UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS BLUMENAU
LICENCIATURA EM MATEMÁTICA

Jhoni Conzatti

Semigrupos e monoides algébricos: uma aplicação na teoria da computação

Blumenau
2021

Jhoni Conzatti

Semigrupos e monoides algébricos: uma aplicação na teoria da computação

Trabalho de Conclusão de Curso de Graduação em Licenciatura em Matemática do Campus Blumenau da Universidade Federal de Santa Catarina para a obtenção do título de Licenciado(a) em Matemática.
Orientador: Prof. Rafael Aleixo de Carvalho, Dr.

Blumenau
2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Conzatti, Jhoni
Semigrupos e monoides algébricos : uma aplicação na teoria da computação / Jhoni Conzatti ; orientador, Rafael Aleixo de Carvalho, 2021.
200 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Blumenau, Graduação em Matemática, Blumenau, 2021.

Inclui referências.

1. Matemática. 2. Semigrupos. 3. Monoides. 4. Linguagens. 5. Autômatos. I. Carvalho, Rafael Aleixo de. II. Universidade Federal de Santa Catarina. Graduação em Matemática. III. Título.

Jhoni Conzatti

Semigrupos e monoides algébricos : uma aplicação na teoria da computação

Este Trabalho Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciado(a) em Matemática e aprovado em sua forma final pelo Curso de Licenciatura em Matemática.

Blumenau, 7 de Maio de 2021.

Documento assinado digitalmente

Julio Faria Correa
Data: 24/05/2021 14:06:55-0300
CPF: 045.818.289-37
Verifique as assinaturas em https://v.ufsc.br

Prof. Júlio Faria Corrêa, Dr(a).
Coordenador do Curso

Banca Examinadora:

Documento assinado digitalmente

Rafael Aleixo de Carvalho
Data: 24/05/2021 10:08:57-0300
CPF: 302.494.178-98
Verifique as assinaturas em https://v.ufsc.br

Prof. Rafael Aleixo de Carvalho, Dr.
Orientador
Universidade Federal de Santa Catarina – UFSC

Prof. Felipe Vieira, Dr.
Avaliador
Universidade Federal de Santa Catarina – UFSC

Prof. Bruno Tadeu Costa, Dr.
Avaliador
Universidade Federal de Santa Catarina – UFSC

Este trabalho é dedicado á minha esposa Thaís de Lima Silva.

AGRADECIMENTOS

Agradeço aos meus pais, Leontina Pisa Conzatti e Vilmar Conzatti (*in memonian*) e aos meus irmãos, Maicon Conzatti e Aline Conzatti que sempre me apoiaram e incentivaram a seguir estudando.

À minha esposa, Thaís de Lima Silva, por compartilhar sua vida comigo, ficando ao meu lado durante toda a graduação, me motivando nos momentos difíceis e comemorando os momentos de felicidade.

Ao meu orientador, professor Rafael Aleixo de Carvalho, por contribuir imensamente para o desenvolvimento deste trabalho. As iniciações científicas que desenvolvemos juntos foram importantes para a elaboração do tema deste trabalho de conclusão de curso.

Ao corpo docente do curso de Licenciatura em Matemática da UFSC Blumenau, pelo excelente trabalho prestado para a formação dos novos professores e pesquisadores de Matemática.

Aos colegas de turma e aos amigos que fiz na universidade, que também fizeram parte da minha formação.

Por fim, agradeço a todos e todas que estiveram presentes durante a vida acadêmica.

"A Matemática é o alfabeto
com o qual Deus escreveu o Universo."
(GALILEI, 1564 - 1642)

RESUMO

O objetivo deste trabalho é aplicar a teoria de semigrupos e monoides algébricos à linguagens e autômatos da teoria da computação. Para tanto, primeiramente é feito um estudo sobre semigrupos e monoides algébricos, abordando os conceitos e teoremas fundamentais da teoria. Em seguida são apresentadas as definições e resultados fundamentais relacionados com os conceitos de linguagens e autômatos da teoria da computação. Usando, principalmente, o conceito de monoide de transformação completa e o teorema fundamental do homomorfismo para semigrupos e monoides, é possível caracterizar os semigrupos e monoides livres, que são linguagens sobre um dado alfabeto. Prova-se que todo semiautômato e autômato tem, respectivamente, um semigrupo ou monoide finito associado, bem como, dado um semigrupo ou monoide finito pode-se construir um semiautômato ou autômato. Por fim, é demonstrado um teorema que caracteriza linguagem regular partindo da ideia de congruência e classes de equivalência.

Palavras-chave: Semigrupos. Monoides. Linguagens. Autômatos.

ABSTRACT

The objective of this work is to apply the theory of algebraic semigroups and monoids to the languages and automata of computer theory. Therefore, first a study is made on semigroups and algebraic monoids, approaching the fundamental concepts and theorems of the theory. Then, are presented the definitions and fundamental results related to the concepts of languages and automata of the computer theory. Using mainly the concept of complete transformation monoid and the fundamental homomorphism theorem for semigroups and monoids, it is possible to characterize free semigroups and monoids, which are languages on a given alphabet. It is proven that every semiautomata and automata has an associated semigroup or monoid respectively, as well as, given a finite semigroup or monoid, a semiautomata or automata can be built. Finally, it is demonstrated a theorem that characterizes regular language starting from the idea of congruence and equivalence classes.

Keywords: Semigroups. Monoids. Languages. Autamatas.

LISTA DE FIGURAS

Figura 1 – Banda retangular $A \times B$ 60
Figura 2 – Subsemigrupo monogênico finito de S gerado por a 63
Figura 3 – Representação gráfica do subsemigrupo monogênico $\langle \alpha \rangle$ 68
Figura 4 – Esquema da Proposição 2.27 77
Figura 5 – Esquema do Teorema 2.4 88
Figura 6 – Diagrama das inclusões nas relações de *Green* . . 95
Figura 7 – Representação do funcionamento de uma porta automática 113
Figura 8 – Representação do funcionamento de uma porta automática com sensores que verificam temperatura corporal e uso de máscara facial 117
Figura 9 – Diagrama de estados do autômato M_1 121
Figura 10 – Diagrama de estados do autômato M_2 122
Figura 11 – Diagrama de estados do autômato M_3 124
Figura 12 – Diagrama de estados do autômato D_1 126
Figura 13 – Diagrama de estados do autômato D_2 126
Figura 14 – Diagrama de estados do autômato D_3 126
Figura 15 – Diagrama de estados do autômato N_1 128
Figura 16 – Computação da *string* 010110 em N_1 130
Figura 17 – Diagrama de estados do autômato N_E 132
Figura 18 – Diagrama de estados do autômato N_2 134
Figura 19 – Diagrama de estados do autômato D_4 136
Figura 20 – Diagrama de estados do autômato D_4 adaptado . 137
Figura 21 – Esquema do diagrama de estados do autômato N_1 140
Figura 22 – Esquema do diagrama de estados do autômato N_2 140
Figura 23 – Esquema do diagrama de estados do autômato N_U 141
Figura 24 – Esquema do diagrama de estados do autômato N_C 143

Figura 25 – Esquema do diagrama de estados do autômato N_E 145
Figura 26 – Diagrama de estados do autômato G_1 148
Figura 27 – Diagrama de estados do autômato determinístico D_5 152
Figura 28 – Diagrama de estados do autômato não determinístico generalizado G_2 equivalente à D_5 153
Figura 29 – Diagrama de estados do autômato não determinístico N_3 154
Figura 30 – Diagrama de estados do autômato não determinístico N_4 154
Figura 31 – Diagrama de estados do autômato não determinístico N_5 155
Figura 32 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular a 155
Figura 33 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular b 156
Figura 34 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular $a \cup b$ 156
Figura 35 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular $(a \cup b)^*$ 157
Figura 36 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular ab 157
Figura 37 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular aba 158

Figura 38 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular $(a \cup b)^* aba$ 159
Figura 39 – Diagrama de estados parcial de G contendo apenas os estados q_r, q_i e q_j com $R_1 = \delta(q_i, q_r)$, $R_2 = \delta(q_r, q_r)$, $R_3 = \delta(q_r, q_j)$, e $R_4 = \delta(q_i, q_j)$ 160
Figura 40 – Diagrama de estados parcial de $\mathrm{red}(G)$ 161
Figura 41 – Diagrama de estados do autômato $G_3 = \mathrm{red}(G_2)$. 164
Figura 42 – Diagrama de estados do autômato $\mathrm{red}(G_3)$ 164
Figura 43 – Diagrama de estados do semiautômato D 182
Figura 44 – Diagrama de estados do semiautômato S 183
Figura 45 – Diagrama de estados do autômato A 187
Figura 46 – Diagrama de estados do semiautômato S_W 191
Figura 47 – Diagrama de estados do autômato A_W 192
Figura 48 – Diagrama de estados do autômato B 195

LISTA DE TABELAS

Tabela 1 – Tabela de Cayley do semigrupo S. 37
Tabela 2 – Tabela de Cayley do monoide W 46
Tabela 3 – Tabela de Cayley do monoide M 53
Tabela 4 – Tabela de Cayley do monoide T 53
Tabela 5 – Tabela de Cayley do grupo cíclico K_α 68
Tabela 6 – Tabela de transição do semiautômato P 115
Tabela 7 – Tabela de transição do semiautômato N 118
Tabela 8 – Tabela de transição do autômato determinístico M_3 124
Tabela 9 – Tabela de transição do autômato N_1 128
Tabela 10 – Tabela de transição do autômato não determinístico N_2 134
Tabela 11 – Tabela de transição do autômato D_4 135
Tabela 12 – Tabela de transição do autômato G_1 148
Tabela 13 – Tabela de transição do autômato determinístico D_5 152
Tabela 14 – Tabela de transição do autômato não determinístico generalizado G_2 152
Tabela 15 – Função transição de red(G_2) com $q_r = 1$ 163
Tabela 16 – Tabela da função σ_0 175
Tabela 17 – Tabela de Cayley do semigrupo monogênico $M(4, 3)$ 181
Tabela 18 – Tabela de Cayley do monoide quociente Σ^*/ρ . . 188
Tabela 19 – Tabela de Cayley do monoide do autômato determinístico A 189
Tabela 20 – Tabela de Cayley do monoide $\langle\delta\rangle^1$ 191

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais (não considera o elemento zero)
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
$\mathcal{P}(S)$	Conjunto de todos os subconjuntos do conjunto S
$\mathcal{T}_X$	Conjunto de todas as funções em um conjunto X
$\mathcal{B}_X$	Conjunto de todas as relações binárias em um conjunto X
$\mathcal{P}_X$	Conjunto de todas as transformações parciais em um conjunto X

SUMÁRIO

1 INTRODUÇÃO 25
2 ÁLGEBRA ABSTRATA: SEMIGRUPOS E MONOIDES 29
2.1 SEMIGRUPOS E MONOIDES 30
2.2 IDEAIS E IDEAIS PRINCIPAIS 37
2.3 SUBSEMIGRUPOS E SUBMONOIDES 46
2.4 GRUPOS E SUBGRUPOS 48
2.5 HOMOMORFISMOS E ISOMORFISMOS 52
2.6 BANDA RETANGULAR 57
2.7 SEMIGRUPO MONOGÊNICO 60
2.8 RELAÇÕES BINÁRIAS 71
2.9 RELAÇÕES DE EQUIVALÊNCIA E SEMIGRUPO QUOCIENTE 79
2.10 RELAÇÕES DE GREEN E SEMIGRUPOS REGULARES 89
3 TEORIA DA COMPUTAÇÃO: LINGUAGENS E AUTÔMATOS 105
3.1 *STRINGS* E LINGUAGENS 106
3.2 SEMIAUTÔMATO 112
3.2.1 Semiautômato Determinístico 113
3.2.2 Semiautômato Não Determinístico 115
3.3 AUTÔMATO 119
3.3.1 Autômato Determinístico 120
3.3.2 Autômato Não Determinístico 127
3.3.3 Autômatos Equivalentes 132
3.4 EXPRESSÕES REGULARES 145
3.4.1 Autômato não determinístico generalizado 147
3.4.2 Relação entre expressão regular e linguagem regular 153

4 SEMIGRUPOS E MONOIDES APLICADOS A LINGUAGENS E AUTÔMATOS 167
4.1 SEMIGRUPOS E MONOIDES LIVRES 167
4.2 SEMIGRUPO DE SEMIAUTÔMATO 177
4.3 SEMIGRUPO DE AUTÔMATO 184
4.4 LINGUAGENS REGULARES 192
5 CONCLUSÃO 197
REFERÊNCIAS 199

1 INTRODUÇÃO

A motivação para o desenvolvimento desse trabalho surgiu durante o desenvolvimento do trabalho de iniciação científica de título "Autômatos, Linguagens regulares e Linguagens livres de contexto". Observamos que as linguagens e os autômatos estudados na Teoria da Computação poderiam estar relacionados com alguma estrutura algébrica. Pensamos isso, pois uma linguagem munida da operação de concatenação de *strings* obedece o fechamento, a associatividade e a existência do elemento identidade. Além disso, as linguagens regulares, que formam o conjunto das linguagens reconhecidas por autômatos, são fechadas para as operações binárias concatenação e união. Buscamos alguma generalização no campo da Álgebra Abstrata. Notamos que tal generalização poderia ser alcançada estudando semigrupos e monoides algébricos.

Semigrupo é uma estrutura algébrica formada por um conjunto munido de uma operação binária fechada e associativa. Monoide é um semigrupo com elemento identidade. Eles têm aplicações em outros campos do conhecimento, como na Biologia e na Sociologia como pode ser visto em Lidl e Pilz [6] e, além disso, os monoides e os semigrupos também são comumente usados na ciência da computação, tanto em seus aspectos fundamentais quanto na programação prática. As linguagens, isto é, o conjunto de *strings* construídas a partir de um determinado conjunto de caracteres é um semigrupo livre. Quando consideremos a *strings* vazia um elemento de um semigrupo livre, então o chamamos de monoide livre.

Obviamente, tanto a teoria de semigrupos e monoides algébricos quanto a teoria da computação são extensas, logo não temos a pretensão de esgotar todo o conteúdo com o desenvolvimento desse trabalho. Assim, este trabalho de conclusão de curso tem um objetivo

principal bem definido e delimitado: aplicar a teoria de semigrupos e monoides algébricos à linguagens e autômatos da teoria da computação. Para tanto buscamos atingir os seguintes objetivos específicos: a) enunciar definições e resultados fundamentais a teoria de semigrupos e monoides algébricos; e, b) abordar definições e resultados referentes à linguagens e autômatos da teoria da computação.

O desenvolvimento do texto desse trabalho é dividido em três capítulos organizados para atingir os objetivos propostos. No Capítulo 2 apresentamos os conceitos de semigrupo e de monoide. Desenvolvemos a teoria a partir dos textos de Howie [5], G. [3], Clifford e Preston [1] e Domingues e Iezzi [2]. Os semigrupos podem ser vistos como uma generalização da teoria de grupos algébricos, por isso, nesse capítulo, comparamos os resultados obtidos para os semigrupos com resultados semelhantes para a teoria de grupos visto na disciplina da Álgebra. As imagens e esquemas do Capítulo 2 foram elaboradas com o *software online* `Math.io` [7].

O Capítulo 3 apresenta os conceitos de linguagem, linguagem regular e os modelos computacionais semiautômatos e autômatos. A teoria é baseada principalmente nos textos de Sipser [9] e Sakarovitch [8]. Esses modelos computacionais possuem representação gráfica chamada de diagrama de estados que foram elaborados para este trabalho com o uso do *software online* `Finite State Machine Designer` [10].

O Capítulo 4 é o último do desenvolvimento deste trabalho, cujo texto é baseado em Ginzburg [4], Lidl e Pilz [6] e Sakarovitch [8]. Nesse capítulo final buscamos uma relação entre os conteúdos abordados nos dois capítulos anteriores. Usando as ideias de monoide de transformação completa e o teorema fundamental do homomorfismo para semigrupos e monoides, conseguimos caracterizar os semigrupos e monoides livres, que são linguagens sobre um dado alfabeto. Além disso, mostramos que todo semiautômato e autômato tem um

semigrupo ou monoide associado, bem como, dado um semigrupo ou monoide finito podemos construir um semiautômato ou autômato. Por fim, demonstramos um teorema que caracteriza linguagem regular partindo da ideia de congruência e classes de equivalência.

2 ÁLGEBRA ABSTRATA: SEMIGRUPOS E MONOIDES

Neste capítulo são apresentadas algumas definições, exemplos e resultados acerca dos conceitos de *semigrupos* e *monoides* algébricos. Ao longo do texto, quando oportuno, fazemos comparações com ideias que são abordadas na teoria de grupos algébricos cuja definição pode ser encontrada em Domingues e Iezzi [2, p. 138-139].

Na Seção 2.1 apresentamos as definições para semigrupos e monoides algébricos. Na Seção 2.2 são apresentados os *ideais* e *ideais principais*. Na Seção 2.3 definimos os *subsemigrupos* e *submonoides*.

Na Seção 2.4 abordamos os *grupos* e *subgrupos*. Como veremos, todo grupo é também um semigrupo, mas nem todo semigrupo é um grupo. Nessa seção, demonstramos uma condição necessária e suficiente para que um semigrupo seja um grupo e caracterizamos os *subgrupos de semigrupos*. Na Seção 2.5 apresentamos *homomorfismos* e *isomorfismos*, bem como os *Teoremas de Cayley* para semigrupos e monoides.

Nas seções 2.6 e 2.7 são apresentados, respectivamente, dois semigrupos com algumas propriedades interessantes: a *banda retangular* e o *semigrupo monogênico*. Em seguida, nas seções 2.8 e 2.9 abordamos, respectivamente, *relações binárias* e *relações de equivalência*. Ainda na Seção 2.9, partindo da definição de relações de equivalência e *partições*, definimos o *semigrupo quociente* e demonstramos o *Teorema Fundamental do Homomorfismo para Semigrupos*.

Finalmente, na última Seção 2.10, retomamos o assunto de ideais principais (apresentado na Seção 2.2) para definirmos as chamadas *relações de Green* e os *semigrupos regulares*.

2.1 SEMIGRUPOS E MONOIDES

Definição 2.1. Um *semigrupo* é um par $(S, \cdot)$ em que S é um conjunto não vazio e $\cdot$ é uma operação binária fechada e associativa em S. Isto é, para todo $a, b, c \in S$ temos

(i) (fechamento) $a \cdot b \in S$

(ii) (associatividade) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Quando a operação binária é clara no contexto apresentado, denotamos o semigrupo $(S, \cdot)$ por S simplesmente. Neste caso, a operação dos elementos a e b do semigrupo S é denotada por ab.

Como todo semigrupo é por definição associativo, então para todo $a, b, c \in S$, com S um semigrupo qualquer, podemos denotar $a(bc) = (ab)c = abc$ sem que ocorram ambiguidades. Indutivamente, também verifica-se que não há problemas em denotar

$$\underbrace{aaa\ldots a}_{n \text{ vezes}}$$

por a^n com $n \in \mathbb{N}$.

Observação 2.1. Não consideraremos o número zero um elemento do conjunto dos números naturais $\mathbb{N}$. Assim, neste momento, evitamos um problema com a notação a^n enunciada no parágrafo anterior uma vez que a^0 não estaria definido.

Exemplo 2.1. (i) Os conjuntos dos números naturais ($\mathbb{N}$), inteiros ($\mathbb{Z}$), racionais ($\mathbb{Q}$) e reais ($\mathbb{R}$) munidos da operação binária de soma ($+$) são todos semigrupos.

(ii) Os conjuntos dos números naturais ($\mathbb{N}$), inteiros ($\mathbb{Z}$), racionais ($\mathbb{Q}$) e reais ($\mathbb{R}$) munidos da operação binária de multiplicação ($\cdot$) são todos semigrupos.

(iii) Todo grupo (veja a Definição 2.16) é também um semigrupo.

(iv) O conjunto das matrizes quadradas de ordem n sobre o corpo dos números reais $\mathbb{R}$, denotado por $\mathcal{M}_n(\mathbb{R})$, com a operação binária de multiplicação matricial $(\cdot)$ é um semigrupo.

(v) Outro exemplo de semigrupo, extraído de Howie [5, p. 3], pode ser obtido do intervalo $I = [0, 1] \subset \mathbb{R}$ munido da operação binária $\cdot : I \times I \longrightarrow I$ em que para todo $a, b \in I$, $a \cdot b = \min(a, b)$.

