrejetora e h' injetora, então existe uma (única) bijeção $b : C \to C'$ tal que $gb = g'$ e $bh' = h$.
Sugestão: Coloque $C = A/ff^{-1}$ e use a Proposição 2.

29. Mostre que toda função $f : A \to B$ admite uma fatoração

$$A \xrightarrow{g} C \xrightarrow{h} B,$$

com g injetora e h sobrejetora. Mostre que esta fatoração não é "única" no sentido do exercício anterior.
Sugestão: Se A e B forem disjuntos, coloque $C = A \cup B$.

30. Seja A um conjunto e sejam a e b elementos de A. A transposição de a com b é a função $t : A \to A$, definida por:

$$xt = \begin{cases} x \text{ se } x \neq a \text{ e } x \neq b \\ b \text{ se } x = a \\ a \text{ se } x = b \end{cases} \qquad (x \in A).$$

Prove que $tt = 1_A$ e conclua que t é uma bijeção.

31. (*Princípio da casa do pombo*, vide Capítulo C.V) — Se n for um número natural, $\mathbf{n}$ denotará o conjunto

$$\mathbf{n} = \{0, 1, ..., n - 1\}.$$

Observe que $\mathbf{0} = \varnothing$ e que $n \leq m$ sse $\mathbf{n} \subseteq \mathbf{m}$. Sejam n e m naturais, e $f : \mathbf{n} \to \mathbf{m}$ uma função. Prove que se f for injetora, então $n \leq m$.
Sugestão: Use indução sobre m. Seja $k = (n - 1)f$ e seja $t : \mathbf{m} \to \mathbf{m}$ a transposição de k com $m - 1$. A função $g = ft$ é injetora. Note que $(n - 1)g = m - 1$ e aplique a hipótese da indução.

32. Sejam n e m naturais e $f : \mathbf{n} \to \mathbf{m}$ uma função. Prove que:
(i) se f for bijetora então $n = m$.
(ii) se $n = m$ então f é injetora sse f é sobrejetora.

33. Um conjunto A é *finito* se existir um número natural n e uma bijeção $f : \mathbf{n} \to A$. Mostre que se A for um conjunto finito então existe um único número natural n para qual existem bijeções $f : \mathbf{n} \to A$. Este número é chamado de *cardinalidade* de A e é denotado por *card* A.

34. Seja A um conjunto finito e $f : A \to A$ uma função. Mostre que f é injetora sse f é sobrejetora.

35. Um conjunto é *infinito* se ele não for finito. Mostre que o conjunto $\mathbb{N}$ dos números naturais não é finito. Usando o axioma da escolha mostre que se A for um conjunto infinito, então existe uma injeção $f : \mathbb{N} \to A$. Prove que um conjunto A é infinito sse existe uma injeção $f : A \to A$ que não é sobrejetora.

36. Dados conjuntos A e B, o conjunto de todas as funções com domínio B e co-domínio A é denotado por A^B, isto é

$$A^B = \{f \mid f : B \to A\}.$$

Ache bijeções entre os seguintes pares de conjuntos, onde A, B e C são conjuntos dados:

(i) $A \times A$ e A^2.
(ii) $\mathfrak{p}(A)$ e $\mathbf{2}^A$.
(iii) $(A \times B)^C$ e $A^C \times B^C$.
(iv) $(A^B)^C$ e $A^{B \times C}$.

37. Uma *permutação* de um conjunto A é uma bijeção $f : A \to A$. Denotamos por *Per* A o conjunto de todas as permutações de A. Para um conjunto A e um natural p, $\binom{A}{p}$ denota o conjunto de todos os subconjuntos de cardinalidade p de A.
Sejam p, n e m naturais, tais que $m = n + 1$. Ache bijeções entre os seguintes pares de conjuntos:

(i) $\mathbf{p}^m$ e $\mathbf{p} \times \mathbf{p}^n$.
(ii) *Per* $\mathbf{m}$ e $\mathbf{m} \times$ *Per* $\mathbf{n}$.
(iii) $\binom{\mathbf{m}}{p}$ e $\binom{\mathbf{n}}{p} \cup \binom{\mathbf{n}}{p-1}$, quando $p \geq 1$.

38. Sejam A e B conjuntos finitos e seja p um natural. Usando os Exercícios 36 e 37, mostre que:

(i) $card\ A^B = (card\ A)^{card\ B}$.
(ii) $card\ \mathfrak{p}(A) = 2^{card\ A}$.
(iii) $card\ (Per\ A) = (card\ A)!$.