(vi) Se S e T são semigrupos, então o produto cartesiano $S \times T$ forma um novo semigrupo com a operação binária $\cdot : (S \times T) \times (S \times T) \longrightarrow S \times T$ dada por $(s_1, t_1) \cdot (s_2, t_2) = (s_1 s_2, t_1 t_2)$. Tal operação binária é conhecida como *produto direto* de S e T.

Definição 2.2. Seja S um semigrupo. Se para todo $a, b, c \in S$,

(i) $ac = bc \Rightarrow a = b$, então dizemos que S é um semigrupo *cancelativo à direita.*

(ii) $ca = cb \Rightarrow a = b$, então dizemos que S é um semigrupo *cancelativo à esquerda.*

(iii) Se um semigrupo S é simultaneamente cancelativo a direita e a esquerda, então dizemos simplesmente que S é *cancelativo.*

Exemplo 2.2. (i) Os semigrupos $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ e $(\mathbb{R}, \cdot)$ dos itens (i) e (ii) do Exemplo 2.1 são todos cancelativos.

(ii) Todo grupo, por consequência da existência do elemento inverso, é um semigrupo cancelativo.

(iii) O semigrupo $(\mathcal{M}_n(\mathbb{R}), \cdot)$ do item (iv) do Exemplo 2.1 não é cancelativo.

(iv) O semigrupo $(I, \cdot)$ do item (v) do Exemplo 2.1 não é cancelativo.

Definição 2.3. Se S é um semigrupo e para todo $a, b \in S$ temos $ab = ba$, então dizemos que S é um semigrupo *comutativo*.

Exemplo 2.3. (i) Os semigrupos $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ e $(\mathbb{R}, \cdot)$ dos itens (i) e (ii) do Exemplo 2.1 são todos comutativos.

(ii) Todo grupo abeliano é um semigrupo comutativo.

(iii) O semigrupo $(\mathcal{M}_n(\mathbb{R}), \cdot)$ do item (iv) do Exemplo 2.1 não é comutativo.

(iv) O semigrupo $(I, \cdot)$ do item (v) do Exemplo 2.1 é comutativo.

Definição 2.4. Seja S um semigrupo. Se existe $e \in S$ tal que $e^2 = e$, então dizemos que e é um elemento *idempotente* de S. Denotamos por

$$E(S) = \{e \in S\,;\ e^2 = e\}$$

o conjunto dos elementos idempotentes de S. Se $E(S) = S$, ou seja, se todo elemento de S é idempotente, então dizemos que S é uma *banda*.

Exemplo 2.4. (i) O elemento 0 dos semigrupos $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$ do item (i) do Exemplo 2.1 é idempotente.

(ii) O elemento 1 do semigrupo $(\mathbb{N}, \cdot)$ do item (ii) do Exemplo 2.1 é idempotente.

(iii) Os elementos 0 e 1 dos semigrupos $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ e $(\mathbb{R}, \cdot)$ do item (ii) do Exemplo 2.1 são idempotentes.

(iv) A identidade de um grupo é um elemento idempotente.

(v) A *matriz identidade* I_n e a *matriz nula* O_n do semigrupo $(\mathcal{M}_n(\mathbb{R}), \cdot)$ do item (iv) do Exemplo 2.1 são elementos idempotentes.

(vi) Todos os elementos do semigrupo $(I, \cdot)$ do item (v) do Exemplo 2.1 são idempotentes, ou seja, $(I, \cdot)$ é uma banda.

(vii) O semigrupo $(\mathbb{N}, +)$ do item (i) do Exemplo 2.1 não possui elementos idempotentes.

Definição 2.5. Um *monoide* é um semigrupo M em que existe o elemento $1 \in M$, tal que para todo $a \in M$, tem-se $a1 = 1a = a$. Neste caso o elemento $1 \in M$ é chamado de *identidade* de M.

Exemplo 2.5. (i) Os semigrupos $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$ do item (i) do Exemplo 2.1 são monoides com identidade igual a 0.

(ii) Os semigrupos $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ e $(\mathbb{R}, \cdot)$ do item (ii) do Exemplo 2.1 são monoides com identidade igual a 1.

(iii) Todo grupo é um monoide com identidade igual a identidade do grupo.

(iv) O semigrupo $(\mathcal{M}_n(\mathbb{R}), \cdot)$ do item (iv) do Exemplo 2.1 é um monoide com identidade igual a I_n.

(v) O semigrupo $(I, \cdot)$ do item (v) do Exemplo 2.1 é um monoide com identidade igual a 1.

(vi) O semigrupo $(\mathbb{N}, +)$ do item (i) do Exemplo 2.1 não é monoide.

Observação 2.2. Note que o elemento identidade de um monoide é sempre único. De fato, se e e f são identidades de um monoide, então temos que $ef = e$ (pois f é identidade) e, simultaneamente, temos que $ef = f$ (pois e é identidade), logo $e = ef = f$ e, portanto, $e = f$.

Observação 2.3. Se M é um monoide com elemento identidade igual a 1, então $1 \in E(M)$. Caso M seja cancelativo, então 1 é o único idempotente de M. De fato, tome $e \in E(M)$, então $e^2 = e \Rightarrow ee = e1$

e, por cancelamento, $e = 1$, ou seja, $E(M) = \{1\}$. Em particular, se M é um grupo, então $E(M) = \{1\}$.

Como vimos na Definição 2.5, um monoide é simplesmente um semigrupo com um elemento identidade. Assim, dado um semigrupo $(S, \cdot)$ qualquer, podemos adicionar ao conjunto S um novo elemento $1 \notin S$, tal que para todo $a \in S$, $1 \cdot a = a \cdot 1 = a$ e $1 \cdot 1 = 1$. Assim, o conjunto $S \cup \{1\}$ munido com a operação $\cdot$ é um monoide com identidade igual à 1. Deste modo, definimos o monoide S^1 da seguinte maneira.

Definição 2.6. Seja $(S, \cdot)$ um semigrupo qualquer. Tome $1 \notin S$ um elemento qualquer, tal que para todo $a \in S$, $1 \cdot a = a \cdot 1 = a$ e $1 \cdot 1 = 1$, então o monoide S^1 com a operação $\cdot$ de S é dado por

$$S^1 = \begin{cases} S, & \text{se } S \text{ é um monoide} \\ S \cup \{1\}, & \text{se } S \text{ não é um monoide} \end{cases} \tag{1}$$

Nesse caso nos referimos à S^1 como o *monoide obtido de S pela adição da identidade, se necessário.*

Observação 2.4. Note que, se S já é um monoide com identidade $e \in S$, então $S \cup \{1\}$ será um novo monoide com o elemento identidade 1. Neste caso, $e \neq 1$ e $1e = e1 = e$. Portanto $S^1 = S \neq S \cup \{1\}$.

Definição 2.7. Seja S um semigrupo com pelo menos dois elementos. Dizemos que $0 \in S$ é um elemento *nulo* ou *zero* do semigrupo S se, para todo $a \in S$, $a0 = 0a = 0$. Neste caso, se tal elemento existe, dizemos que S é um *semigrupo com zero.*

Exemplo 2.6. (i) Os semigrupos $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$ do item (i) do Exemplo 2.1 não são semigrupos com zero.

(ii) Os semigrupos $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ e $(\mathbb{R}, \cdot)$ do item (ii) do Exemplo 2.1 são semigrupos com zero e elemento nulo igual a 0.

(iii) O semigrupo $(\mathcal{M}_n(\mathbb{R}), \cdot)$ do item (iv) do Exemplo 2.1 é um semigrupo com zero e elemento nulo igual a O_n.

(iv) O semigrupo $(I, \cdot)$ do item (v) do Exemplo 2.1 é um semigrupo com zero e elemento nulo igual a 0.

(v) O semigrupo $(\mathbb{N}, \cdot)$ do item (ii) do Exemplo 2.1 não é semigrupo com zero.

Observação 2.5. Assim como o elemento identidade de um monoide, o elemento nulo de um semigrupo com zero também é único. De fato, se e e f são elementos nulos de um semigrupo com zero, então temos que $ef = e$ (pois e é um elemento nulo) e, simultaneamente, temos que $ef = f$ (pois f é um elemento nulo), logo $e = ef = f$ e, portanto, $e = f$.

Temos que um semigrupo com zero precisa ter, de acordo com a Definição 2.7, pelo menos dois elementos. Afinal, caso S tivesse apenas um zero, teríamos $S = \{e\}$ com $ee = e^2 = e$, então o único elemento de S não seria um zero e sim uma identidade. Neste caso, S seria um semigrupo (ou um monoide ou, ainda, um grupo) chamado de *semigrupo (ou monoide, ou grupo) trivial*.

Novamente, de modo análogo ao que ocorre com a Definição 2.6, dado um semigrupo $(S, \cdot)$ qualquer, podemos adicionar ao conjunto S um novo elemento $0 \notin S$, tal que para todo $a \in S$, $0 \cdot a = a \cdot 0 = 0$ e $0 \cdot 0 = 0$. Assim, o conjunto $S \cup \{0\}$ munido da operação $\cdot$ é um semigrupo com zero e elemento nulo igual à 0. Deste modo, definimos o semigrupo com zero S^0 da seguinte maneira.

Definição 2.8. Seja $(S, \cdot)$ um semigrupo qualquer. Tome $0 \notin S$ um elemento qualquer, tal que para todo $a \in S$, $0 \cdot a = a \cdot 0 = 0$ e $0 \cdot 0 = 0$,

então o semigrupo com zero S^0 com a operação $\cdot$ de S é dado por

$$S^0 = \begin{cases} S, & \text{se } S \text{ é um semigrupo com zero} \\ S \cup \{0\}, & \text{se } S \text{ não é um semigrupo com zero} \end{cases} \tag{2}$$

Nesse caso, nos referimos à S^0 como o *semigrupo com zero obtido de S pela adição do zero, se necessário.*

De acordo com Howie [5, p. 3, tradução livre],

> apesar da facilidade em adicionar identidade e zero à um semigrupo, não podemos reduzir completamente o estudo de semigrupos à monoides com zero, a adição de elementos extras pode sacrificar algumas propriedades importantes do semigrupo. Se, por exemplo, adicionarmos um zero a um semigrupo que é um grupo, obtemos um semigrupo que não é um grupo.

Definição 2.9. Seja S um semigrupo com zero com elemento zero, dado por 0. Dizemos que S é um *semigrupo nulo* se a operação entre quaisquer elementos de S resultar em zero, isto é, se para todo $a, b \in S$, $ab = 0$.

Definição 2.10. Seja S um semigrupo.

(i) Se para todo $a, b \in S$, $ab = a$, então dizemos que S é um *semigrupo nulo à esquerda.*

(ii) Se para todo $a, b \in S$, $ab = b$, então dizemos que S é um *semigrupo nulo à direita.*

Semigrupos com um número finito de elementos podem ser representados por uma *tabela de Cayley*: os elementos do semigrupo ficam dispostos na primeira coluna e na primeira linha da tabela, e os elementos internos da tabela são o resultado da operação do elemento da primeira coluna com o elemento da primeira linha respectivamente.

Exemplo 2.7. Seja $S = \{a, b, c\}$ um semigrupo em que $aa = a$, $ab = b$, $ac = c$, $ba = b$, $bb = b$, $bc = c$, $ca = c$, $cb = b$ e $cc = c$. Então, S pode ser representado com a tabela de Cayley exibida na Tabela 1. Note que, o semigrupo S é de fato um monoide não cancelativo e não comutativo com identidade igual a a.

Tabela 1 – Tabela de Cayley do semigrupo S.

	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

Dada uma tabela de Cayley, verificar a associatividade dos elementos pode ser um trabalho tedioso. A fim de facilitar um pouco este processo Clifford e Preston [1] descrevem um método, que foi apresentado por Dr. F. W. Light em 1949, para determinar se os elementos de uma tabela de Cayley obedecem a propriedade associativa, e são, portanto, elementos de um semigrupo. Tal procedimento recebe o nome de *teste de associatividade de Light* e pode ser consultado com detalhes na obra de Clifford e Preston [1, p. 7-8].

2.2 IDEAIS E IDEAIS PRINCIPAIS

Se A e B são subconjuntos de um semigrupo S, então definimos o conjunto

$$AB = \{ab; a \in A, b \in B\} \tag{3}$$

Assim se C é outro subconjunto qualquer de S, então temos que $A(BC) = (AB)C$. De fato,

$$\begin{aligned} A(BC) &= \{ax;\ a \in A,\ x \in BC\} \\ &= \{ax;\ a \in A, x \in \{bc;\ b \in B,\ c \in C\}\} \\ &= \{a(bc);\ a \in A,\ b \in B,\ c \in C\} \\ &= \{(ab)c;\ a \in A,\ b \in B,\ c \in C\} \\ &= \{yc;\ y \in \{ab; a \in A,\ b \in B\},\ c \in C\} \\ &= \{yc;\ y \in AB,\ c \in C\} \\ &= (AB)C \end{aligned}$$

Logo, podemos escrever ABC no lugar de $A(BC)$ ou $(AB)C$ sem que ocorram ambiguidades, e, além disso, segue que o conjunto de todos os subconjuntos do semigrupo S, denotado por $\mathcal{P}(S)$, com a operação binária dada pela equação (3) é um monoide com identidade igual ao conjunto vazio $\emptyset$.

Ademais, denotamos

$$AA = \{ab;\ a, b \in A\} \tag{4}$$

por A^2. Seja s um elemento qualquer de S, denotamos

$$\{s\}B = \{sb;\ b \in B\} \tag{5}$$

por sB,

$$B\{s\} = \{bs;\ b \in B\} \tag{6}$$

por Bs e

$$\begin{aligned} A\{s\}B &= \{xv;\ x \in A,\ v \in sB\} \\ &= \{xsy;\ x \in A,\ y \in B\} \\ &= \{uy;\ u \in As,\ y \in B\} \end{aligned} \tag{7}$$

por AsB.

Definição 2.11. Sejam S um semigrupo e $\emptyset \neq I \subseteq S$, então dizemos que

(i) I é um *ideal a direita* de S, se $IS \subseteq I$.

(ii) I é um *ideal a esquerda* de S, se $SI \subseteq I$.

(iii) I é um *ideal* (a direita e a esquerda) de S, se $IS \cup SI \subseteq I$.

Seja $(S, \cdot)$ um semigrupo, então, uma vez que S é fechado para a operação $\cdot$, facilmente verifica-se que S é um ideal dele mesmo. Caso S contenha o elemento zero igual a 0, então $\{0\}$ é um ideal de S. Além disso, se I é um ideal (a direita, a esquerda ou ambos) de S com $\{0\} \subset I \subset S$, então dizemos que I é um *ideal próprio* (a direita, a esquerda ou ambos) de S.

Proposição 2.1. *Sejam S um semigrupo comutativo e $I \subseteq S$. Então $IS = SI = IS \cup SI$.*

Demonstração. Tome $x \in IS$, então existem $h \in I$ e $s \in S$, tais que $x = hs$. Como S é comutativo então $x = hs = sh \in SI$. Portanto $IS \subseteq SI$.

Reciprocamente prova-se que $SI \subseteq IS$. Logo $IS = SI$, e consequentemente $IS \cup SI = IS = SI$. ■

É uma consequência imediata da Proposição 2.1, que, se I é um ideal a esquerda de um semigrupo comutativo S, então I também é ideal a direita de S e vice-versa. Neste caso, I é simplesmente ideal de S.

Definição 2.12. Seja S um semigrupo, dizemos que

(i) S é *simples a direita*, se S é o único ideal a direita de S.

(ii) S é *simples a esquerda*, se S é o único ideal a esquerda de S.

(iii) S é *simples*, se S é o único ideal de S.

Exemplo 2.8. Todo grupo é um semigrupo simples. De fato, seja G um grupo e $\emptyset \neq I \subseteq G$ um ideal de G, logo $IG \cup GI \subseteq I$. Tome $g \in G$ e $a \in I$, então $g = (ga^{-1})a \in GI \subseteq I$, logo $G \subseteq I$, e consequentemente $I = G$.

Sejam S um semigrupo e $A \subseteq S$, temos que

$$S^1A = \{sa;\ s \in S^1,\ a \in A\}$$

Se S não é monoide, pela Definição 2.6, segue que

$$\begin{aligned} S^1A &= \{sa;\ s \in S \cup \{1\},\ a \in A\} \\ &= \{sa;\ s \in S,\ a \in A\} \cup \{1a;\ a \in A\} \\ &= SA \cup A \end{aligned}$$

Por outro lado, se S é monoide com identidade e, então

$$S^1A = \{sa;\ s \in S,\ a \in A\} = SA$$

No entanto, note que neste caso $A \subseteq SA$. De fato, tome $a \in A$, logo $a = ea \in SA$. Daí segue que $A \subseteq SA$. Portanto $SA = SA \cup A$ e, consequentemente, também temos que $S^1A = SA \cup A$.

Analogamente, concluí-se que $AS^1 = AS \cup A$. Em consequência disso temos que

$$\begin{aligned} S^1AS^1 &= S^1(AS^1) \\ &= S(AS^1) \cup (AS^1) \\ &= S(AS \cup A) \cup (AS \cup A) \\ &= SAS \cup SA \cup AS \cup A \end{aligned}$$

Assim, um subconjunto não vazio I de um semigrupo S é um ideal a direita de S se, e somente se, $IS^1 \subseteq I$, e, também I é um ideal

a esquerda de S se, e somente se, $S^1I \subseteq I$. E finalmente, o seguinte resultado demonstra que também é válido afirmar que I é um ideal de S se, e somente se, $S^1IS^1 \subseteq I$.

Proposição 2.2. *Sejam S um semigrupo e $\emptyset \neq I \subseteq S$. I é um ideal de S se, e somente se, $S^1IS^1 \subseteq I$.*

Demonstração. Seja I um ideal de S, então $IS \cup SI \subseteq I$. Logo, $IS \cup SI \cup I \subseteq I$. Tome, agora, $x \in SIS$, então existem $s_1, s_2 \in S$ e $h_1 \in I$, tal que $x = s_1h_1s_2$. Como $s_1h_1 \in SI \subseteq I$, então existe $h_2 \in I$, tal que $h_2 = s_1h_1$. Assim, $x = h_2s_2 \in IS \subseteq I$. Portanto, $x \in SIS$ implica em $x \in I$, consequentemente $SIS \subseteq I$, daí segue que $SIS \cup IS \cup SI \cup I \subseteq I$ e, assim, conclui-se que $S^1IS^1 \subseteq I$. A recíproca é imediata. ■

Nas próximas três proposições provaremos que aS^1 é o menor ideal a direita, S^1a é o menor ideal a esquerda e S^1aS^1 é o menor ideal de S que contém o elemento a de S. Note que, os conjuntos aS, Sa e SaS não, necessariamente, contém o elemento a, no entanto a sempre é um elemento de aS^1, S^1a e S^1aS^1. Já o elemento 1 pode não pertencer a qualquer um dos conjuntos aS^1, S^1a ou S^1aS^1.

Proposição 2.3. *Sejam S um semigrupo e $a \in S$. Então aS^1 é o menor ideal a direita de S contendo a.*

Demonstração. Uma vez que $a \in aS^1$, segue que aS^1 é um conjunto não vazio. Além disso, como $a \in S$ e S é fechado, então $aS \subseteq S$. Segue daí, que $aS^1 = aS \cup \{a\} \subseteq S$. Logo, $\emptyset \neq aS^1 \subseteq S$.

Para provar que aS^1 é ideal a direita de S, precisamos demonstrar que $(aS^1)S \subseteq aS^1$. A fim de mostrar isso, tome $x \in (aS^1)S$, então segue que existem $y \in aS^1$ e $s_1 \in S$, tais que $x = ys_1$. Como $y \in aS^1$, então existe $s_2 \in S^1$, tal que $y = as_2$. Logo, $x = (as_2)s_1 = a(s_2s_1)$. Como S^1 é semigrupo e $s_1 \in S \subseteq S^1$, então $s_2s_1 \in S^1$ e, portanto, $x \in aS^1$.

Por fim, provaremos que aS^1 é o menor ideal a direita de S que contém a. Para tanto, suponha que $\emptyset \neq I \subseteq S$ seja um ideal a direita de S com $a \in I$. Tome $as \in aS^1$. Como $a \in I$, então $as \in IS^1$. Caso $s \neq 1$, então $s \in S$, o que implica que $as \in IS \subseteq I$. Caso $s = 1$, então $as = a1 = a \in I$. Portanto, em todo caso, $as \in I$, logo $aS^1 \subseteq I$, consequentemente aS^1 está contido em todo ideal a direita de S que contém a, ou seja, aS^1 é o menor ideal a direita de S que contém a. ■

Proposição 2.4. *Sejam S um semigrupo e $a \in S$. Então S^1a é o menor ideal a esquerda de S contendo a.*

Demonstração. Análoga a demonstração da Proposição 2.3. ■

Proposição 2.5. *Sejam S um semigrupo e $a \in S$. Então S^1aS^1 é o menor ideal de S contendo a.*

Demonstração. Uma vez que $a \in aS^1$, segue que S^1aS^1 é um conjunto não vazio. Além disso, como $a \in S$ e S é fechado, então $SaS, Sa, aS, \{a\} \subseteq S$. Segue daí, que $S^1aS^1 = SaS \cup Sa \cup aS \cup \{a\} \subseteq S$. Logo, $\emptyset \neq S^1aS^1 \subseteq S$.

Para provar que S^1aS^1 é ideal de S, precisamos demonstrar que $(S^1aS^1)S \cup S(S^1aS^1) \subseteq S^1aS^1$. A fim de mostrar isso, tome $x \in (S^1aS^1)S$, então existem $y \in S^1aS^1$ e $s_1 \in S$, tais que $x = ys_1$. Como $y \in S^1aS^1$, então existem $s_2, s_3 \in S^1$, tais que $y = s_3as_2$. Assim, $x = (s_3as_2)s_1 = (s_3a)(s_2s_1)$. Como S^1 é semigrupo e $s_1 \in S \subseteq S^1$, então $z = s_2s_1 \in S^1$, portanto $x = s_3az \in S^1aS^1$ e, consequentemente, $(S^1aS^1)S \subseteq S^1aS^1$. De maneira semelhante, se tomarmos $x \in S(S^1aS^1)$, então concluímos que $x \in S^1aS^1$, portanto $S(S^1aS^1) \subseteq S^1aS^1$, consequentemente, $(S^1aS^1)S \cup S(S^1aS^1) \subseteq S^1aS^1$.

Por fim provaremos que S^1aS^1 é o menor ideal de S que contém a. Para tanto, suponha que $\emptyset \neq I \subseteq S$ seja um ideal de S com

$a \in I$. Tome $ras \in S^1aS^1$. Como $a \in I$, então $ras \in S^1IS^1 \subseteq I$ (pela Proposição 2.2). Portanto $ras \in I$, logo $S^1aS^1 \subseteq I$, assim temos que S^1aS^1 está contido em todo ideal de S que contém a e, consequentemente, concluímos que S^1aS^1 é o menor ideal de S que contém a. ■

Agora que sabemos que aS^1, S^1a e S^1aS^1 são, de fato, ideais de S, faz sentido escrevermos a seguinte definição.

Definição 2.13. Sejam S um semigrupo e $a \in S$, dizemos que

(i) aS^1 é o *ideal principal a direita* de S gerado por a.

(ii) S^1a é o *ideal principal a esquerda* de S gerado por a.

(iii) S^1aS^1 é o *ideal principal* de S gerado por a.

Proposição 2.6. *Se S é um semigrupo comutativo, então para todo $a \in S$, $aS^1 = S^1a = S^1aS^1$.*

Demonstração. Seja $a \in S$ qualquer. Imediatamente notamos que $aS^1 = S^1a$, pois se tomarmos $x \in aS^1$ então existe $s \in S^1$, tal que $x = as$. Como S é comutativo, S^1 também o é, logo $x = sa \in S^1a$ e, portanto, $aS^1 \subseteq S^1a$. Analogamente, conclui-se que $S^1a \subseteq aS^1$.

Agora provaremos que $S^1a = S^1aS^1$. Por um lado notamos que $S^1a \subseteq S^1aS^1$, pois basta tomar $sa \in S^1a$, então, se S é monoide, existe $e \in S^1$, tal que $sa = sae \in S^1aS^1$. E, se S não é monoide, então existe $1 \in S^1$, tal que $sa = sa1 \in S^1aS^1$. Logo em todo caso $sa \in S^1aS^1$. Agora, por outro lado, precisamos verificar que $S^1aS^1 \subseteq S^1a$. De fato, tome $ras \in S^1aS^1$. Como S^1 é comutativo e $r, s, a \in S^1$, então $ras = rsa = (rs)a \in S^1a$. ■

Proposição 2.7. *Se G é um grupo, então para todo $a \in G$, $aG^1 = G^1a = G^1aG^1 = G$.*

Demonstração. Sendo G um grupo, segue que para todo $a \in G$, existe o elemento inverso $a^{-1} \in G$, e com isso prova-se que $aG \subseteq G \subseteq Ga \subseteq GaG \subseteq aG$. Como $G = G^1$, conclui-se que $aG^1 = G^1a = G^1aG^1 = G$. ■

Lema 2.1 (Lema dos ideais principais a esquerda)**.** *Sejam S um semigrupo e $a, b \in S$, então as seguintes sentenças são equivalentes:*

(i) $S^1a \subseteq S^1b$

(ii) $a \in S^1b$

(iii) existe $t \in S^1$, tal que $a = tb$

(iv) $a = b$ ou existe $t \in S$, tal que $a = tb$

Demonstração. Vamos demonstrar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.

- $(i) \Rightarrow (ii)$: Note que $a \in S^1a \subseteq S^1b \Rightarrow a \in S^1b$.
- $(ii) \Rightarrow (iii)$: Como $a \in S^1b$, então existe $t \in S^1$, tal que $a = tb$.
- $(iii) \Rightarrow (iv)$: Suponha que existe $t \in S^1$, tal que $a = tb$. Se S é monoide, então $S^1 = S$ e portanto existe $t \in S$, tal que $a = tb$. Se S não é monoide, então $S^1 = S \cup \{1\}$, logo existe $t \in S \cup \{1\}$, tal que $a = tb$, o que implica que $t = 1$ ou $t \in S$. Caso $t = 1$, então $a = tb = 1b = b$. Caso $t \in S$ então existe $t \in S$, tal que $a = tb$. Portanto, em todo caso, $a = b$ ou existe $t \in S$ tal que $a = tb$.
- $(iv) \Rightarrow (i)$: Se $a = b$, obviamente, $S^1a = S^1b \Rightarrow S^1a \subseteq S^1b$. Por outro lado, se $a \neq b$, então existe $t \in S$, tal que $a = tb$. Tome, daí, $x \in S^1a$, logo existe $s \in S^1$, tal que $x = sa = s(tb) = (st)b \in S^1b$, portanto $S^1a \subseteq S^1b$.

■

Lema 2.2 (Lema dos ideais principais a direita)**.** *Sejam S um semigrupo e $a, b \in S$, então as seguintes sentenças são equivalentes:*

(i) $aS^1 \subseteq bS^1$

(ii) $a \in bS^1$

(iii) *existe* $t \in S^1$, *tal que* $a = bt$

(iv) $a = b$ *ou existe* $t \in S$, *tal que* $a = bt$

Demonstração. Análoga ao do Lema 2.1. ■

Lema 2.3 (Lema dos ideais principais)**.** *Sejam S um semigrupo e $a, b \in S$, então as seguintes sentenças são equivalentes:*

(i) $S^1aS^1 \subseteq S^1bS^1$

(ii) $a \in S^1bS^1$

(iii) *existem* $s, t \in S^1$, *tais que* $a = sbt$

Demonstração. Vamos demonstrar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

- $(i) \Rightarrow (ii)$: Note que $a \in S^1aS^1 \subseteq S^1bS^1 \Rightarrow a \in S^1bS^1$.
- $(ii) \Rightarrow (iii)$: Como $a \in S^1bS^1$, então existem $s, t \in S^1$, tais que $a = sbt$.
- $(iii) \Rightarrow (i)$: Suponha que existem $s, t \in S^1$, tais que $a = sbt$. Tome $x \in S^1aS^1$, logo exitem $u, v \in S^1$ tal que $x = uav = u(sbt)v = (us)b(tv) \in S^1bS^1$, portanto $S^1aS^1 \subseteq S^1bS^1$.

■

2.3 SUBSEMIGRUPOS E SUBMONOIDES

Definição 2.14. Sejam S um semigrupo e T um subconjunto não vazio de S. Dizemos que T é um *subsemigrupo* de S se para todo $a, b \in T$, $ab \in T$.

Em outras palavras, um subsemigrupo de um semigrupo S é um subconjunto não vazio de S, que munido com a operação binária de S, é também um semigrupo.

Definição 2.15. Sejam M um monoide com elemento identidade igual a 1 e T um subconjunto não vazio de M. Dizemos que T é um *submonoide* de M se T é um subsemigrupo de M e, adicionalmente, $1 \in T$.

Exemplo 2.9. Considere o monoide $W = \{1, e, f\}$ com a tabela de Cayley exibida na Tabela 2. Note que $\{1\}, \{1, e\}, \{1, f\}, W \subseteq W$ são submonoides de W.

Tabela 2 – Tabela de Cayley do monoide W

	1	e	f
1	1	e	f
e	e	e	f
f	f	f	f

A propriedade associativa de um subsemigrupo ou submonoide é estendida trivialmente do semigrupo ou monoide respectivo, uma vez que o subsemigrupo ou o submonoide é um subconjunto fechado do respectivo semigrupo ou monoide.

Um submonoide tem, por definição, a mesma identidade de seu respectivo monoide. Ainda assim, é possível tomar um subconjunto de um monoide que seja um novo monoide com seu próprio elemento

identidade. Observe, por exemplo, o subconjunto $N = \{e, f\}$ do monoide W do Exemplo 2.9 com a tabela de Cayley (Tabela 2). Note que N é também um monoide com identidade $e \in N$, no entanto $e \neq 1$ e $1 \notin N$ e, consequentemente, N não é um submonoide de W.

A proposição a seguir apresenta uma condição alternativa para caracterizar um subsemigrupo.

Proposição 2.8. *Sejam S um semigrupo e $A \subseteq S$. A é um subsemigrupo de S se, e somente se, $A \neq \emptyset$ e $A^2 \subseteq A$.*

Demonstração. Como A é subsemigrupo de S, por definição, segue que $A \neq \emptyset$. Tome, portanto, $a \in A^2$, então existem $x, y \in A$ tais que $a = xy$. Mas $x, y \in A \Rightarrow xy \in A$, portanto $a \in A$, consequentemente $A^2 \subseteq A$.

Reciprocamente, suponha $\emptyset \neq A \subseteq S$ com $A^2 \subseteq A$. Tome $x, y \in A$, então $xy \in A^2 \subseteq A$, portanto A é um subsemigrupo de S. ■

As três proposições seguintes mostram que todo ideal (a direita, a esquerda ou de ambos os lados) de um semigrupo qualquer é também um subsemigrupo.

Proposição 2.9. *Sejam S um semigrupo e $I \subseteq S$ um ideal a direita em S. Então, I é um subsemigrupo de S.*

Demonstração. Tome $a, b \in I$, então $b \in S$ (pois $I \subseteq S$). Logo $ab \in IS$. Como I é ideal a direita em S, então $IS \subseteq I$, portanto $ab \in I$, consequentemente I é subsemigrupo de S. ■

Proposição 2.10. *Sejam S um semigrupo e $I \subseteq S$ um ideal a esquerda em S. Então, I é um subsemigrupo de S.*

Demonstração. Tome $a, b \in I$, então $a \in S$. Logo $ab \in SI \subseteq I$, portanto $ab \in I$. ■

Proposição 2.11. *Sejam S um semigrupo e $I \subseteq S$ um ideal em S. Então, I é um subsemigrupo de S.*

Demonstração. Tome $a, b \in I$, então $b \in S$. Logo $ab \in IS \subseteq IS \cup SI \subseteq I$, portanto $ab \in I$. ■

2.4 GRUPOS E SUBGRUPOS

Apresentaremos, inicialmente, nessa seção, a definição de *grupo*, já mencionada anteriormente. Em poucas palavras, um grupo é um monoide em que todo elemento possui um elemento inverso. Ou dito formalmente:

Definição 2.16. Um *grupo* é um par ordenado $(G, \cdot)$ em que G é um conjunto não vazio e $\cdot$ é uma operação binária em G, tal que para todo $a, b, c \in G$ valem as seguintes propriedades:

(i) (fechamento) $a \cdot b \in G$

(ii) (associatividade) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(iii) (elemento identidade) existe $1 \in G$ tal que $a1 = 1a = a$

(iv) (elemento inverso) para todo $a \in G$, existe um elemento inverso em G, denotado por a^{-1}, tal que $aa^{-1} = a^{-1}a = 1$

As seguintes propriedades seguem trivialmente da definição de grupo:

(i) O elemento identidade do grupo é único.

(ii) Cada elemento do grupo possui um único elemento inverso.

(iii) Para todo $a \in G$, $(a^{-1})^{-1} = a$.

(iv) Para todo $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

(v) Todo grupo é cancelativo.

Estas propriedades e outros resultados relacionadas a grupos podem ser consultadas em Domingues e Iezzi [2, p. 137-210].

A seguinte proposição exibe uma descrição alternativa que pode ser usada para definir um grupo, partindo da definição de semigrupo.

Proposição 2.12. *Seja S um semigrupo. S é um grupo se, e somente se, para todo $a \in S$, $aS = Sa = S$.*

Demonstração. Pela Proposição 2.7, já temos provado que se S é um grupo, então para todo $a \in S$, $aS = Sa = S$. Precisamos, então, mostrar que se S é um semigrupo com a propriedade de que para todo $a \in S$, $aS = Sa = S$, então S é um grupo.

Suponha que S é um semigrupo com a propriedade mencionada. Tome $a \in S$, logo pela propriedade acima $aS = Sa = S$. Segue daí que existem $e, f \in S$, tais que $ae = a = fa$. Consequentemente, também existem $b, c \in S$, tais que $ab = e$ e $ca = f$. De $fa = a$ temos que $(fa)b = ab \Rightarrow f(ab) = ab \Rightarrow fe = e$. Por outro lado, de $ae = a$ temos que $c(ae) = ca \Rightarrow (ca)e = ca \Rightarrow fe = f$. Portanto $e = fe = f$ e consequentemente $e^2 = e$ e $ae = ea = a$.

Note que o elemento $e \in S$ tem propriedade de identidade para o elemento $a \in S$. Vamos provar que $e \in S$ é identidade para todo elemento de S e consequentemente S é monoide com identidade e. De fato, tome $x \in S$. Como $S = Sa$, então existe $u \in S$ tal que $x = ua$. Logo $xe = (ua)e = u(ae) = ua = x$. Como $S = aS$, então existe $w \in S$ tal que $x = aw$. Logo $ex = e(aw) = (ea)w = aw = x$. Temos provado, portanto, até aqui que existe $e \in S$, tal que $xe = ex = x$ para todo $x \in S$, ou seja, S é um monoide com identidade igual a e. Vamos provar agora a existência de elemento inverso para cada elemento de S.

De $ab = e$, $ca = f$ e $e = f$, temos que $ab = e = ca$. Segue daí que $b = eb = (ca)b = c(ab) = ce = c$, logo $b = c$ e, consequentemente, $ab = e = ba$. Ou seja, b é elemento inverso de a, e S é, portanto, um grupo. ■

A Proposição 2.7 prova que se G é um grupo e a é um elemento arbitrário de G, então $aG = Ga = G = GaG$. Logo, pela Proposição 2.12 acima, segue que sendo S um semigrupo em que para todo $a \in S$, $aS = Sa = S$, então $SaS = S$.

Definição 2.17. Seja G um grupo. Chamamos G^0 de *grupo com zero* ou *0-grupo*.

Exemplo 2.10. Note que ao adicionarmos zero ao grupo G, obtemos o semigrupo com zero $G^0 = G \cup \{0\}$ que não é um grupo. Por exemplo, $(\mathbb{Q} - \{0\}, \cdot)$ é um grupo. No entanto $(\mathbb{Q}, \cdot)$ é um semigrupo com zero que não é um grupo.

Proposição 2.13. *Seja S um semigrupo com zero, com elemento nulo igual a 0. S é um 0-grupo se, e somente se, para todo $a \in S - \{0\}$, $aS = Sa = S$.*

Demonstração. Suponha que $S = G^0$ é um 0-grupo, e seja $a \in G = S - \{0\}$. Como G é grupo, certamente $aG = Ga = G$. Como $aS = aG \cup \{0\}$ e $Sa = Ga \cup \{0\}$, segue que $aS = Sa = S$.

Reciprocamente, suponha que S seja um semigrupo com zero, com elemento zero igual a 0 e com a seguinte propriedade: para todo $a \in S - \{0\}$, $aS = Sa = S$. Seja $G = S - \{0\}$. Como S é um semigrupo com zero, então, por definição, S tem pelo menos dois elementos, logo $G \neq \emptyset$.

Para mostrar que G é um grupo, primeiro provaremos que G é fechado para a operação de S. Então, suponha, por contradição, que existem $a, b \in G$, tais que $ab = 0$. Logo $S^2 = (Sa)(bS) = S(ab)S =$

$S0S = \{0\}$ e, assim, $S = aS \subseteq S^2 = \{0\}$, ou seja, $S \subseteq \{0\}$ e isto implicaria que ou $S = \{0\}$ ou $S = \emptyset$ e, consequentemente, $G = S - \{0\} = \emptyset$. O que é uma contradição com o fato de que $G \neq \emptyset$. Portanto G é fechado para a operação de S.

A propriedade assumida para S implica que para todo $a, b \in G$, existem $x, y \in S$, tais que $ax = b = ya$. Como $a, b \in G$ então $a \neq 0$ e $b \neq 0$, logo $ax = b \neq 0$ e $ya = b \neq 0$, o que implica que $x \neq 0$ e $y \neq 0$, portanto $x, y \in G$. Em outras palavras, para todo $a, b \in G$, existem $x, y \in G$, tais que $ax = b = ya$. Ou seja, para todo $a \in G$, $aG = G = Ga$. Portanto, pela Proposição 2.12, G é um grupo. ■

Um *subgrupo de um grupo* G é um subconjunto de G, que munido com a operação binária de G, é também um grupo. No entanto podemos também encontrar um *subgrupo de um semigrupo*, que de modo análogo, é um subconjunto de um semigrupo S, que munido com a operação binária de S, é um grupo. Formalmente definimos da seguinte maneira:

Definição 2.18. Sejam S um semigrupo e $H \subseteq S$, dizemos que H é um *subgrupo* de S, denotado por $H < S$, se e somente se, H é um grupo com a operação de S. Isto é, para todo $a, b, c \in H$ valem as seguintes propriedades:

(i) (fechamento) $ab \in H$

(ii) (associatividade) $a(bc) = (ab)b$

(iii) (elemento identidade) existe $e \in H$ tal que $ae = ea = a$

(iv) (elemento inverso) para todo $a \in H$, existe $b \in H$ tal que $ab = ba = e$

Assim, enquanto que a identidade de um subgrupo de um grupo é igual à identidade do grupo herdado, um mesmo semigrupo poderá

conter vários subgrupos, cada um com uma identidade distinta do outro. Como pode ser observado no monoide M do Exemplo 2.9, $\{1\}$, $\{e\}$ e $\{f\}$ são subgrupos de M, mas $1 \neq e \neq f$.

O seguinte resultado é uma consequência imediata da Definição 2.18 e da Proposição 2.12:

Proposição 2.14. *Sejam S um semigrupo e T um subsemigrupo de S. T é um subgrupo de S se, e somente se, para todo $a \in T$, $aT = Ta = T$.*

2.5 HOMOMORFISMOS E ISOMORFISMOS

Definição 2.19. Sejam S, T semigrupos. Dizemos que a função $\theta : S \longrightarrow T$ é um *homomorfismo de semigrupos*, se para todo $a, b \in S$, $\theta(ab) = \theta(a)\theta(b)$

Definição 2.20. Sejam S, T monoides. Dizemos que a função $\theta : S \longrightarrow T$ é um *homomorfismo de monoides*, se é um homomorfismo de semigrupos e, além disso, $\theta(1_S) = 1_T$, em que $1_S, 1_T$ são as identidades de S e de T, respectivamente.