(iv) se $p \leq card\, A$ então $card \binom{A}{p} = \binom{card\, A}{p}$, onde, para naturais $n \leq m$, $\binom{m}{n}$ denota o coeficiente binomial dado por:

$$\binom{m}{n} = \frac{m!}{n!\,(m-n)!}.$$

39. (*Hall*) — Sejam A e B conjuntos finitos. Mostre que uma relação $r \subseteq A \times B$ contém uma função injetora sse para todo subconjunto S de A $card\ Sr \geq card\ S$.
Sugestão: Use o Teorema de Hall, demonstrado no Capítulo C. III.
40. (*Banach*) — Dados conjuntos A e B, bem como funções $f : A \rightarrow B$ e $g : B \rightarrow A$, mostre que existem conjuntos S, T, X e Y tais que:

$A = S \cup T$, $\quad S \cap T = \emptyset$, $\quad B = X \cup Y$, $\quad X \cap Y = \emptyset$,
$Sf = X$ e $Yg = T$.

Sugestão: Defina uma função $h : \mathfrak{p}(A) \rightarrow \mathfrak{p}(A)$, colocando, para $V \subseteq A$, $Vh = A \backslash (B \backslash Vf)g$. Seja $\mathcal{F} = \{V \subseteq A \mid Vh \subseteq V\}$. A coleção $\mathcal{F}$ não é vazia, pois $A \in \mathcal{F}$. Seja $S = \bigcap_{V \in \mathcal{F}} V$. Se $V \subseteq W \subseteq A$, então $Vh \subseteq Wh$. Segue que $\mathcal{F}$ é fechada sob intersecção, bem como, se $V \in \mathcal{F}$ então $Vh \in \mathcal{F}$. Assim, tanto S como Sh pertencem a $\mathcal{F}$. Segue que $Sh = S$. Agora basta colocar $X = Sf$, $T = A \backslash S$ e $Y = B \backslash X$.
41. (*Schröder-Bernstein*) — Sejam $f : A \rightarrow B$ e $g : B \rightarrow A$ funções injetoras. Mostre que existe uma bijeção $h : A \rightarrow B$.
Sugestão: Use o Exercício 40. Alternativamente, defina $S_0 = A \backslash Bg$ e $S_{n+1} = S_n fg$, para todo $n \geq 0$. Sejam $S = \bigcup_{n \in \mathbb{N}} S_n$ e $X = Sf$. Prove que $(B \backslash X)g = A \backslash S$.
42. Seja $f : M_1 \rightarrow M_2$ um morfismo de monóides. Mostre que se S for um submonóide de M_1 então Sf é um submonóide de M_2. Mostre também que se T for um submonóide de M_2 então Tf^{-1} é um submonóide de M_1.
43. Monóides M_1 e M_2 são *isomorfos*, escreve-se $M_1 \simeq M_2$, se existir um isomorfismo de M_1 para M_2. Seja A um conjunto, e seja M_1 (M_2) o monóide que consiste do conjunto $\mathfrak{p}(A)$, munido da operação de união (intersecção). Mostre que $M_1 \simeq M_2$.

44. O conjunto $\mathbb{N}$ dos números naturais, munido da operação de soma é um monóide. Este monóide será também denotado por $\mathbb{N}$. Seja Σ um conjunto não vazio. Prove que a função comprimento $|\,| : \Sigma^* \to \mathbb{N}$ é um epimorfismo que é injetor sse Σ é unitário. Conclua que $\mathbb{N}$ é isomorfo a um monóide livre gerado por um único elemento.

45. Seja M um monóide e a um elemento de M. Mostre que existe um único morfismo $f : \mathbb{N} \to M$, tal que $1f = a$.

46. Um elemento z de um monóide M é um *zero à esquerda* (*à direita*) se para todo m em M $zm = z$ ($mz = z$). Um elemento z de M é um *zero* se ele for tanto um zero à esquerda como um zero à direita, isto é, para todo m em M, $mz = zm = z$. Mostre que um monoide tem no máximo um zero. Mostre também que se z_e for um zero à esquerda em M e z_d for um zero à direita em M, então $z_e = z_d$, e este elemento é o único zero de M.

47. Mostre que todo monóide M satisfaz exatamente uma das quatro afirmações seguintes:
    (i) M não tem zeros à direita nem zeros à esquerda.
    (ii) M não tem zeros à direita mas tem um ou mais zeros à esquerda.
    (iii) M tem um ou mais zeros à direita mas não tem zeros à esquerda.
    (iv) M tem um único zero e não tem outros zeros à esquerda nem à direita.

    Dê exemplos de monóides satisfazendo cada uma destas quatro afirmações.

48. Seja A um conjunto com pelo menos dois elementos. Classifique os monóides *Rel A* e *Fun A* de acordo com as afirmações do Exercício 47. Caracterize os zeros de cada tipo nos dois casos.