Na teoria de grupos algébricos, temos que se G e H são grupos e $\theta : G \longrightarrow H$ é um homomorfismo de grupos, então $\theta(1_G) = 1_H$, em que 1_G e 1_H são as identidades de G e de H, respectivamente. Isso é uma consequência da definição de homomorfismo de grupos pelo fato da existência de elemento inverso. No entanto, o mesmo não é verdade para monoides. Ou seja, poderíamos ter um homomorfismo de semigrupos entre monoides que não leva a identidade de um monoide na identidade do outro, logo o fato de levar identidade em identidade não é uma consequência da definição de homomorfismo de monoides e por isso esse fato é colocado junto com a definição.

Podemos notar que esta situação ocorre se, por exemplo, construirmos uma função θ que leva um monoide M qualquer em outro monoide T que tenha um elemento idempotente $e \in T$ diferente do seu elemento identidade tal que para todo $m \in M$, $\theta(m) = e$. Tal situação é exemplificada abaixo.

Exemplo 2.11. Sejam $M = \{1_M, a, b, c, d\}$ e $T = \{1_T, \alpha, \beta\}$ dois monoides com identidades iguais a 1_M e 1_T respectivamente, representados pelas tabelas de Cayley exibidas na Tabela 3 e na Tabela 4. Tome, daí, a função $\theta : M \longrightarrow T$ dada por $\theta(m) = \beta$, para todo $m \in M$. Observe que θ é um homomorfismo de semigrupos. De fato, para todo $u, v \in M$ temos $\theta(uv) = \beta = \beta^2 = \beta\beta = \theta(u)\theta(v)$. No entanto $\theta(1_M) = \beta \neq 1_T$.

Tabela 3 – Tabela de Cayley do monoide M

	1_M	a	b	c	d
1_M	1_M	a	b	c	d
a	a	a	b	a	b
b	b	a	b	a	b
c	c	c	d	c	d
d	d	c	d	c	d

Tabela 4 – Tabela de Cayley do monoide T

	1_T	α	β
1_T	1_T	α	β
α	α	α	β
β	β	α	β

Definição 2.21. Chamamos de *monomorfismo de semigrupos (monoides)* um homomorfismo de semigrupos (monoides) que é injetivo. Chamamos de *endomorfismo de semigrupos (monoides)* um homomorfismo de semigrupos (monoides) que tem o mesmo semigrupo (monoide) como domínio e contradomínio.

Definição 2.22. Um homomorfismo de semigrupos (monoides) bijetivo é chamado de *isomorfismo de semigrupos (monoides)*. Sejam S e T dois semigrupos (monoides), se existe um isomorfismo entre S e T, então dizemos que S é *isomorfo* a T e, denotamos $S \cong T$. Chamamos de *automorfismo de semigrupos (monoides)* um isomorfismo de semigrupos (monoides) que tem o mesmo semigrupo (monoide) como domínio e contradomínio.

Sejam f e g funções quaisquer em um conjunto X, definimos a operação binária de composição de funções por $f \circ g(x) = f(g(x))$, para todo $x \in X$.

Sejam X um conjunto qualquer não vazio e $\mathcal{S}_X$ *o conjunto de todas as funções bijetivas em* X, isto é,

$$\mathcal{S}_X = \{\alpha : X \longrightarrow X; \alpha \text{ é uma bijeção}\}$$

então $\mathcal{S}_X$ munido da operação binária de composição de funções ($\circ$) é um grupo conhecido como *grupo de permutação em* X. Em particular, denota-se por $\mathcal{S}_n$ o conjunto $\mathcal{S}_{I_n}$ em que

$$I_n = \{x \in \mathbb{N}; 1 \leq x \leq n\} \tag{8}$$

De modo semelhante, definimos $\mathcal{T}_X$ *o conjunto de todas as funções em* X, isto é,

$$\mathcal{T}_X = \{\alpha : X \longrightarrow X\}.$$

Então $(\mathcal{T}_X, \circ)$ é um monoide, conhecido como *monoide de transformação completa em* X, com identidade igual a *função identidade em* X ($I_X : X \longrightarrow X$ dada por $I_X(x) = x$, $\forall x \in X$). Em particular, denota-se por $\mathcal{T}_n$ o conjunto $\mathcal{T}_{I_n}$ em que I_n é o conjunto definido na Equação (8).

Seja v um elemento do conjunto X, denotamos por $c_v \in \mathcal{T}_X$ a função constante que faz corresponder todo elemento de X a v, ou

seja, para todo $x \in X$, $c_v(x) = v$. O *conjunto de todas as funções constantes em* X munido da operação de composição de funções é um subsemigrupo de $\mathcal{T}_X$. Já $(\mathcal{S}_X, \circ)$ é um subgrupo de $(\mathcal{T}_X, \circ)$.

Se $X = \{x_1, x_2, \ldots, x_n\}$ é um conjunto finito com n elementos, então podemos denotar $\alpha \in \mathcal{S}_X$ por

$$\alpha = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \alpha(x_1) & \alpha(x_2) & \ldots & \alpha(x_n) \end{pmatrix}$$

e também podemos denotar $\beta \in \mathcal{T}_X$ por

$$\beta = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \beta(x_1) & \beta(x_2) & \ldots & \beta(x_n) \end{pmatrix}.$$

Com alguns argumentos simples de análise combinatória podemos mostrar que, se $|X| = n$ (em que $|X|$ denota a cardinalidade do conjunto X), então $|\mathcal{S}_X| = n!$ e $|\mathcal{T}_X| = n^n$.

Proposição 2.15. *Sejam S, T semigrupos, $\emptyset \neq A \subseteq S$ e $f : S \longrightarrow T$ um homomorfismo. Se A é um subsemigrupo de S, então $f(A) = \{f(a); a \in A\}$ é um subsemigrupo de T.*

Demonstração. Sendo A subsemigrupo de S, então para todo $a, b \in A$, $ab \in A$. Como f é uma função, segue que $f(a), f(b), f(ab) \in f(A)$. Como f é um homomorfismo, então $f(a)f(b) = f(ab) \in f(A)$. Como $\emptyset \neq f(A) \subseteq T$, então $f(A)$ é um subsemigrupo de T. ■

Proposição 2.16. *Sejam S, T semigrupos, $\emptyset \neq B \subseteq T$, $f : S \longrightarrow T$ um homomorfismo. Se B subsemigrupo de T, então $f^{-1}(B) = \{s \in S; f(s) \in B\}$ é um subsemigrupo de S ou então $f^{-1}(B) = \emptyset$.*

Demonstração. Caso, para todo $b \in B$, não exista $s \in S$ tal que $b = f(s)$ então $f^{-1}(B) = \emptyset$.

Caso, exista algum $y \in B$ tal que exista $s \in S$ tal que $y = f(s)$ então $s \in f^{-1}(B) \neq \emptyset$. Sejam, assim, $a, b \in S$ tais que $f(a), f(b) \in B$,

então $a, b \in f^{-1}(B)$. Como B subsemigrupo de T, então $f(a)f(b) \in B$. Como f é um homomorfismo, então $f(a)f(b) = f(ab) \in B$ e portanto $ab \in f^{-1}(B)$. Logo $f^{-1}(B)$ é um subsemigrupo de S. ■

Definição 2.23. Sejam S e T dois semigrupos (monoides), se S é isomorfo a algum subsemigrupo (submonoide) de T, então dizemos que S está *imerso* em T.

Seja $\alpha : S \longrightarrow T$ um homomorfismo de semigrupos, segue da Proposição 2.15 que $\operatorname{Im}\alpha$ é um subsemigrupo de T. Se α é injetiva, então $\alpha' : S \longrightarrow \operatorname{Im}\alpha$ dada por $\alpha'(x) = \alpha(x)$ para todo $x \in S$ é um isomorfismo ($S \cong \operatorname{Im}\alpha$), ou seja, S está imerso em T. Em outras palavras podemos enunciar a seguinte proposição, cuja prova pode ser obtida diretamente das definições 2.21 e 2.23 e da Proposição 2.15.

Proposição 2.17. *Sejam S, T semigrupos (monoides). S está imerso em T se, e somente se, existe um monomorfismo de semigrupos (monoides) de S em T.*

Pelo *Teorema de Cayley* para grupos, temos que se G é um grupo então ele é isomorfo a um subgrupo de $\mathcal{S}_G$. Em particular, se G tem ordem n então G é isomorfo a um subgrupo de $\mathcal{S}_n$. Assim, adaptando a Definição 2.23 para grupos, podemos afirmar que G está imerso em $\mathcal{S}_G$. Resultado semelhante pode ser obtido para semigrupos e monoides.

Teorema 2.1 (Cayley para Semigrupos)**.** *Seja S um semigrupo, então S está imerso em $\mathcal{T}_{S^1}$*

Demonstração. Para cada $s \in S$, definimos $\rho_s \in \mathcal{T}_{S^1}$ dada por $\rho_s(x) = sx$ para todo $x \in S^1$. E daí, definimos $\alpha : S \longrightarrow \mathcal{T}_{S^1}$ dada por $\alpha(s) = \rho_s$, para todo $s \in S$.

Tome $a, b \in S$ tais que $a = b$, então $ax = bx$, para todo $x \in S^1$. Logo $\rho_a(x) = \rho_b(x)$, para todo $x \in S^1$. Consequentemente $\alpha(a) = \alpha(b)$. Portanto α está bem definida.

Tome $a, b \in S$ tais que $\alpha(a) = \alpha(b)$, então $\rho_a = \rho_b$. Logo $\rho_a(x) = \rho_b(x)$, para todo $x \in S^1$. Assim $ax = bx$, para todo $x \in S^1$. Em particular, $a1 = b1$ e consequentemente $a = b$. Portanto α é injetiva.

Ademais, tome $u, v \in S$ quaisquer. Então, para cada $x \in S^1$ temos $\rho_u \circ \rho_v(x) = \rho_u(\rho_v(x)) = \rho_u(vx) = u(vx) = (uv)x = \rho_{uv}(x)$. Consequentemente $\rho_u \circ \rho_v = \rho_{uv}$ e então $\alpha(u) \circ \alpha(v) = \rho_u \circ \rho_v = \rho_{uv} = \alpha(uv)$. Portanto α é um homomorfismo de semigrupos.

Segue daí que α é um homomorfismo de semigrupos injetivo, ou seja, α é um monomorfismo de semigrupos. Consequentemente, pela Proposição 2.17, S está imerso em $\mathcal{T}_{S^1}$. ■

Teorema 2.2 (Cayley para Monoides)**.** *Seja M um monoide, então M está imerso em $\mathcal{T}_M$*

Demonstração. Sendo M um monoide com identidade 1 e definindo α e ρ como no Teorema 2.1, concluímos analogamente que α é um homomorfismo injetivo de semigrupos. Para mostrar que α é um homomorfismo de monoides, precisamos provar que $\alpha(1) = I_M$ em que I_M é a função identidade em M. De fato, $\alpha(1) = \rho_1$, e para todo $x \in M$ temos que $\rho_1(x) = 1x = x = I_M(x)$. Portanto $\alpha(1) = \rho_1 = I_M$. ■

2.6 BANDA RETANGULAR

Nesta seção abordarmos um tipo especial de semigrupo conhecido como *banda retangular*. Definido formalmente como segue:

Definição 2.24. Dizemos que um semigrupo S é uma *banda retangular*, se para todo a, b em S temos $aba = a$.

Teorema 2.3. *Seja S um semigrupo, então as seguintes condições são equivalentes:*

(i) *S é uma banda retangular;*

(ii) *todo elemento de S é idempotente, e $abc = ac$ para todo $a, b, c \in S$;*

(iii) *existe um semigrupo zero à esquerda L e um semigrupo zero à direita R tais que S é isomorfo ao produto direto de L e R ($S \cong L \times R$);*

(iv) *S é isomorfo a um semigrupo da forma $(A \times B, \cdot)$, em que A e B são conjuntos não vazios, e $\cdot$ é uma operação binária em $A \times B$ dada por $(a_1, b_1) \cdot (a_2, b_2) = (a_1, b_2)$;*

Demonstração. Vamos demonstrar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.

- $(i) \Rightarrow (ii)$: Seja $a \in S$, então, pelo item (i), $a^3 = a$. Consequentemente $a^4 = a^2$. Novamente pelo item (i) temos $a = a(a^2)a = a^4$, logo $a^2 = a$. Agora, sejam $a, b, c \in S$. Do item (i) segue que $a = aba$, $c = cbc$ e $b = b(ac)b$. Portanto $ac = (aba)(cbc) = a(bacb)c = abc$.

- $(ii) \Rightarrow (iii)$: Escolha e fixe um elemento c de S. Sejam $L = Sc$ e $R = cS$. Então, usando o item (ii), vemos que para todo $x = zc$ e $y = tc$ em L, $xy = zctc = zc^2 = zc = x$, logo L é um semigrupo zero à esquerda. Analogamente conclui-se que R é um semigrupo zero à direita.

  Definamos $\theta : S \longrightarrow L \times R$ dada por $\theta(x) = (xc, cx)$ para todo $x \in S$. Então θ é injetiva. De fato, se $(xc, cx) = (yc, cy)$ então $x = x^2 = xcx = ycx = ycy = y^2 = y$. θ também é sobrejetiva,

desde que para todo $(ac, cb) \in L \times R$, podemos usar o item (ii), para verificar que $(ac, cb) = (abc, cab) = \theta(ab)$. Portanto θ é bijetiva.

Note, além disso que θ é um homomorfismo. De fato, para todo $x, y \in S$, $\theta(xy) = (xyc, cxy) = (xc, cy) = (xcyc, cxcy) = (xc, cx)(yc, cy) = \theta(x)\theta(y)$. Portanto θ é um isomorfismo de S em $L \times R$.

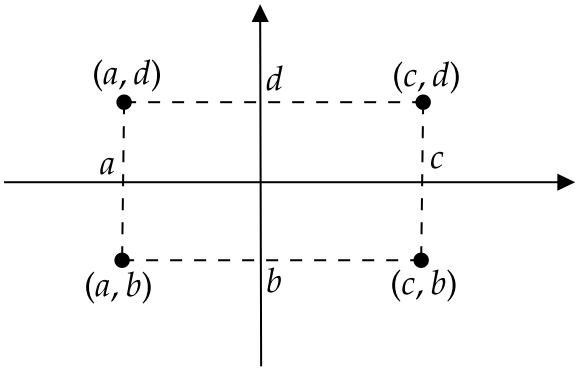
- $(iii) \Rightarrow (iv)$: Suponha que $S = L \times R$ em que L é um semigrupo zero à esquerda e R é um semigrupo zero à direita. Então para todo $(a, b), (c, d) \in S$, $(a, b)(c, d) = (ac, bd) = (a, d)$. Assim precisamos apenas obter $A = L$ e $B = R$.

- $(iv) \Rightarrow (i)$: Seja $S = A \times B$ com operação binária dada. Então para todo $a = (x, y)$ e $b = (z, t)$ em S temos $aba = (x, y)(z, t)(x, y) = (x, t)(x, y) = (x, y) = a$. Logo S é uma banda retangular.

■

Quanto a nomenclatura do semigrupo banda retangular, note que o termo "banda" provém do item (ii) do Teorema 2.3, pois trata-se de um semigrupo em que todos os seus elementos são idempotentes. O termo "retangular" provém do item (iv) do Teorema 2.3: se pensarmos em (a, b) e (c, d) como pontos de um plano cartesiano então $(a, b)(c, d)$ e $(c, d)(a, b)$ são colocados nos vértices do retângulo, como vemos na Figura 1.

Figura 1 – Banda retangular $A \times B$



2.7 SEMIGRUPO MONOGÊNICO

Nesta seção abordarmos um outro tipo especial de semigrupo conhecido como *semigrupo monogênico* que, como veremos, se assemelha ao *grupo cíclico* de teoria de grupos.

Seja S um semigrupo e $\{U_i; i \in I \neq \emptyset\}$ uma família de subsemigrupos de S. Se a intersecção $U = \bigcap_{i \in I} U_i$ não é vazia, então U é um subsemigrupo de S. De fato, tome $x, y \in U \neq \emptyset$, então $x, y \in U_i$ para todo $i \in I$, consequentemente $xy \in U_i$ para todo $i \in I$. Portanto $xy \in U = \bigcap_{i \in I} U_i$, logo U é um subsemigrupo de S. Para todo subconjunto A de S, existe pelo menos um subsemigrupo de S contendo A (trivialmente S é um subsemigrupo dele mesmo e $A \subseteq S$). Consequentemente a intersecção de todos os subsemigrupos de S contendo A é um subsemigrupo de S que contém A.

Definição 2.25. Sejam S um semigrupo e A um subconjunto de S. Denotamos por $\langle A \rangle$ o subsemigrupo dado pela *intersecção de todos os*

subsemigrupos de S que contém A. Tal subsemigrupo pode ser definido pelas seguintes propriedades:

(i) $A \subseteq \langle A \rangle$;

(ii) se U é um subsemigrupo de S contendo A, então $\langle A \rangle \subseteq U$.

Caso o conjunto A, mencionado na Definição 2.25, seja finito com $n \in \mathbb{N}$ elementos (sendo assim $A = \{a_1, a_2, a_3, \ldots, a_n\}$), então podemos denotar $\langle A \rangle$ por $\langle a_1, a_2, a_3, \ldots, a_n \rangle$. No caso particular em que A contém um único elemento ($A = \{a\}$), temos

$$\begin{aligned} \langle A \rangle &= \langle a \rangle \\ &= \{a, a^2, a^3, \ldots\} \\ &= \{a^n; n \in \mathbb{N}\} \end{aligned}$$

Note, além disso, que $\langle a \rangle$ é um subsemigrupo comutativo de S.

Definição 2.26. Sejam S um semigrupo e $A \subseteq S$. Se $S = \langle A \rangle$, então dizemos que A é um *conjunto de geradores* de S.

Definição 2.27. Sejam S um semigrupo e $a \in S$. Chamamos $\langle a \rangle$ de *subsemigrupo monogênico de S gerado por a.*

Definição 2.28. Seja S um semigrupo. Se existe algum elemento a em S tal que $S = \langle a \rangle$, ou seja, se S é gerado por um único elemento, então dizemos que S é um *semigrupo monogênico.*

Exemplo 2.12. O semigrupo $(\mathbb{N}, +)$ do item (i) do Exemplo 2.1 é um semigrupo monogênico, uma vez que $\mathbb{N} = \langle 1 \rangle$.

Definição 2.29. Seja S um semigrupo. Se S é finito (tem uma quantidade finita de elementos), então dizemos que a cardinalidade de S, denotada por $|S|$, é a *ordem de S*, denotado por $O(S)$. Neste caso, $O(S) = |S|$ e dizemos que S *tem ordem finita.* Se S é infinito, então

dizemos que S *tem ordem infinita*, denotamos este fato por $O(S) = \infty$. Se a é um elemento de S, então chamamos a ordem do subsemigrupo $\langle a \rangle$ de *ordem de* a (denotamos por $O(a)$).

Na teoria de grupos algébricos, o grupo gerado por um único elemento é chamado de *grupo cíclico*. Um grupo cíclico finito com n elementos é isomorfo a $(\mathbb{Z}_n, +)$, enquanto que um grupo cíclico infinito é isomorfo a $(\mathbb{Z}, +)$. No caso de semigrupos, podemos analogamente, enunciar o seguinte resultado:

Proposição 2.18. *Sejam S um semigrupo e $a \in S$. Então uma das duas possibilidades seguintes ocorre:*

(i) $\langle a \rangle$ *é infinito e isomorfo a* $(\mathbb{N}, +)$*; ou*

(ii) $\langle a \rangle$ *é finito e existem naturais* $n, r \in \mathbb{N}$ *tais que*

(i) $\langle a \rangle = \{a, a^2, a^3, \ldots, a^{n+r-1}\}$*;*

(ii) a *possui ordem igual a* $n + r - 1$*;*

(iii) $a^n = a^{n+r}$*;*

(iv) para todo $u, v \in \mathbb{N}^0$*,* $a^{n+u} = a^{n+v}$ *se, e somente se,* $u \equiv v \mod r$*.*

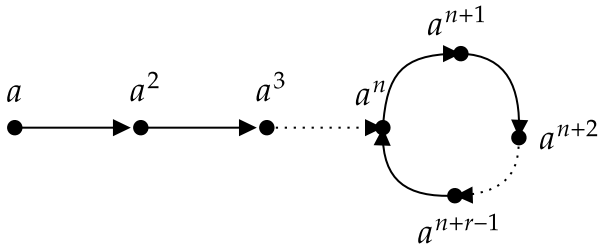
Demonstração. Sendo $a \in S$ temos dois casos a analisar para um subsemigrupo monogênico de S gerado por a: ou $\langle a \rangle$ possui elementos distintos para toda potência de números naturais distintos dois a dois; ou $\langle a \rangle$ possui elementos iguais para algumas potências de números naturais diferentes.

Caso $\langle a \rangle$ possua elementos distintos para toda potência de números naturais distintos dois a dois, segue que $a^i \neq a^j$ para todo $i, j \in \mathbb{N}$ com $i \neq j$, então $\theta : \langle a \rangle \longrightarrow \mathbb{N}$ dada por $\theta(a^i) = i$ é um isomorfismo de semigrupos e, consequentemente, $\langle a \rangle \cong (\mathbb{N}, +)$.

Caso $\langle a \rangle$ possua elementos iguais para algumas potências de números naturais diferentes, segue que na listagem de elementos de $\langle a \rangle$ existe alguma repetição, isto é, existem $a^i = a^j$ para algum $i, j \in \mathbb{N}$ com $i \neq j$. Sem perda de generalidade, considere $i < j$. Seja $k \in \mathbb{N}$ o menor natural tal que $a^k = a^n$ para algum $n \in \mathbb{N}$ com $n < k$. Então exite $r \in \mathbb{N}$ tal que $k = n + r$. Como k foi tomado o menor natural tal que $a^k = a^n$ com $n < k$, então os elementos $a, a^2, a^3, \ldots, a^{n+r-1}$ são todos distintos e $a^n = a^{n+r}$. Note daí que $a^{n+2r} = a^{n+r+r} = a^{n+r}a^r = a^n a^r = a^{n+r} = a^n$ e consequentemente $a^{n+rm} = a^n$ para todo $m \in \mathbb{N}^0$. Seja $u \in \mathbb{N}^0$. Escrevemos, pelo algorítimo de Euclides, $u = qr + t$ para algum $q, t \in \mathbb{N}^0$ com $0 \leq t < r$. Então $a^{n+u} = a^{n+qr+t} = a^{n+qr}a^t = a^n a^t = a^{n+t}$ e portanto temos que $\langle a \rangle = \{a, a^2, a^3, \ldots, a^{n+r-1}\}$ e consequentemente a ordem de a é $n + r - 1$ ■

Os naturais n e r mencionados no item (ii) da Proposição 2.18 são, respectivamente, chamados de **índice** e **período** do elemento a. A representação gráfica de um subsemigrupo monogênico finito de S gerado por a pode ser observada na Figura 2.

Figura 2 – Subsemigrupo monogênico finito de S gerado por a



Observação 2.6. Sejam S um semigrupo e $a \in S$. Suponha que $\langle a \rangle$ seja finito com índice n e período r, então $\langle a \rangle = \{a, a^2, a^3, \ldots, a^{n+r-1}\}$ e daí denotaremos por K_a subconjunto $\{a^n, a^{n+1}, \ldots, a^{n+r-1}\}$ de $\langle a \rangle$. Note que K_a possui ordem r e é um ideal de $\langle a \rangle$.

Proposição 2.19. *Sejam S um semigrupo e $a \in S$. Se $\langle a \rangle$ é finito então $\langle a \rangle$ contém um elemento idempotente.*

Demonstração. Sejam n e r respectivamente o índice e o período de $a \in S$. Escolha $s \in \mathbb{N}^0$ tal que $n + s \equiv 0 \mod r$. Então existe $k \in \mathbb{N}$ tal que $n+s = kr$. Logo $(a^{n+s})^2 = a^{n+n+s+s} = a^{n+kr+s} = a^{n+kr}a^s = a^n a^s = a^{n+s}$. Portanto $a^{n+s} \in E(S)$. ■

Corolário 2.1. *Todo semigrupo finito contém um idempotente.*

Demonstração. Seja S um semigrupo finito. Note que para todo $a \in S$, $\langle a \rangle \subseteq S$ é finito. Logo $\langle a \rangle$ contém idempotente e, consequentemente, S contém idempotente. ■

Proposição 2.20. *Sejam S um semigrupo e $a \in S$. Se $\langle a \rangle$ é finito em que $n, r \in \mathbb{N}$ são o índice e o período do elemento a respectivamente, então K_a é um subgrupo cíclico de $\langle a \rangle$*

(i) com identidade a^{n+s} em que $0 \leq s < r$ e $n + s \equiv 0 \mod r$; e

(ii) gerado pelo elemento a^{n+g} em que $0 \leq g < r$ e $n+g \equiv 1 \mod r$.

Demonstração. Primeiramente, observe que de acordo com a demonstração da Proposição 2.18, pelo algorítimo de Euclides, temos que $K_a = \{a^n, a^{n+1}, \ldots, a^{n+r-1}\}$ é um conjunto fechado para a operação binária do semigrupo S. Como $K_a \subseteq S$, segue que os elementos de K_a são associativos. Logo K_a é um semigrupo.

Além disso, sendo $0 \leq s < r$ e $n + s \equiv 0 \mod r$, temos que existe existe $k \in \mathbb{N}$ tal que $s + n = kr$. Tome $b \in K_a$, então existe $u \in \mathbb{N}^0$, $0 \leq u < r$ tal que $b = a^{n+u}$, segue daí que

$$\begin{aligned} ba^{n+s} &= a^{n+u}a^{n+s} \\ &= a^{n+n+s+u} \\ &= a^{n+kr+u} \\ &= a^{n+u} \\ &= b \end{aligned}$$

e, analogamente, $a^{n+s}b = b$, logo a^{n+s} é um elemento identidade para K_a. Assim K_a é um monoide.

Note que para qualquer $a^{n+u} \in K_a$ com $u \in \mathbb{N}^0$, $0 \leq u < r$ existe $a^{n+v} \in K_a$ com $v \in \mathbb{N}^0$, $0 \leq v < r$ tal que $v \equiv s - n - u \mod r$ que é elemento inverso de a^{n+u}, ou seja,

$$\begin{aligned} a^{n+u}a^{n+v} &= a^{n+u+n+v} \\ &= a^{n+v+n+u} \\ &= a^{n+v}a^{n+u} \\ &= a^{n+s} \end{aligned}$$

De fato, sendo $v \equiv s - n - u \mod r$ então

$$r|v - (s - n - u) \Rightarrow r|n + u + v - s$$

logo existe $q \in \mathbb{N}^0$ tal que $n + u + v - s = qr$ e assim

$$\begin{aligned} n + u + v = s + qr &\Rightarrow n + n + u + v = n + s + qr \\ &\Rightarrow n + u + n + v = n + s + qr \end{aligned}$$

e consequentemente

$$\begin{aligned} a^{n+u}a^{n+v} &= a^{n+u+n+v} \\ &= a^{n+s+qr} \\ &= a^{n+qr+s} \\ &= a^{n+qr}a^{s} \\ &= a^{n}a^{s} \\ &= a^{n+s} \end{aligned}$$

Portanto K_a é um grupo.

Por fim, provaremos que o grupo K_a é cíclico. Afim de provar isto observe que existe $g \in \mathbb{N}^0$ tal que $0 \leq g < r$ e $n + g \equiv 1 \mod r$ e, consequentemente, existe $q \in \mathbb{N}$ tal que $n + g = 1 + qr$. Daí para todo $k \in \mathbb{N}$ com $1 \leq k \leq r$ temos

$$\begin{aligned} (a^{n+g})^{k} &= a^{k(n+g)} \\ &= a^{n+g+(k-1)(n+g)} \\ &= a^{n+g+(k-1)(1+qr)} \\ &= a^{n+g+(k-1)+(k-1)qr} \\ &= a^{n+(k-1)qr+g+(k-1)} \\ &= a^{n+(k-1)qr}a^{g+(k-1)} \\ &= a^{n}a^{g+(k-1)} \\ &= a^{n+g+(k-1)} \\ &= a^{n+(g+k-1)} \end{aligned}$$

Como $0 \leq g < r$ e $1 \leq k \leq r$ então $0 \leq g + k - 1 < 2r$. Como K_a tem ordem r e k varia entre os naturais 1 e r, temos que cada valor diferente de k neste intervalo deve corresponder a um diferente elemento de K_a e com isso podemos concluir que cada potencia k de a^{n+g} corresponde biunivocamente a um elemento de K_a. Consequentemente conclui-se

que a^{n+g} gera K_a e portanto é cíclico. De fato, para cada k que faz $0 \leq g+k-1 < r$ temos $(a^{n+g})^k = a^{n+(g+k-1)}$ um elemento distinto de K_a; e para cada k que faz $r \leq g+k-1 < 2r$ temos que $g+k-1 = r+p$ para algum $p \in \mathbb{N}$ com $0 \leq p < r$ e daí

$$\begin{aligned}(a^{n+g})^k &= a^{n+(g+k-1)} \\ &= a^{n+(r+p)} \\ &= a^{n+r}a^p \\ &= a^{n+p}\end{aligned}$$

também é um elemento distinto de K_a. Portanto $\langle a^{n+g} \rangle = K_a$. ■

Observação 2.7. Sejam S um semigrupo e $a \in S$. Note que se a tem índice igual a 1 e período r então $\langle a \rangle$ é um subgrupo cíclico finito de ordem r de S.

Extraímos (com algumas adaptações) o seguinte exemplo de Howie [5, p. 11-12].

Exemplo 2.13. Considere o elemento

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 5 \end{pmatrix}$$

de $\mathcal{T}_7$, então temos que

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 5 & 6 \end{pmatrix}, \quad \alpha^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 5 & 6 & 7 \end{pmatrix},$$

$$\alpha^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 5 & 6 & 7 & 5 \end{pmatrix}, \quad \alpha^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 5 & 6 & 7 & 5 & 6 \end{pmatrix},$$

$$\alpha^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 6 & 7 & 5 & 6 & 7 \end{pmatrix}, \quad \alpha^7 = \alpha^4.$$

e então α tem índice 4 e período 3. Assim $K_\alpha = \{\alpha^4, \alpha^5, \alpha^6\}$ tem a tabela de Cayley conforme é exibida na Tabela 5.

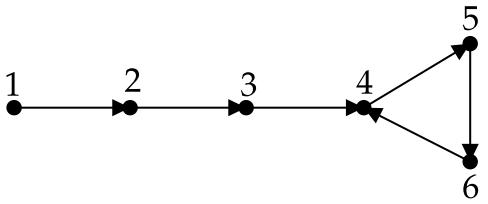
Tabela 5 – Tabela de Cayley do grupo cíclico K_α

	α^4	α^5	α^6
α^4	α^5	α^6	α^4
α^5	α^6	α^4	α^5
α^6	α^4	α^5	α^6

De acordo com o item (i) da Proposição 2.20, α^6 é o elemento identidade do grupo cíclico K_α, uma vez que $6 = 4 + 2 \equiv 0 \mod 3$. Ainda, pelo item (ii) da Proposição 2.20, α^4 gera K_α, uma vez que $4 = 4 + 0 \equiv 1 \mod 3$: $(\alpha^4)^2 = \alpha^5$, $(\alpha^4)^3 = \alpha^6$.

A representação gráfica de $\langle\alpha\rangle$ pode ser observada na Figura 3.

Figura 3 – Representação gráfica do subsemigrupo monogênico $\langle\alpha\rangle$



No que foi exposto até aqui, não fica claro se para todo par ordenado $(n, r) \in \mathbb{N} \times \mathbb{N}$ existe algum subsemigrupo monogênico finito com índice n e período r. No entanto isso de fato ocorre. Basta verificar que para quaisquer que sejam os naturais n e r podemos tomar o

elemento

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & \dots & n+r-1 & n+r \\ 2 & 3 & 4 & \dots & n+1 & n+2 & \dots & n+r & n+1 \end{pmatrix} \in \mathcal{T}_{n+r}$$

tal que $\langle a \rangle$ é um subsemigrupo monogênico finito de $\mathcal{T}_{n+r}$ gerado por a com índice n e período r. Note que para todo $k, m \in \mathbb{N}$ com $1 \leq m \leq n+r$ temos

$$a^k(m) = \begin{cases} m+k, & \text{se } m+k \leq n+1 \\ n+1+t, & \text{com } 0 \leq t < r,\ m+k+t \equiv n+1 \mod r \end{cases}$$

daí é possível verificar que os todos os subitens do item (ii) da Proposição 2.18 ocorrem.

Proposição 2.21. *Sejam S e T semigrupos quaisquer. Sejam a e b elementos de ordem finita de S e T, respectivamente, tais que $O(a) = O(b)$. Segue que $\langle a \rangle \cong \langle b \rangle$ se, e somente se, a e b têm os mesmos índices e períodos.*

Demonstração. Sejam S e T semigrupos quaisquer. Tome $a \in S$ e $b \in T$. Suponha que a e b sejam elementos de ordem finita tais que $O(a) = O(b)$. Sejam $n, r \in \mathbb{N}$ índice e período de a e $m, s \in \mathbb{N}$ índice e período de b. Logo $n + r = m + s$.

Suponha que $\langle a \rangle \cong \langle b \rangle$, logo existe um isomorfismo ϕ entre $\langle a \rangle$ e $\langle b \rangle$. Segue que para todo $k \in \mathbb{N}$, $\phi(a^k) = \phi(a)^k$. Analisaremos agora dois casos possíveis: $m > 1$ ou $m = 1$

Tome $m > 1$ e suponha, por absurdo, que $\phi(a) \neq b$. Logo existe $u \in \mathcal{N}$, tal que $1 < u < m + s$ tal que $\phi(a) = b^u$, consequentemente para todo $k \in \mathbb{N}$, $\phi(a^k) = \phi(a)^k = (b^u)^k \neq b$ (pois o índice de b é maior que 1), implicando que $b \notin \operatorname{Im}\phi$ e assim $\operatorname{Im}\phi \neq \langle b \rangle$. O que contradiz o fato de $\operatorname{Im}\phi$ ser sobrejetiva. Logo $\phi(a) = b$, consequentemente para todo $k \in \mathbb{N}$, $\phi(a^k) = \phi(a)^k = b^k$. Logo $a^n = a^{n+r}$, implica que

$\phi(a^n) = \phi(a^{n+r})$, daí $\phi(a)^n = \phi(a)^{n+r}$, assim $b^n = b^{n+r}$ e portanto $m = n$ e $s = r$.

Caso $m = 1$, então $\langle b\rangle$ é um grupo cíclico finito de ordem $O(b) = s$. Como existe um isomorfismo entre $\langle a\rangle$ e $\langle b\rangle$ então $\langle a\rangle$ também é um grupo cíclico finito de ordem $O(a) = s$. Portanto $n = 1$ e $r = s$.

Reciprocamente, suponha que $m = n$ e $s = r$. Logo

$$\langle a\rangle = \{a, a^2, \ldots, a^n, \ldots, a^{n+r-1}\}$$

e

$$\langle b\rangle = \{b, b^2, \ldots, b^n, \ldots, b^{n+r-1}\}$$

Daí note que a função $\phi : \langle a\rangle \longrightarrow \langle b\rangle$ dada por $\phi(a^i) = b^i$ para todo $i \in \mathbb{N}$ é um isomorfismo. Portanto $\langle a\rangle \cong \langle b\rangle$. ■

Como consequência da Proposição 2.21 acima e o que foi mencionado no paragrafo anterior, temos que, a menos de isomorfismos, para cada par ordenado $(n, r) \in \mathbb{N} \times \mathbb{N}$ existe exatamente um semigrupo monogênico finito de índice n e período r.

Notação 2.1. Denotamos o semigrupo monogênico finito de índice n e período r por $M(n, r)$.

Definição 2.30. Um semigrupo é chamado de *periódico* se todos os seus elementos têm ordem finita.

Obviamente, todo semigrupo finito é periódico. Vimos no Corolário 2.1 que todo semigrupo finito contém um idempotente. Na seguinte proposição provaremos que todo semigrupo periódico contém um idempotente.

Proposição 2.22. *Em um semigrupo periódico, todo elemento tem uma potência que é idempotente. Consequentemente todo semigrupo periódico contém ao menos um idempotente.*

Demonstração. Seja S um semigrupo periódico. Note que para todo $a \in S$, $\langle a \rangle \subseteq S$ é finito. Logo $\langle a \rangle$ contém idempotente que é a identidade de K_a. Consequentemente $a \in S$ tem uma potência que é idempotente e portanto S contém ao menos um idempotente. ■

2.8 RELAÇÕES BINÁRIAS

Nesta seção abordaremos o conceito de relação binária e sua conexão com semigrupos.

Definição 2.31. Seja X um conjunto, chamamos de *relação binária em* X um subconjunto do produto cartesiano $X \times X$. Seja ρ uma relação binária em X. Se $(x, y) \in \rho$, então dizemos que x *é* ρ*-relacionado a* y e escrevemos $x \rho y$. Se $(x, y) \notin \rho$, então dizemos que x *não é* ρ*-relacionado a* y e escrevemos $x \not\rho y$.

Note que $\emptyset \subseteq X \times X$, logo $\emptyset$ é uma relação binária em X. O produto cartesiano $X \times X$ é uma relação binária em X conhecida como *relação binária universal em* X. Já $I_X = \{(x, x); x \in X\} \subseteq X \times X$ é uma relação binária em X conhecida como *relação binária diagonal em* X (adiante veremos que esta notação não causa confusão com a usada para representar a função identidade em X mencionada na Seção 2.5).

Notação 2.2. Denotaremos o conjunto de todas as relações binárias em um conjunto X por $\mathcal{B}_X$.

Definição 2.32. Definimos a operação binária $\circ$ em $\mathcal{B}_X$, chamada de *composição de relações binárias*, dada pela regra em que para todo $\rho, \sigma \in \mathcal{B}_X$ temos

$$\rho \circ \sigma = \{(x, y) \in X \times X; (\exists z \in X)(x, z) \in \sigma, (z, y) \in \rho\} \qquad (9)$$

A Definição 2.32 está um pouco diferente da definição encontrada em Howie [5, p. 16]. Fizemos esta alteração pois resolvemos denotar a imagem de um elemento x de um conjunto X, sob uma função f em X por $f(x)$, enquanto que Howie [5, p. 1] e Clifford e Preston [1, p. 1] usam a notação xf. Assim, se mantivéssemos a definição como escrita por Howie [5, p. 16], teríamos problemas para demonstrar a Proposição 2.28. Dito isso, tomamos o cuidado de adaptar também todos os resultados que dependem dessa definição.

Proposição 2.23. *Seja X um conjunto qualquer, então para todo $\rho, \sigma, \tau \in \mathcal{B}_X$, temos que $\rho \subseteq \sigma$ implica em $\rho \circ \tau \subseteq \sigma \circ \tau$ e $\tau \circ \rho \subseteq \tau \circ \sigma$*

Demonstração. Sejam $\rho, \sigma, \tau \in \mathcal{B}_X$. Suponha $\rho \subseteq \sigma$.

Tome $(x, y) \in \rho \circ \tau$, logo existe $z \in X$ tal que $(x, z) \in \tau$ e $(z, y) \in \rho$. Como $\rho \subseteq \sigma$ então $(z, y) \in \sigma$. Consequentemente $(x, y) \in \sigma \circ \tau$.