49. Sejam M_1 e M_2 monóides. O *produto direto* de M_1 e M_2 consiste do conjunto $M_1 \times M_2$, munido da seguinte operação: para todo $m_1, m'_1 \in M_1$ e $m_2, m'_2 \in M_2$ $(m_1, m_2)(m'_1, m'_2) = (m_1m'_1, m_2m'_2)$. Mostre que
    (i) $M_1 \times M_2$ é um monóide.
    (ii) $M_1 \times M_2 \simeq M_2 \times M_1$.
    (iii) Existem epimorfismos $p_i : M_1 \times M_2 \to M_i$ para $i = 1, 2$.
    (iv) Se M_1 e M_2 forem, respectivamente, dos tipos (ii) e (iii), de acordo com a classificação do Exercício 47, então $M_1 \times M_2$ é do tipo (i).

50. Um *grupo* é um monóide M, em que para cada a em M existe b em M, tal que $ab = ba = 1$. Mostre que para todo conjunto A, *Per* A é um grupo. (Veja Exercício 37.)

51. Mostre que um monóide M é um grupo sse para todo a em M, $aM = Ma = M$.

52. Um elemento e de um monóide M é *idempotente* se $e^2 = e$. Seja $f : M_1 \to M_2$ um morfismo de monóides. Mostre que se e for idempotente em M_1 então ef é um idempotente em M_2. Mostre por meio de um exemplo que a recíproca não é verdadeira.

53. Mostre que uma função f em *Fun* A é idempotente sse a restrição $g : Af \to Af$ de f a Af é a função identidade 1_{Af}.

54. Um subconjunto T de um monóide M é um *monóide em* M sse $T^2 \subseteq T$ e T contém um elemento e, tal que para todo t em T, $et = te = t$. Note que um monóide T em M é um submonóide de M sse $1 \in T$. Mostre que se e for um idempotente em M, então eMe é um monóide em M, enquanto eM ou Me podem não ser monóides em M. Porém, $eMe = eM \cap Me$.

55. Mostre que um grupo tem um único elemento idempotente.

56. Seja r uma relação em *Rel* A, e seja t dado por:

$$t = 1_A \cup r \cup r^2 \cup \ldots \cup r^n \cup \ldots .$$

Mostre que $(a, b) \in t$ sse $a = b$, ou existem um natural $n \geq 1$ e $c_0, c_1, \ldots, c_n \in A$, tais que $a = c_0$, $c_n = b$ e $(c_i, c_{i+1}) \in r$, para $i = 0, 1, \ldots, n-1$. Mostre que t é a única relação minimal reflexiva e transitiva que contém r. A relação t é chamada de *fecho reflexivo e transitivo* de r. (Confronte com o Exercício B.III.25.) Observação: Note que t e r^* são entidades distintas! De fato, enquanto t é um elemento de *Rel* A, r^* (isto é $\{r\}^*$) é um subconjunto de *Rel* A. No entanto, $t = \bigcup_{s \in r^*} s$.

57. Seja M um monóide. Mostre que a intersecção de relações de congruência sobre M é uma relação de congruência sobre M.

58. Mostre que dada uma relação r sobre um monóide M, existe uma única relação de congruência minimal sobre M que contém r. Esta relação é chamada de *relação de congruência gerada por* r.

59. Nas condições do exercício anterior, seja r_c a relação de congruência gerada por r. Seja s a relação sobre M dada por:

$(m, m') \in s$ sse existem $u, v, x, y \in M$, tais que $m = uxv$, $m' = uyv$ e $(x, y) \in r \cup r^{-1}$. Seja t o fecho reflexivo e transitivo de s (vide Exercício 56). Mostre que $t = r_c$.

Sugestão: Mostre que t é uma relação de congruência que contêm r, logo $r_c \subseteq t$. Mostre que $s \subseteq r_c$, pois r_c é uma relação de congruência que contém r. Segue que o fecho transitivo, t, de s está contido no fecho transitivo, r_c, de r_c. Logo, $t \subseteq r_c$.

60. Sejam A, B e C subconjuntos de um monóide. Mostre que:
   (i) Se $A \subseteq B$ então $AC \subseteq BC$ e $CA \subseteq CB$.
   (ii) $A(B \cup C) = AB \cup AC$.
   (iii) $(A \cup B)C = AC \cup BC$.
   (iv) $A(B \cap C) \subseteq AB \cap AC$.
   (v) $(A \cap B)C \subseteq AC \cap BC$.
   (vi) Se $A \subseteq B$ então $A^* \subseteq B^*$.
   (vii) $(A^*)^* = A^*$.

61. Seja $f : M_1 \to M_2$ um morfismo de monóides, e sejam A e B subconjuntos de M_1. Mostre que:
   (i) $(AB)f = (Af)(Bf)$.
   (ii) $A^*f = (Af)^*$.

62. Seja A um subconjunto do monóide M. Mostre que existem um monóide livre Σ^* e um morfismo $f : \Sigma^* \to M$, tais que $\Sigma f = A$ e $\Sigma^* f = A^*$.