Analogamente, tome $(x, y) \in \tau \circ \rho$, logo existe $z \in X$ tal que $(x, z) \in \rho$ e $(z, y) \in \tau$. Como $\rho \subseteq \sigma$ então $(x, z) \in \sigma$. Consequentemente $(x, y) \in \tau \circ \sigma$. ■

Proposição 2.24. *Seja X um conjunto qualquer, então para todo $\rho, \sigma, \tau \in \mathcal{B}_X$, temos que $(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)$.*

Demonstração.

$$
\begin{aligned}
&(x, y) \in (\rho \circ \sigma) \circ \tau \\
&\quad \iff (\exists z \in X)(x, z) \in \tau \text{ e } (z, y) \in \rho \circ \sigma \\
&\quad \iff (\exists z \in X)(\exists u \in X)(x, z) \in \tau,\ (z, u) \in \sigma \text{ e } (u, y) \in \rho \\
&\quad \iff (\exists u \in X)(x, u) \in \sigma \circ \tau \text{ e } (u, y) \in \rho \\
&\quad \iff (x, y) \in \rho \circ (\sigma \circ \tau)
\end{aligned}
$$

■

Com a Proposição 2.24, provamos que munido da composição de relações binárias, o conjunto $\mathcal{B}_X$ é associativo, e, pela Equação (9) temos que para todo $\rho, \sigma \in \mathcal{B}_X$, $\rho \circ \sigma \in \mathcal{B}_X$, ou seja, $\mathcal{B}_X$ é um conjunto fechado para a composição de relações binárias, e, portanto

Proposição 2.25. $(\mathcal{B}_X, \circ)$ *é um semigrupo.*

Na Seção 2.5, definimos o monoide de transformação completa em um conjunto X denotado por $\mathcal{T}_X$. Caso $X = \{x_1, x_2, \ldots, x_n\}$ é um conjunto finito com n elementos, então podemos denotar $\beta \in \mathcal{T}_X$ por

$$\beta = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \beta(x_1) & \beta(x_2) & \ldots & \beta(x_n) \end{pmatrix}.$$

Podemos usar uma notação semelhante para escrever os elementos de $\mathcal{B}_X$. Nesse caso, denotamos $\delta \in \mathcal{B}_X$ com δ possuindo k elementos por

$$\delta = \begin{pmatrix} x_{n_1} & x_{n_2} & \ldots & x_{n_k} \\ y_{n_1} & y_{n_2} & \ldots & y_{n_k} \end{pmatrix}$$

em que $(x_{n_i}, y_{n_i}) \in \delta$.

Definição 2.33. Seja $\rho \in \mathcal{B}_X$. Chamamos de *domínio de* ρ o conjunto

$$\operatorname{dom} \rho = \{x \in X; (\exists y \in X)(x, y) \in \rho\} \tag{10}$$

Chamamos de *imagem de* ρ o conjunto

$$\operatorname{im} \rho = \{y \in X; (\exists x \in X)(x, y) \in \rho\} \tag{11}$$

Imediatamente observa-se que, para todo $\rho, \sigma \in \mathcal{B}_X$, $\rho \subseteq \sigma$ implica em $\operatorname{dom} \rho \subseteq \operatorname{dom} \sigma$ e $\operatorname{im} \rho \subseteq \operatorname{im} \sigma$.

Definição 2.34. Para cada elemento x do conjunto X e $\rho \in \mathcal{B}_X$, definimos um subconjunto $\rho(x)$ de X por

$$\rho(x) = \{y \in X; (x, y) \in \rho\} \tag{12}$$

Se A é um subconjunto de X, então definimos

$$\rho(A) = \bigcup_{a \in A} \rho(a) \tag{13}$$

Definição 2.35. Para todo $\rho \in \mathcal{B}_X$ definimos a *relação inversa de* ρ por

$$\rho^{-1} = \{(y, x) \in X \times X; (x, y) \in \rho\} \tag{14}$$

Certamente $\rho^{-1} \in \mathcal{B}_X$. Sejam $\rho, \sigma, \rho_1, \rho_2, \ldots, \rho_n \in \mathcal{B}_X$ e $x \in X$, então as seguintes propriedades são facilmente verificadas

$$(\rho^{-1})^{-1} = \rho \tag{15}$$

$$(\rho_1 \circ \rho_2 \circ \ldots \circ \rho_n)^{-1} = \rho_n^{-1} \circ \ldots \circ \rho_2^{-1} \circ \rho_1^{-1} \tag{16}$$

$$\rho \subseteq \sigma \Rightarrow \rho^{-1} \subseteq \sigma^{-1} \tag{17}$$

$$\operatorname{dom}(\rho^{-1}) = \operatorname{im} \rho \tag{18}$$

$$\operatorname{im}(\rho^{-1}) = \operatorname{dom} \rho \tag{19}$$

$$\rho(x) \neq \emptyset \iff x \in \operatorname{dom} \rho \tag{20}$$

$$\rho^{-1}(x) \neq \emptyset \iff x \in \operatorname{im} \rho \tag{21}$$

Definição 2.36. Um elemento $\phi \in \mathcal{B}_X$ é chamado de uma *transformação parcial de* X se para todo $x \in \operatorname{dom} \phi$, $|\phi(x)| = 1$. Isto é, se, para todo $x, y_1, y_2 \in X$, $(x, y_1) \in \phi$ e $(x, y_2) \in \phi$ implicam em $y_1 = y_2$.

Notação 2.3. Denotaremos o conjunto de todas as transformações parciais de em um conjunto X por $\mathcal{P}_X$.

Note que $\mathcal{P}_X$ é um subconjunto de $\mathcal{B}_X$. Se $\phi \in \mathcal{P}_X$ com $(x, y) \in \phi$, então, obviamente, $\phi(x) = \{y\}$. Neste caso podemos escrever $\phi(x) = y$ para denotar o único elemento que está relacionado a x.

Definição 2.37. Sejam $\phi, \psi \in \mathcal{P}_X$ tais que $\phi \subseteq \psi$. Dizemos, daí, que ϕ é uma *restrição* de ψ ou que ψ é uma *extensão* de ϕ. Nestas circunstancias temos que $\operatorname{dom}\phi = A \subseteq \operatorname{dom}\psi$. Daí denotamos ϕ por $\psi|_A$ (lê-se: ψ *restrito a* A).

Proposição 2.26. $(\mathcal{P}_X, \circ)$ *é um subsemigrupo de* $(\mathcal{B}_X, \circ)$.

Demonstração. Sejam $\phi, \psi \in \mathcal{P}_X$, e suponha que $(x, y_1), (x, y_2) \in \phi\circ\psi$. Então existem $z_1, z_2 \in X$ tais que $(x, z_1) \in \psi$, $(z_1, y_1) \in \phi$, $(x, z_2) \in \psi$, $(z_2, y_2) \in \phi$. Daí, pela definição Definição 2.36 em ψ segue que $z_1 = z_2$, e pela mesma definição em ϕ temos que $y_1 = y_2$. Logo $\phi \circ \psi \in \mathcal{P}_X$. ■

Em vista da Proposição 2.26 acima podemos dizer que $(\mathcal{P}_X, \circ)$ é um semigrupo, o qual recebe o nome de *semigrupo das transformações parciais de* X. É importante observarmos que $\phi \in \mathcal{P}_X$ não implica que $\phi^{-1} \in \mathcal{P}_X$. Por exemplo, se $X = \{1, 2\}$, então $\phi = \{(1, 1), (2, 1)\}$ é uma transformação parcial de X, mas ϕ^{-1} não é.

As duas proposições seguintes mostram alguns resultados relacionados a composição de relações binárias $\circ$ nos conjuntos $\mathcal{B}_X$ e $\mathcal{P}_X$.

Proposição 2.27. *Se* $\phi, \psi \in \mathcal{B}_X$, *então*

(i) $\operatorname{dom}(\phi \circ \psi) = \psi^{-1}(\operatorname{dom}\phi \cap \operatorname{im}\psi)$

(ii) $\operatorname{im}(\phi \circ \psi) = \phi(\operatorname{dom}\phi \cap \operatorname{im}\psi)$

Demonstração. Vamos primeiramente demonstrar o item (i). Para isso mostraremos que $\operatorname{dom}(\phi\circ\psi) \subseteq \psi^{-1}(\operatorname{dom}\phi\cap\operatorname{im}\psi)$ e que $\psi^{-1}(\operatorname{dom}\phi\cap \operatorname{im}\psi) \subseteq \operatorname{dom}(\phi \circ \psi)$.

Tome $x \in \mathrm{dom}(\phi \circ \psi)$, então existe $y \in X$ tal que $(x, y) \in \phi \circ \psi$. Logo existe $z \in X$ tal que $(x, z) \in \psi$ e $(z, y) \in \phi$. Assim $z \in \mathrm{im}\,\psi$ e $z \in \mathrm{dom}\,\phi$, isto é, $z \in \mathrm{dom}\,\phi \cap \mathrm{im}\,\psi$. Como $(x, z) \in \psi$, então $(z, x) \in \psi^{-1}$, e então $x \in \psi^{-1}(z) \subseteq \psi^{-1}(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$. Logo $\mathrm{dom}(\phi \circ \psi) \subseteq \psi^{-1}(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$.

Tome, agora, $x \in \psi^{-1}(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$, então existe $z \in \mathrm{dom}\,\phi \cap \mathrm{im}\,\psi$ tal que $x \in \psi^{-1}(z)$, isto é, $(z, x) \in \psi^{-1}$, ou seja, $(x, z) \in \psi$. Como $z \in \mathrm{dom}\,\phi$, então existe $y \in X$ tal que $(z, y) \in \phi$. Consequentemente, $(x, y) \in \phi \circ \psi$, logo $x \in \mathrm{dom}(\phi \circ \psi)$. Portanto

$$\mathrm{dom}(\phi \circ \psi) = \psi^{-1}(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$$

Analogamente, demonstraremos o item (ii). Ou seja, mostraremos que $\mathrm{im}(\phi\circ\psi) \subseteq \phi(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$ e que $\phi(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi) \subseteq \mathrm{im}(\phi\circ\psi)$.

Tome $y \in \mathrm{im}(\phi \circ \psi)$, então existe $x \in X$ tal que $(x, y) \in \phi \circ \psi$. Logo existe $z \in X$ tal que $(x, z) \in \psi$ e $(z, y) \in \phi$. Assim $z \in \mathrm{im}\,\psi$ e $z \in \mathrm{dom}\,\phi$, isto é, $z \in \mathrm{dom}\,\phi \cap \mathrm{im}\,\psi$. Como $(z, y) \in \phi$, então $y \in \phi(z) \subseteq \phi(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$. Logo $\mathrm{im}(\phi \circ \psi) \subseteq \phi(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$.

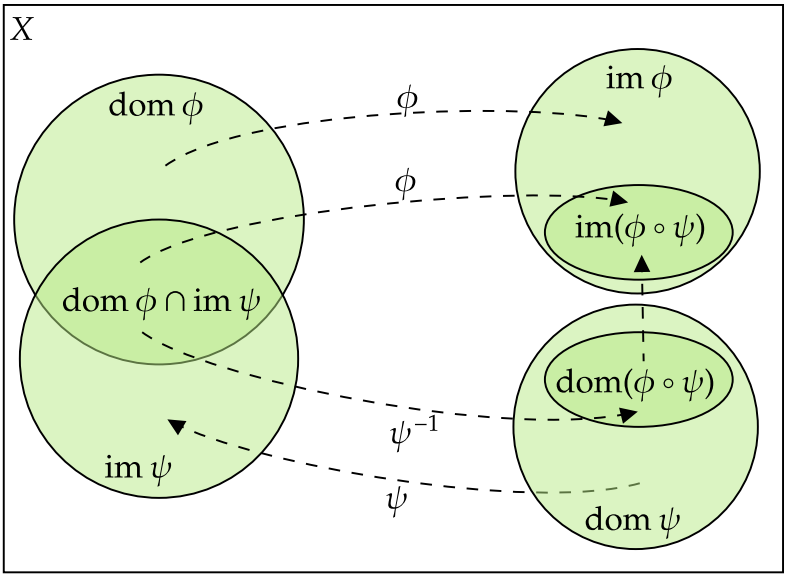
Tome, agora, $y \in \phi(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$, então existe $z \in \mathrm{dom}\,\phi \cap \mathrm{im}\,\psi$ tal que $y \in \phi(z)$, isto é, $(z, y) \in \phi$. Como $z \in \mathrm{im}\,\psi$, então existe $x \in X$ tal que $(x, z) \in \psi$. Consequentemente, $(x, y) \in \phi\circ\psi$, logo $y \in \mathrm{im}(\phi\circ\psi)$. Portanto

$$\mathrm{im}(\phi \circ \psi) = \phi(\mathrm{dom}\,\phi \cap \mathrm{im}\,\psi)$$

■

Esquematicamente, o resultado da Proposição 2.27 acima pode ser observado na Figura 4.

Figura 4 – Esquema da Proposição 2.27



Proposição 2.28. *Se $\phi, \psi \in \mathcal{P}_X$, então para todo $x \in \text{dom}(\phi \circ \psi)$ temos $\phi \circ \psi(x) = \phi(\psi(x))$*

Demonstração. Sejam $\phi, \psi \in \mathcal{P}_X$. Tome $x \in \text{dom}(\phi \circ \psi)$, então existe $y \in X$ tal que $(x, y) \in \phi \circ \psi$, logo existe $z \in X$ tal que $(x, z) \in \psi$ e $(z, y) \in \phi$. Como $\phi, \psi \in \mathcal{P}_X$, então, pela Proposição 2.26, $\phi \circ \psi \in \mathcal{P}_X$ e, consequentemente, $\phi \circ \psi(x) = y$. Mas, também temos que $\psi(x) = z$ e $\phi(z) = y$. Portanto $\phi(\psi(x)) = y$, ou seja, $\phi \circ \psi(x) = \phi(\psi(x))$. ■

Definição 2.38. Dizemos que $\phi \in \mathcal{P}_X$ é uma *função em X*, se $\text{dom}\,\phi = X$. Em outras palavras, uma transformação parcial em X é uma função em X se, e somente se, para todo $x \in X$, $|\phi(x)| = 1$.

Note que o conjunto $\mathcal{T}_X$ mencionado na Seção 2.5 é um subconjunto de $\mathcal{P}_X$. De fato, os elementos de $\mathcal{T}_X$ são funções em X conforme a Definição 2.38. Ademais, de acordo com a Proposição 2.28, a composição de relações binárias na Definição 2.32 coincide com a composição de funções mencionado na Seção 2.5. Logo, se $\phi, \psi \in \mathcal{P}_X$ são funções em X, então $\phi \circ \psi$ também é uma função em X. Isso demonstra a seguinte proposição:

Proposição 2.29. $(\mathcal{T}_X, \circ)$ *é um subsemigrupo de* $(\mathcal{P}_X, \circ)$

Observe que a relação binária diagonal em X é, de fato, equivalente a função identidade em X. Tal relação binária, denotada por I_X, se comporta como uma identidade para os semigrupos $(\mathcal{T}_X, \circ)$, $(\mathcal{P}_X, \circ)$ e $(\mathcal{B}_X, \circ)$, portanto, estes semigrupos são também monoides e além disso $(\mathcal{T}_X, \circ)$ é um submonoide de $(\mathcal{P}_X, \circ)$ que é um submonoide de $(\mathcal{B}_X, \circ)$.

É importante destacar que $\phi \in \mathcal{P}_X$ não implica que $\phi^{-1} \in \mathcal{P}_X$. No entanto temos o seguinte resultado:

Proposição 2.30. *Seja X um conjunto não vazio.*

(i) Se $\phi \in \mathcal{P}_X$, então $\phi^{-1} \in \mathcal{P}_X$ se, e somente se, ϕ é injetiva.

(ii) Se $\phi \in \mathcal{T}_X$, então $\phi^{-1} \in \mathcal{T}_X$ se, e somente se, ϕ é bijetiva.

Demonstração. Primeiramente demonstraremos o item (i). Seja, daí, $\phi \in \mathcal{P}_X$.

Suponha $\phi^{-1} \in \mathcal{P}_X$, então $(\phi(x), x) \in \phi^{-1}$ $(\forall x \in \operatorname{dom}\phi)$, logo $\phi^{-1}(\phi(x)) = x$ $(\forall x \in \operatorname{dom}\phi)$. Tome, agora, $x_1, x_2 \in \operatorname{dom}\phi$ tais que $\phi(x_1) = \phi(x_2)$, então $x_1 = \phi^{-1}(\phi(x_1)) = \phi^{-1}(\phi(x_2)) = x_2$. Portanto ϕ é injetiva.

Reciprocamente, suponha que ϕ é injetiva. Tome $y, x_1, x_2 \in X$ tais que $(y, x_1), (y, x_2) \in \phi^{-1}$, logo $(x_1, y), (x_2, y) \in \phi$. Assim $\phi(x_1) = y = \phi(x_2)$. Como ϕ é injetiva, então $x_1 = x_2$. Portanto $\phi^{-1} \in \mathcal{P}_X$

Agora demonstraremos o item (ii). Seja, daí, $\phi \in \mathcal{T}_X$.

Suponha $\phi^{-1} \in \mathcal{T}_X$, então $(\phi(x), x) \in \phi^{-1}$ $(\forall x \in X)$, logo $\phi^{-1}(\phi(x)) = x$ $(\forall x \in X)$. Tome, agora, $x_1, x_2 \in X$ tais que $\phi(x_1) = \phi(x_2)$, então $x_1 = \phi^{-1}(\phi(x_1)) = \phi^{-1}(\phi(x_2)) = x_2$. Portanto ϕ é injetiva.

Note que $\operatorname{im}\phi \subseteq X$ é imediato. Por outro lado, tome $y \in \operatorname{dom}\phi^{-1} = X$, logo existe $x \in X$ tal que $\phi^{-1}(y) = x$, então $(y, x) \in \phi^{-1}$, logo $(x, y) \in (\phi^{-1})^{-1} = \phi$, daí $\phi(x) = y$, ou seja, $y \in \operatorname{im}\phi$. Assim $X \subseteq \operatorname{im}\phi$. Logo $X = \operatorname{im}\phi$ o que implica que ϕ é sobrejetiva. Portanto ϕ é bijetiva.

Reciprocamente, suponha que ϕ é bijetiva. Tome $y, x_1, x_2 \in X$ tais que $(y, x_1), (y, x_2) \in \phi^{-1}$, logo $(x_1, y), (x_2, y) \in \phi$. Assim $\phi(x_1) = y = \phi(x_2)$. Como ϕ é bijetiva, é em particular injetiva, então $x_1 = x_2$. Portanto $\phi^{-1} \in \mathcal{T}_X$ ■

2.9 RELAÇÕES DE EQUIVALÊNCIA E SEMIGRUPO QUOCIENTE

Na seção anterior vimos que uma relação binária em um conjunto qualquer munido da operação de composição de relações binárias é um semigrupo. Nesta seção estudaremos um tipo especial de relação binária conhecida como *relação de equivalência*. Veremos que ela é fundamental para a construção do *semigrupo quociente*.

Definição 2.39. Seja $\rho \in \mathcal{B}_X$, dizemos que a relação binária ρ é

(i) *reflexiva* se para todo $a \in X$, $(a, a) \in \rho$, ou seja, se $I_X \subseteq \rho$;

(ii) *simétrica* se para todo $a, b \in X$, $(a, b) \in \rho$ implica em $(b, a) \in \rho$, ou seja, se $\rho \subseteq \rho^{-1}$;

(iii) *antissimétrica* se para todo $a, b \in X$, $(a, b), (b, a) \in \rho$ implica em $a = b$, ou seja, se $\rho \cap \rho^{-1} \subseteq I_X$;

(iv) *transitiva* se para todo $a, b, c \in X$, $(a, b), (b, c) \in \rho$ implica em $(a, c) \in \rho$, ou seja, se $\rho \circ \rho \subseteq \rho$.

Definição 2.40. Seja $\rho \in \mathcal{B}_X$, dizemos que a relação binária ρ é uma *relação de equivalência* se é reflexiva, simétrica e transitiva.

Note que se ρ é uma relação binária simétrica, então $\rho \subseteq \rho^{-1}$. Mas como $\rho \subseteq \rho^{-1} \Rightarrow \rho^{-1} \subseteq (\rho^{-1})^{-1} = \rho$, então a propriedade simétrica pode ser expressa por $\rho = \rho^{-1}$. Do mesmo modo, se ρ é uma relação de equivalência em X, então podemos deduzir, pela Proposição 2.23, que $\rho = I_X \circ \rho \subseteq \rho \circ \rho$, logo a propriedade transitiva pode ser expressa por $\rho = \rho \circ \rho$. Além disso, sendo ρ uma relação de equivalência em X, tem-se que $\operatorname{dom} \rho \supseteq \operatorname{dom} I_X = X$, $\operatorname{im} \rho \supseteq \operatorname{im} I_X = X$ e consequentemente $\operatorname{dom} \rho = \operatorname{im} \rho = X$.

Definição 2.41. Dizemos que uma família $\pi = \{A_i; i \in I\}$ de subconjuntos de um conjunto X forma uma *partição de* X se

(i) cada A_i é não vazio ($A_i \neq \emptyset \ \ (\forall i \in I)$);

(ii) para todo $i, j \in I$ ou $A_i = A_j$ ou $A_i \cap A_j = \emptyset$;

(iii) $\bigcup_{i \in I} A_i = X$.

Em vista disso, nota-se que as noções de equivalência (da Definição 2.40) e de partição (da Definição 2.41) são bastante diferentes, no entanto, podemos ver que, de acordo com a proposição a seguir, elas estão intimamente relacionadas.

Proposição 2.31. *Seja X um conjunto não vazio, segue que*

i. Se ρ é uma relação de equivalência em X, então a família $\Phi(\rho) = \{\rho(x); x \in X\}$ de subconjuntos de X é uma partição de X.

ii. Reciprocamente, se $\pi = \{A_i; i \in I\}$ *é uma partição de* X*, então a relação binária* $\Psi(\pi) = \{(x, y) \in X \times X; (\exists i \in I) \;\; x, y \in A_i\}$ *é uma relação de equivalência em* X*.*

iii. Para toda relação de equivalência ρ *em* X*,* $\Psi(\Phi(\rho)) = \rho$*, e para toda partição* π *de* X*,* $\Phi(\Psi(\pi)) = \pi$*.*

Demonstração. A demonstração pode ser encontrada em Domingues e Iezzi [2, p. 83]. ■

Definição 2.42. Sejam X um conjunto, ρ uma relação de equivalência em X e $x \in X$. Chamamos o conjunto $\rho(x)$ de *classe de equivalência* ρ *de* x (ou ρ*-classe de* x). Nesse caso, escrevemos ρ_x para denotar o conjunto $\rho(x)$.

O seguinte resultado nos fornece uma relação alternativa para verificar se duas classes de equivalência são iguais.

Proposição 2.32. *Seja* ρ *uma relação de equivalência em um conjunto* X *e* $a, u \in X$*. Então* $\rho_a = \rho_u$ *se, e somente se,* $u \in \rho_a$

Demonstração. Primeiramente, suponha que $\rho_a = \rho_u$, então existe $x \in X$ tal que $(a, x), (u, x) \in \rho$. Logo $(x, u) \in \rho$ por simetria e, consequentemente, $(a, u) \in \rho$ por transitividade, ou seja, $u \in \rho_a$.

Reciprocamente, suponha $u \in \rho_a$, ou seja $(a, u) \in \rho$. Segue que $(u, a) \in \rho$ por simetria. Tome, daí, $v \in \rho_a$, então $(a, v) \in \rho$, e, consequentemente, $(u, v) \in \rho$ por transitividade, ou seja, $v \in \rho_u$. Logo $\rho_a \subseteq \rho_u$. Analogamente, prova-se que $\rho_u \subseteq \rho_a$. Portanto $\rho_a = \rho_u$. ■

Definição 2.43. Sejam X um conjunto e ρ uma relação de equivalência em X. Chamamos de *conjunto quociente de* X *por* ρ o conjunto cujos elementos são classes de equivalências ρ de elementos em X. Denotamos tal conjunto por X/ρ, ou seja

$$X/\rho = \{\rho_x; x \in X\}$$

De acordo com o item i. da Proposição 2.31, temos que X/ρ definido em 2.42 forma uma partição do conjunto X.

Definição 2.44. Sejam X, Y conjuntos e $\alpha : X \longrightarrow Y$ uma função. Chamamos de *kernel de* α a relação binária $\ker\alpha$ em X dada por

$$\ker\alpha = \{(a,b) \in X \times X; \alpha(a) = \alpha(b)\}$$

Observação 2.8. Claramente $\ker\alpha$ é uma relação de equivalência em X. Além disso, note que $\ker\alpha = \alpha^{-1} \circ \alpha$. De fato,

$$\begin{aligned}
\alpha^{-1} \circ \alpha &= \{(a,b) \in X \times X;\ (\exists t \in X)\ (a,t) \in \alpha, (t,b) \in \alpha^{-1}\} \\
&= \{(a,b) \in X \times X;\ (\exists t \in X)\ (a,t) \in \alpha, (b,t) \in \alpha\} \\
&= \{(a,b) \in X \times X;\ (\exists t \in X)\ \alpha(a) = t = \alpha(b)\} \\
&= \{(a,b) \in X \times X;\ \alpha(a) = \alpha(b)\} \\
&= \ker\alpha
\end{aligned}$$

Exemplo 2.14. Seja $\alpha : \{1,2,3,4,5,6\} \longrightarrow \{a,b,c,d\}$ dada por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ c & b & c & b & a \end{pmatrix}$$

então

$$\ker\alpha = \{(1,1),(1,3),(3,3),(3,1),(2,2),(2,4),(4,2),(4,4),(5,5)\}$$

Se $\rho, \lambda \in \mathcal{B}_X$ são relações de equivalência, então podemos facilmente provar que $\rho \cap \lambda$ também é uma relação de equivalência. Ademais, indutivamente, prova-se que se $\pi = \{\rho_i; i \in I\}$ é uma família de relações de equivalência em um conjunto X, então $\bigcap_{i\in I} \rho_i$ também é uma relação de equivalência em X. Porém o mesmo não é válido para as relações binárias $\rho \cup \lambda$ e $\rho \circ \lambda$, isto é, o fato de ρ e λ serem relações de equivalência, não implica, necessariamente, que $\rho \cup \lambda$ e $\rho \circ \lambda$ também o sejam.

Exemplo 2.15. Seja $X = \{1, 2, 3\}$. Note que

$$\rho = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$$

e

$$\lambda = \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$$

são relações de equivalência em X, mas $\rho \circ \lambda$ (que neste exemplo é igual a $\rho \cup \lambda$) não é transitiva, logo não é relação de equivalência. De fato, $(2,1)$ e $(1,3)$ são elementos de $\rho \circ \lambda = \rho \cup \lambda$, mas $(2,3)$ não é.

No entanto, podemos ter que $\rho \circ \lambda$ é uma relação de equivalência, se ρ e λ forem relações de equivalência com $\rho \circ \lambda = \lambda \circ \rho$. Conforme enunciado e provado na seguinte proposição:

Proposição 2.33. *Sejam $\rho, \lambda \in \mathcal{B}_X$ relações de equivalência com $\rho \circ \lambda = \lambda \circ \rho$, então $\rho \circ \lambda$ é uma relação de equivalência. Além disso, $\rho \circ \lambda$ é a menor relação de equivalência contendo $\rho \cup \lambda$.*

Demonstração. Seja $\phi = \rho \circ \lambda = \lambda \circ \rho$. Daí

$$\begin{aligned} \phi &= \{(x,y) \in X \times X;\ (\exists z \in X)\ (x,z) \in \lambda, (z,y) \in \rho\} \\ &= \{(x,y) \in X \times X;\ (\exists z \in X)\ (x,z) \in \rho, (z,y) \in \lambda\} \end{aligned}$$

Vamos, primeiro, provar que ϕ é uma relação de equivalência, ou seja, que é uma relação binária reflexiva, simétrica e transitiva.

Como ρ e λ são reflexivos, segue que para todo $a \in X$, $(a,a) \in \rho$ e $(a,a) \in \lambda$, logo existe $a \in X$ tal que $(a,a) \in \rho$ e $(a,a) \in \lambda$. Assim $(a,a) \in \lambda \circ \rho = \phi$. Daí para todo $a \in X$ temos $(a,a) \in \phi$. Portanto ϕ é reflexiva.

Tome $(a,b) \in \phi$. Como $\phi = \lambda \circ \rho$ então existe $c \in X$ tal que $(a,c) \in \rho$ e $(c,b) \in \lambda$. Como ρ e λ são simétricas, então $(c,a) \in \rho$ e $(b,c) \in \lambda$. Assim existe $c \in X$ tal que $(b,c) \in \lambda$ e $(c,a) \in \rho$, logo $(b,a) \in \rho \circ \lambda = \phi$. Portanto ϕ é simétrica.

Suponha que (a, b) e (b, c) sejam elementos de ϕ. Como $\phi = \lambda \circ \rho$, então existe $x \in X$ tal que $(a, x) \in \rho$ e $(x, b) \in \lambda$. Por outro lado, como $\phi = \rho \circ \lambda$, então existem $y \in X$ tal que $(b, y) \in \lambda$ e $(y, c) \in \rho$. Como λ é transitiva, então $(x, b) \in \lambda$ e $(b, y) \in \lambda$ implicam que $(x, y) \in \lambda$. Logo existe $y \in X$ tal que $(x, y) \in \lambda$ e $(y, c) \in \rho$. Assim $(x, c) \in \rho \circ \lambda = \phi$. Como $\phi = \lambda \circ \rho$, então existe $z \in X$ tal que $(x, z) \in \rho$ e $(z, c) \in \lambda$. Como ρ é transitiva, então $(a, x) \in \rho$ e $(x, z) \in \rho$ implicam que $(a, z) \in \rho$. Portanto existe $z \in X$ tal que $(a, z) \in \rho$ e $(z, c) \in \lambda$, ou seja $(a, c) \in \lambda \circ \rho = \phi$ e consequentemente ϕ é transitiva.

Agora vamos mostrar que $\rho \cup \lambda \subseteq \phi$. Para tanto vamos provar que $\rho \subseteq \phi$ e também que $\lambda \subseteq \phi$.

Tome $(a, b) \in \rho$. Como $(b, b) \in \lambda$ então existe $b \in X$ tal que $(a, b) \in \rho$ e $(b, b) \in \lambda$, logo $(a, b) \in \lambda \circ \rho = \phi$, logo $\rho \subseteq \phi$. E, de modo análogo, prova-se que $\lambda \subseteq \phi$.

Já provamos que $\rho \cup \lambda \subseteq \phi$, falta provar que é a menor relação que equivalência com esta propriedade. Para tanto, vamos tomar uma relação de equivalência τ qualquer com $\rho \cup \lambda \subseteq \tau$ e vamos concluir que $\phi \subseteq \tau$.

Tome $(a, b) \in \phi = \lambda \circ \rho$, então existe $c \in X$ tal que $(a, c) \in \rho$ e $(c, b) \in \lambda$. Como $\rho \subseteq \tau$ e, também, $\lambda \subseteq \tau$, então $(a, c), (c, b) \in \tau$. Como τ é transitiva, então $(a, b) \in \tau$, portanto $\phi \subseteq \tau$. ■

Até aqui, nessa seção, vimos relações binárias de equivalência em um conjunto X, mas ainda não relacionamos com o conceito de semigrupos. Para aproximar esses conceitos, usamos as definições de *compatibilidade* e *congruência* que seguem.

Definição 2.45. Sejam S um semigrupo e ρ uma relação binária em S. Dizemos que ρ é *compatível a esquerda (com a operação de S)* se para todo $a \in S$, $(s, t) \in \rho$ implica em $(as, at) \in \rho$. Neste caso, se ρ é

uma relação de equivalência, então dizemos que ρ é uma *congruência a esquerda*.

Definição 2.46. Sejam S um semigrupo e ρ uma relação binária em S. Dizemos que ρ é *compatível a direita (com a operação de S)* se para todo $a \in S$, $(s,t) \in \rho$ implica em $(sa,ta) \in \rho$. Neste caso, se ρ é uma relação de equivalência, então dizemos que ρ é uma *congruência a direita*.

Definição 2.47. Sejam S um semigrupo e ρ uma relação binária em S. Dizemos que ρ é *compatível (com a operação de S)* se para todo $(s,t),(u,v) \in \rho$ implica em $(su,tv) \in \rho$. Neste caso, se ρ é uma relação de equivalência, então dizemos que ρ é uma *congruência*.

Proposição 2.34. *Uma relação binária ρ em um semigrupo S é uma congruência se, e somente se, é simultaneamente uma congruência a esquerda e a direita.*

Demonstração. Suponha, primeiramente, que ρ é uma congruência. Se $(s,t) \in \rho$ e $a \in S$, então $(a,a) \in \rho$ pela propriedade reflexiva, logo $(as,at),(sa,ta) \in \rho$ pelo fato de ser compatível. Portanto ρ é simultaneamente compatível a esquerda e a direita, ou seja, é simultaneamente uma congruência a esquerda e a direita.

Reciprocamente, suponha que ρ é simultaneamente uma congruência a esquerda e a direita, e sejam $(s,t),(u,v) \in \rho$. Então $(su,tu) \in \rho$ por ser compatível a direita e $(tu,tv) \in \rho$ por ser compatível a esquerda. Consequentemente $(su,tv) \in \rho$ por transitividade. Portanto ρ é uma congruência. ■

Se ρ é uma congruência em um semigrupo S, podemos definir uma operação binária no conjunto quociente S/ρ dada por $\rho_a\rho_b = \rho_{ab}$, para todo $\rho_a, \rho_b \in S/\rho$. Note que tal operação está bem definida. De

fato, se $\rho_a = \rho_{a'}$ e $\rho_b = \rho_{b'}$, então $(a, a'), (b, b') \in \rho$ pela Proposição 2.32. Sendo ρ uma congruência em S, segue que $(ab, a'b') \in \rho$ e consequentemente $\rho_{ab} = \rho_{a'b'}$.

Tome, agora, $\rho_a, \rho_b, \rho_c \in S/\rho$. Então $\rho_a(\rho_b\rho_c) = \rho_a\rho_{bc} = \rho_{a(bc)} = \rho_{(ab)c} = \rho_{ab}\rho_c = (\rho_a\rho_b)\rho_c$. E, em particular, se S é um monoide com identidade 1, então $\rho_1\rho_a = \rho_{1a} = \rho_a = \rho_{a1} = \rho_a\rho_1$. Ou seja, sendo S um semigrupo, S/ρ é também um semigrupo e, em particular, sendo S um monoide, S/ρ é também um monoide, para a operação definida acima.

Com isso acabamos de definir o *semigrupo (ou monoide) quociente de S por ρ*, ou formalmente:

Definição 2.48. Sejam S um semigrupo e ρ uma congruência em S. Chamamos de *semigrupo quociente de S por ρ* o conjunto quociente S/ρ munido da operação binária dada por $\rho_a\rho_b = \rho_{ab}$, para todo $\rho_a, \rho_b \in S/\rho$. Em particular, se S é um monoide, dizemos que S/ρ é o *monoide quociente de S por ρ.*

Proposição 2.35. *Sejam S um semigrupo (monoide) e ρ uma congruência em S. Então a função $f : S \longrightarrow S/\rho$ dada por $f(s) = \rho_s$ para todo $s \in S$ é um homomorfismo de semigrupo (monoide) e $\rho = \ker f$.*

Demonstração. De fato, para todo $s, t \in S$ temos $f(s)f(t) = \rho_s\rho_t = \rho_{st} = f(st)$. Note também que para todo $s, t \in S$ temos $(s, t) \in \ker f \iff f(s) = f(t) \iff \rho_s = \rho_t \iff (s, t) \in \rho$. Logo $\rho = \ker f$. ■

Proposição 2.36. *Sejam S, T semigrupos e $\theta : S \longrightarrow T$ um homomorfismo então $\ker\theta$ é uma congruência em S.*

Demonstração. Note que $\ker\theta$ é uma relação de equivalência em S. Suponha que $a, b, c, d \in S$ com $(a, b), (c, d) \in \ker\theta$, então $\theta(a) = \theta(b)$ e $\theta(c) = \theta(d)$. Sendo θ um homomorfismo, temos $\theta(ac) = \theta(a)\theta(c) =$

$\theta(b)\theta(d) = \theta(bd)$. Logo $(ac, bd) \in \ker\theta$ e consequentemente $\ker\theta$ é uma congruência em S. ■

Assim, de acordo com a Proposição 2.36 acima e a Definição 2.48, faz sentido falarmos em semigrupo quociente de S por $\ker\theta$. Com isto, podemos enunciar e provar o seguinte teorema:

Teorema 2.4 (Fundamental do Homomorfismo para Semigrupos)**.** *Sejam S, T semigrupos e $\theta : S \longrightarrow T$ um homomorfismo de semigrupos, então $S/\ker\theta \cong \operatorname{im}\theta$*

Demonstração. Defina a função $\alpha : S/\ker\theta \longrightarrow \operatorname{im}\theta$ dada por $\alpha(\ker\theta_a) = \theta(a)$ para todo $a \in S$.

Note que α está bem definida e é injetiva uma vez que para todo $\ker\theta_a, \ker\theta_b \in S/\ker\theta$, temos

$$\begin{aligned} \ker\theta_a = \ker\theta_b &\iff (a,b) \in \ker\theta \\ &\iff \theta(a) = \theta(b) \\ &\iff \alpha(\ker\theta_a) = \alpha(\ker\theta_b) \end{aligned}$$

Além disso, para cada $x \in \operatorname{im}\theta$ temos que existe $a \in S$ tal que $x = \theta(a) = \alpha(\ker\theta_a)$. Logo α é sobrejetiva. Consequentemente é bijetiva.

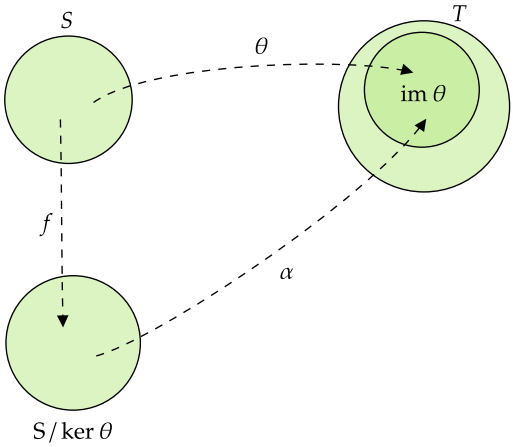
Finalmente, para todo $\ker\theta_a, \ker\theta_b \in S/\ker\theta$, temos

$$\begin{aligned} \alpha(\ker\theta_a \ker\theta_b) &= \alpha(\ker\theta_{ab}) \\ &= \theta(ab) = \theta(a)\theta(b) \\ &= \alpha(\ker\theta_a)\alpha(\ker\theta_b) \end{aligned}$$

Logo α é um homomorfismo. Sendo α bijetivo, temos que α é um isomorfismo de $S/\ker\theta$ em $\operatorname{im}\theta$, isto é, $S/\ker\theta \cong \operatorname{im}\theta$. ■

De acordo com o resultado do Teorema 2.4, claramente $\operatorname{im}\alpha = \operatorname{im}\theta \subseteq T$. Além disso, se definirmos uma função $f : S \longrightarrow S/\ker\theta$ dada por $f(s) = \ker\theta_s$ para todo $s \in S$, temos que $\operatorname{im} f = S/\ker\theta$ e que $\alpha \circ f = \theta$. Esquematicamente temos o diagrama da Figura 5 e o Teorema 2.5 generaliza esta ideia.

Figura 5 – Esquema do Teorema 2.4



Teorema 2.5. *Sejam S, T semigrupos, $\theta : S \longrightarrow T$ um homomorfismo, ρ uma congruência em S e $f : S \longrightarrow S/\rho$ uma função dada por $f(s) = \rho_s$ para todo $s \in S$. Suponha que $\rho \subseteq \ker\theta$, então existe um único homomorfismo $\beta : S/\rho \longrightarrow T$ tal que $\operatorname{im}\beta = \operatorname{im}\theta$ e tal que $\beta \circ f = \theta$.*

Demonstração. Definamos a função $\beta : S/\rho \longrightarrow T$ dada por $\beta(\rho_s) = \theta(s)$ para todo $s \in S$.

Note que β está bem definida uma vez que para todo $\rho_a, \rho_b \in S/\rho$, temos

$$\begin{aligned}\rho_a = \rho_b &\iff (a,b) \in \rho \subseteq \ker\theta \\ &\implies \theta(a) = \theta(b) \\ &\iff \beta(\rho_a) = \beta(\rho_b)\end{aligned}$$

Além disso, para todo $\rho_a, \rho_b \in S/\rho$, temos

$$\begin{aligned}\beta(\rho_a\rho_b) &= \beta(\rho_{ab}) \\ &= \theta(ab) = \theta(a)\theta(b) \\ &= \beta(\rho_a)\beta(\rho_b)\end{aligned}$$

Agora, tome $t \in \operatorname{im}\theta$, logo existe $s \in S$ tal que $\theta(s) = t$, então $\beta(\rho_s) = t$ e consequentemente $t \in \operatorname{im}\beta$. Por outro lado, tome $t \in \operatorname{im}\beta$, logo existe $\rho_s \in S/\rho$ tal que $\beta(\rho_s) = t$, então $\theta(s) = t$ e consequentemente $t \in \operatorname{im}\theta$. Portanto $\operatorname{im}\beta = \operatorname{im}\theta$.