63. Sejam A e B subconjuntos do monóide livre Σ^*, tais que $\Sigma = A \cup B$. Mostre que $\Sigma^* = A^*(BA^*)^*$.

64. Sejam A e B subconjuntos do monóide livre Σ^*. Mostre que:
   (i) $A(BA)^* = (AB)^*A$.
   (ii) $(A \cup B)^* = A^*(BA^*)^*$.
   (iii) $A^*(BA^*)^* = (B^*A)^*B^*$.

65. Sejam s e t palavras em Σ^*. Mostre que $st = ts$ sse existem naturais m e n e uma palavra x em Σ^*, tais que $s = x^m$ e $t = x^n$.

66. Sejam A e B subconjuntos de monóide livre Σ^*. Definimos:

$$A^{-1}B = \{t \in \Sigma^* \mid \text{existe } s \in A \text{ tal que } st \in B\},$$
$$\text{e} \quad AB^{-1} = \{s \in \Sigma^* \mid \text{existe } t \in B \text{ tal que } st \in A\}.$$

Mostre que para todo $A, B, C \subseteq \Sigma^*$,
   (i) $(AC^{-1})B^{-1} = A(BC)^{-1}$.
   (ii) $(A^{-1}B)C^{-1} = A^{-1}(BC^{-1})$.
   (iii) $(AB)^{-1}C = B^{-1}(A^{-1}C)$.

67. Seja Σ^* um monóide livre. A função *reversão* $\rho : \Sigma^* \to \Sigma^*$ é definida por: $1\rho = 1$ e $(s\sigma)\rho = \sigma(s\rho)$ para todo $s \in \Sigma^*$ e $\sigma \in \Sigma$. A imagem de $s \in \Sigma^*$ por ρ é chamada de *reverso* de s. Sendo $s, t \in \Sigma^*$ e $A, B \subseteq \Sigma^*$, mostre que:
   (i) $s\rho\rho = s$.
   (ii) $(st)\rho = (t\rho)(s\rho)$.
   (iii) $(AB)\rho = (B\rho)(A\rho)$.
   (iv) $A^*\rho = (A\rho)^*$.
   (v) $(A^{-1}B)\rho = B\rho(A\rho)^{-1}$ e $(AB^{-1})\rho = (B\rho)^{-1}(A\rho)$:
   (Vide Exercício 66).

68. Um subconjunto A de Σ^* é um *prefixo* se para todo s em A, o único segmento inicial de s que pertence a A é o próprio s. Em símbolos, para todo $s, t \in \Sigma^*$, se $s, st \in A$, então $t = 1$. Mostre que as afirmações abaixo são equivalentes (vide Exercício 66 para notação):
   (i) A é um prefixo.
   (ii) Para todo $s_1, s_2, t_1, t_2 \in \Sigma^*$, se $s_1t_1 = s_2t_2$ e $s_1, s_2 \in A$, entao $s_1 = s_2$ e $t_1 = t_2$.
   (iii) Para todo $s, t_1, t_2 \in \Sigma^*$, se $st_1, st_2 \in A$, então $t_1t_2 = 1$ ou $s \notin A$.
   (iv) $s^{-1}A = 1$ para todo $s \in A$.
   (v) $A = \varnothing$ ou $A^{-1}A = 1$.

69. Sejam A, B e C subconjuntos de Σ^*. Mostre que (confronte com o Exercício 60):
   (i) Se $A \cup B$ for um prefixo, então $(A \cap B)C = AC \cap BC$.
   (ii) Se A for um prefixo, então $A(B \cap C) = AB \cap AC$.
   (iii) Se A for um prefixo, então[2] $A(B \oplus C) = AB \oplus AC$.

70. Um subconjunto A de Σ^* é um *sufixo* se o reverso $A\rho$ de A for um prefixo. Enuncie e demonstre os análogos dos Exercícios 68 e 69, substituindo prefixos por sufixos.

71. Seja A um submonóide do monóide livre Σ^*. Um subconjunto B de A é um *gerador* de A se $B^* = A$. Mostre que

$$(A\backslash 1)\backslash(A\backslash 1)^2$$

é o único gerador minimal de A.

---

(2) Para conjuntos A e B, $A \oplus B$ denota a diferença simétrica de A e B, isto é, $A \oplus B = A\backslash B \cup B\backslash A$.

NOTAS BIBLIOGRÁFICAS

Os conceitos e resultados deste capítulo fazem parte do folclore da Matemática. Para um estudo mais detalhado de relações e funções recomendamos os livros de Halmos [47] ou de MacLane e Birkhoff [72]. O leitor interessado encontrará um tratamento detalhado de monóides no livro de Clifford e Preston [15].