Por fim, tome $s \in S$, logo $\beta \circ f(s) = \beta(f(s)) = \beta(\rho_s) = \theta(s)$. Portanto $\beta \circ f = \theta$. Note que f é uma função sobrejetora, logo possui inversa a direita $g : S/\rho \longrightarrow S$. Seja, daí, h um homomorfismo de semigrupos tal que $h \circ f = \theta$, logo $h \circ f = \beta \circ f$, consequentemente $h \circ f \circ g = \beta \circ f \circ g$, portanto $h = \beta$, ou seja, desse modo β é única. ■

2.10 RELAÇÕES DE GREEN E SEMIGRUPOS REGULARES

A partir dos ideiais principais apresentados na Definição 2.13 da Seção 2.2 algumas relações de equivalência surgem naturalmente como veremos a seguir. Estas relações foram primeiramente estudadas por A. J. Green em 1951 em seu artigo *"On the structure of semigroups"* e por isso recebem o nome de relações de Green. Nesse mesmo artigo, a partir dessas relações, Green também introduziu os semigrupos regulares.

Definição 2.49. Seja S um semigrupo. Definimos a relação binária em S, $\mathcal{L}$, por

$$\mathcal{L} = \{(a,b) \in S \times S; S^1a = S^1b\} \tag{22}$$

Proposição 2.37. *Sejam S um semigrupo e $a, b \in S$, então $(a,b) \in \mathcal{L}$ se, e somente se existem $s, t \in S^1$ tais que $a = sb$ e $b = ta$.*

Demonstração. Note que $(a,b) \in \mathcal{L}$ se, e somente se $S^1a = S^1b$ se, e somente se $S^1a \subseteq S^1b$ e $S^1b \subseteq S^1a$. Daí, pelo item (iii) do Lema 2.1, temos equivalentemente que existe $s \in S^1$ tal que $a = sb$ e que existe $t \in S^1$ tal que $b = ta$, ou seja, existem $s, t \in S^1$ tais que $a = sb$ e $b = ta$. ■

Definição 2.50. Seja S um semigrupo. Definimos a relação binária em S, $\mathcal{R}$, por

$$\mathcal{R} = \{(a,b) \in S \times S; aS^1 = bS^1\} \tag{23}$$

Proposição 2.38. *Sejam S um semigrupo e $a, b \in S$, então $(a,b) \in \mathcal{R}$ se, e somente se existem $s, t \in S^1$ tais que $a = bs$ e $b = at$.*

Demonstração. Note que $(a,b) \in \mathcal{R}$ se, e somente se $aS^1 = bS^1$ se, e somente se $aS^1 \subseteq bS^1$ e $bS^1 \subseteq aS^1$. Daí, pelo item (iii) do Lema 2.2, temos equivalentemente que existe $s \in S^1$ tal que $a = bs$ e que existe $t \in S^1$ tal que $b = at$, ou seja, existem $s, t \in S^1$ tais que $a = bs$ e $b = at$. ■

Exemplo 2.16. Para o semigrupo $S = \mathcal{M}_n(\mathbb{R})$, as relações de *Green* $\mathcal{L}$ e $\mathcal{R}$ são relações das matrizes *equivalente linha* e *equivalente coluna*, respectivamente. De fato, tome $a, b \in S$, então dizemos que a e b são equivalente linha se existem matrizes elementares $e_1, e_2, \ldots e_n \in S$ tais que $e = e_1e_2 \ldots e_n$ e, por consequência, $a = eb$ e $b = e^{-1}a$ (pois toda matriz elementar é invertível). Logo existem $e, e^{-1} \in S$ tais que

$a = eb$ e $b = e^{-1}a$ e portanto $a\mathcal{L}b$. Por outro lado, se a e b são equivalente coluna se existem matrizes elementares $e_1, e_2, \dots e_n \in S$ tais que $e = e_1e_2 \dots e_n$ e, por consequência, $a^T = eb^T \Rightarrow a = be^T$ e $b^T = e^{-1}a^T \Rightarrow b = ae^{-T}$. Logo existem $e^T, e^{-T} \in S$ tais que $a = be^T$ e $b = ae^{-T}$ e portanto $a\mathcal{R}b$.

Definição 2.51. Seja S um semigrupo. Definimos a relação binária em S, $\mathcal{H}$, por

$$\mathcal{H} = \mathcal{L} \cap \mathcal{R} \tag{24}$$

Proposição 2.39. *Sejam S um semigrupo e $a, b \in S$, então $(a, b) \in \mathcal{H}$ se, e somente se existem $s_1, s_2, t_1, t_2 \in S^1$ tais que $a = s_1b$, $b = t_1a$, $a = bs_2$ e $b = at_2$.*

Demonstração. Note que $(a, b) \in \mathcal{H}$ se, e somente se $(a, b) \in \mathcal{L}$ e $(a, b) \in \mathcal{R}$ se, e somente se existem $s_1, t_1 \in S^1$ tais que $a = s_1b$ e $b = t_1a$ e existem $s_2, t_2 \in S^1$ tais que $a = bs_2$ e $b = at_2$, ou seja, existem $s_1, t_1, s_2, t_2 \in S^1$ tais que $a = s_1b$, $b = t_1a$, $a = bs_2$ e $b = at_2$. ■

Definição 2.52. Seja S um semigrupo. Definimos a relação binária em S, $\mathcal{J}$, por

$$\mathcal{J} = \{(a, b) \in S \times S; S^1aS^1 = S^1bS^1\} \tag{25}$$

Proposição 2.40. *Sejam S um semigrupo e $a, b \in S$, então $(a, b) \in \mathcal{J}$ se, e somente se existem $s, t, u, v \in S^1$ tais que $a = sbt$ e $b = uav$.*

Demonstração. Note que $(a, b) \in \mathcal{J}$ se, e somente se $S^1aS^1 = S^1bS^1$ se, e somente se $S^1aS^1 \subseteq S^1bS^1$ e $S^1bS^1 \subseteq S^1aS^1$. Daí, pelo item (iii) do Lema 2.3, temos equivalentemente que existem $s, t \in S^1$ tais que $a = sbt$ e que existem $u, v \in S^1$ tais que $b = uav$, ou seja, existem $s, t, u, v \in S^1$ tais que $a = sbt$ e $b = uav$. ■

Definição 2.53. Seja S um semigrupo. Definimos a relação binária em S, $\mathcal{D}$, por

$$\mathcal{D} = \mathcal{L} \circ \mathcal{R} \tag{26}$$

Proposição 2.41. *Sejam S um semigrupo e $a, b, c \in S$, então $(a, b) \in \mathcal{D}$ se, e somente se existem $s, t, u, w \in S^1$ e $c \in S$ tais que $a = cs$, $c = at$, $c = ub$ e $b = wc$.*

Demonstração. Note que $(a, b) \in \mathcal{D}$ se, e somente se existe $c \in S$ tal que $(a, c) \in \mathcal{R}$ e $(c, b) \in \mathcal{L}$ se, e somente se existem $s, t \in S^1$ tais que $a = cs$ e $c = at$ e existem $u, w \in S^1$ tais que $c = ub$ e $b = wc$, ou seja, existem $s, t, u, w \in S^1$ e $c \in S$ tais que $a = cs$, $c = at$, $c = ub$ e $b = wc$. ■

As relações das Definições 2.49, 2.50, 2.51, 2.52 e 2.53 são equivalentes às respectivas Proposições 2.37, 2.38, 2.39, 2.40 e 2.41, logo tais proposições poderiam ser usadas como a definição das relações $\mathcal{L}$, $\mathcal{R}$, $\mathcal{H}$, $\mathcal{J}$ e $\mathcal{D}$. Estas são as chamadas relações de Green.

Facilmente podemos verificar que as relações $\mathcal{L}$, $\mathcal{R}$ e $\mathcal{J}$ são reflexivas, simétricas e transitivas em S, e, portanto, são *relações de equivalência em S*. Consequentemente $\mathcal{H}$ é também uma relação de equivalência, pois trata-se da interseção de duas relações de equivalência. Agora, para verificarmos se $\mathcal{D}$ é também uma relação de equivalência, basta verificarmos se $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$, aplicando um resultado obtido pela Proposição 2.33. De fato, a Proposição 2.42 prova que $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$.

Proposição 2.42. $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$

Demonstração. Vamos provar que $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{R} \circ \mathcal{L}$ e $\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{L} \circ \mathcal{R}$.

Tome $(a, b) \in \mathcal{L} \circ \mathcal{R}$, então existe $c \in S^1$ tal que $(a, c) \in \mathcal{R}$ e $(c, b) \in \mathcal{L}$. Logo, pela Proposição 2.38 e pela Proposição 2.37, existem

$s, t, u, w \in S^1$ tais que

$$a = cs \tag{27}$$

$$c = at \tag{28}$$

$$c = ub \tag{29}$$

$$b = wc \tag{30}$$

Seja, daí, $d = bs$, assim,

$$a \overset{(27)}{=} cs \overset{(29)}{=} (ub)s = u(bs) = ud$$

e também

$$d = bs \overset{(30)}{=} (wc)s = w(cs) \overset{(27)}{=} wa$$

Logo existem $u, w \in S^1$ tais que $a = ud$ e $d = wa$. Portanto, pela Proposição 2.37,

$$(a, d) \in \mathcal{L}$$

Além disso, também temos que,

$$b \overset{(30)}{=} wc \overset{(28)}{=} w(at) = wat \overset{(27)}{=} w(cs)t = (wc)(st) \overset{(30)}{=} b(st) = (bs)t = dt$$

Logo existem $s, t \in S^1$ tais que $d = bs$ e $b = dt$. Portanto, pela Proposição 2.38,

$$(d, b) \in \mathcal{R}$$

Ou seja, temos que existe $d \in S^1$ tal que $(a, d) \in \mathcal{L}$ e $(d, b) \in \mathcal{R}$. Portanto, pela Definição 2.32, segue que $(a, b) \in \mathcal{R} \circ \mathcal{L}$. Isto é

$$\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{R} \circ \mathcal{L}$$

Por outro lado e analogamente, provamos que

$$\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{L} \circ \mathcal{R}$$

■

Proposição 2.43. *$\mathcal{R}$ é uma congruência a esquerda.*

Demonstração. Sejam $(a, b) \in \mathcal{R}$ e $c \in S$, então existem $s, t \in S^1$ tais que $a = bs$ e $b = at$. Logo $ca = c(bs) = (cb)s$ e $cb = c(at) = (ca)t$. Portanto $(ca, cb) \in \mathcal{R}$. Ou seja, $\mathcal{R}$ é compatível a esquerda. Como $\mathcal{R}$ é uma relação de equivalência, segue que $\mathcal{R}$ é uma congruência a esquerda. ■

Proposição 2.44. *$\mathcal{L}$ é uma congruência a direita.*

Demonstração. Sejam $(a, b) \in \mathcal{L}$ e $c \in S$, então existem $s, t \in S^1$ tais que $a = sb$ e $b = ta$. Logo $ac = (sb)c = s(bc)$ e $bc = (ta)c = t(ac)$. Portanto $(ac, bc) \in \mathcal{L}$. Ou seja, $\mathcal{L}$ é compatível a direita. Como $\mathcal{L}$ é uma relação de equivalência, segue que $\mathcal{L}$ é uma congruência a direita. ■

Quanto às relações de *Green* podemos determinar algumas relações de inclusão. Primeiramente é fácil notar que $\mathcal{H} \subseteq \mathcal{L}$ e $\mathcal{H} \subseteq \mathcal{R}$, pois $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$.

Seja $(a, b) \in \mathcal{L}$ em um semigrupo S. Então existem $x, y \in S$ tais que $a = xb$ e $b = ya$. Como $1 \in S^1$ (suponha 1 igual a identidade se S for um monoide) então $a = xb1$ e $b = ya1$ o que implica que $S^1aS^1 = S^1bS^1$ e portanto $a\mathcal{J}b$, logo $(a, b) \in \mathcal{J}$, consequentemente $\mathcal{L} \subseteq \mathcal{J}$. Por outro lado, se supormos que $(a, b) \in \mathcal{R}$, analogamente, concluímos que $(a, b) \in \mathcal{J}$, logo $\mathcal{R} \subseteq \mathcal{J}$. Assim notamos que $\mathcal{L} \cup \mathcal{R} \subseteq \mathcal{J}$.

Além disso, para todo $(a, b) \in \mathcal{L}$, obviamente $(b, b) \in \mathcal{R}$, então $(a, b) \in \mathcal{D}$. Portanto $\mathcal{L} \subseteq \mathcal{D}$. E também $(a, b) \in \mathcal{R}$ implica $(a, b) \in \mathcal{D}$. Logo $\mathcal{R} \subseteq \mathcal{D}$. Ou seja, $\mathcal{L} \cup \mathcal{R} \subseteq \mathcal{D}$.

Por fim, tome $(a, b) \in \mathcal{D}$, então existe $c \in S^1$ tal que $(a, c) \in \mathcal{R}$ e $(c, b) \in \mathcal{L}$. Logo existem $s, t, u, w \in S^1$ tais que

$$a = cs \tag{31}$$

$$c = at \tag{32}$$

$$c = ub \tag{33}$$

$$b = wc \tag{34}$$

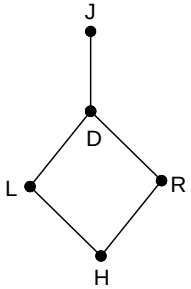
Então $a \overset{(31)}{=} cs \overset{(33)}{=} (ub)s = ubs$ e $b \overset{(34)}{=} wc \overset{(32)}{=} w(at) = wat$. Portanto $(a, b) \in \mathcal{J}$, consequentemente $\mathcal{D} \subseteq \mathcal{J}$.

Assim temos as seguintes inclusões entre as relações de *Green* que podem ser visualizadas no diagrama da Figura 6:

$$\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{D} \subseteq \mathcal{J}$$

$$\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{D} \subseteq \mathcal{J}$$

Figura 6 – Diagrama das inclusões nas relações de *Green*



Lema 2.4. *Sejam S um semigrupo, $a \in S$ e $e \in E(S)$, então $(a, e) \in \mathcal{L} \Rightarrow ae = a$, $(a, e) \in \mathcal{R} \Rightarrow ea = a$ e $(a, e) \in \mathcal{H} \Rightarrow ae = ea = a$.*

Demonstração. Primeiro vamos provar que $(a, e) \in \mathcal{L} \Rightarrow ae = a$. Note que

$$(a, e) \in \mathcal{L} \iff S^1a = S^1e \Rightarrow S^1a \subseteq S^1e$$

Afirmamos que

$$S^1a \subseteq S^1e \iff ae = a$$

De fato, por um lado, suponha que $S^1a \subseteq S^1e$, então, pelo Lema 2.1, existe $t \in S^1$ tal que $a = te$. Logo

$$ae = (te)e = t(ee) = te^2 = te = a$$

Por outro lado, suponha que $ae = a$, tome $x \in S^1a$, então existe $s \in S^1$ tal que $x = sa$, logo $x = s(ae) = (sa)e \in S^1e$ e portanto $S^1a \subseteq S^1e$. Com isto prova-se que

$$(a, e) \in \mathcal{L} \iff S^1a = S^1e \Rightarrow S^1a \subseteq S^1e \iff ae = a$$

Portanto

$$(a, e) \in \mathcal{L} \Rightarrow ae = a$$

Agora vamos provar que $(a, e) \in \mathcal{R} \Rightarrow ea = a$. Note que

$$(a, e) \in \mathcal{R} \iff aS^1 = eS^1 \Rightarrow aS^1 \subseteq eS^1$$

Afirmamos que

$$aS^1 \subseteq eS^1 \iff ea = a$$

De fato, por um lado, suponha que $aS^1 \subseteq eS^1$, então, pelo Lema 2.2, existe $t \in S^1$ tal que $a = et$. Logo

$$ea = e(et) = (ee)t = e^2t = et = a$$

Por outro lado, suponha que $ea = a$, tome $x \in aS^1$, então existe $s \in S^1$ tal que $x = as$, logo $x = (ea)s = e(as) \in eS^1$ e portanto $aS^1 \subseteq eS^1$. Com isto prova-se que

$$(a, e) \in \mathcal{R} \iff aS^1 = eS^1 \Rightarrow aS^1 \subseteq eS^1 \iff ea = a$$

Portanto

$$(a, e) \in \mathcal{R} \Rightarrow ea = a$$

Por fim, resta provar que $(a, e) \in \mathcal{H} \Rightarrow ae = ea = a$. De fato,

$$\begin{aligned}(a, e) \in \mathcal{H} &\iff (a, e) \in \mathcal{L}, (a, e) \in \mathcal{R} \\ &\implies ae = a, ea = a \\ &\iff ae = ea = a\end{aligned}$$

■

Note que, na demonstração do Lema 2.4, obtemos os seguintes resultados: $S^1a \subseteq S^1e \iff ae = a$ e $aS^1 \subseteq eS^1 \iff ea = a$.

Como as relações de Green, são relações de equivalência, então podemos obter as suas classes de equivalência conforme a Definição 2.42.

Notação 2.4. Sejam as relações de Green de um semigrupo S e $a \in S$, denotamos:

(i) $\mathcal{H}_a$ a $\mathcal{H}$-*classe de* a

(ii) $\mathcal{L}_a$ a $\mathcal{L}$-*classe de* a

(iii) $\mathcal{R}_a$ a $\mathcal{R}$-*classe de* a

(iv) $\mathcal{D}_a$ a $\mathcal{D}$-*classe de* a

(v) $\mathcal{J}_a$ a $\mathcal{J}$-*classe de* a

Teorema 2.6 (Subgrupo maximal)**.** *Seja S um semigrupo com $e \in E(S)$, então $\mathcal{H}_e$ é o subgrupo maximal de S com identidade e.*

Demonstração. Primeiramente vamos provar que $\mathcal{H}_e$ é um subgrupo de S, isto é, que é um subconjunto de S, fechado para a operação de S, associativo com elemento identidade e e com elemento inverso.

Como $\mathcal{H}_e = \{x \in S; (x, e) \in \mathcal{H}\}$, imediatamente notamos que $\mathcal{H}_e \subseteq S$.

Tome $a, b \in \mathcal{H}_e$, então $(a, e), (b, e) \in \mathcal{H} = \mathcal{L} \cap \mathcal{R}$. Como, pela Proposição 2.44, $\mathcal{L}$ é uma congruência a direita, então $(ab, eb) \in \mathcal{L}$. E como, pela Proposição 2.43, $\mathcal{R}$ é uma congruência a esquerda, então $(ab, ae) \in \mathcal{R}$.

Pelo Lema 2.4 segue que

$$a\mathcal{H}e \Rightarrow ae = ea = a \tag{35}$$

$$b\mathcal{H}e \Rightarrow be = eb = b \tag{36}$$

Logo $(ab, eb) = (ab, b) \in \mathcal{L}$ e $(ab, ae) = (ab, a) \in \mathcal{R}$.

Como $(a, e) \in \mathcal{R}$, $(b, e) \in \mathcal{L}$ e $\mathcal{R}$ e $\mathcal{L}$ são transitivas, então $(ab, a) \in \mathcal{R}$ e $(a, e) \in \mathcal{R}$, logo $(ab, e) \in \mathcal{R}$ e, também, $(ab, b) \in \mathcal{L}$ e $(b, e) \in \mathcal{L}$, logo $(ab, e) \in \mathcal{L}$. Portanto $(ab, e) \in \mathcal{H}$ e, consequentemente, $ab \in \mathcal{H}_e$.

Como $\mathcal{H}_e \subseteq S$ fechado para a operação de S, obviamente, os elementos de $\mathcal{H}_e$ são associativos.

Como $e \in \mathcal{H}_e$, $e = e^2$, e pelo Lema 2.4, segue que para todo $x \in \mathcal{H}_e$ temos $xe = ex = x$. Ou seja, e é o elemento identidade de $\mathcal{H}_e$.

De $(a, e) \in \mathcal{H}$ segue, pela Proposição 2.39, que existem $s_1, s_2, s_3, s_4 \in S^1$ tais que

$$a = s_1 e \tag{37}$$

$$e = s_2 a \tag{38}$$

$$a = e s_3 \tag{39}$$

$$e = a s_4 \tag{40}$$

De $(b, e) \in \mathcal{H}$ segue, pela Proposição 2.39, que existem $t_1, t_2, t_3, t_4 \in$

S^1 tais que

$$b = t_1 e \tag{41}$$

$$e = t_2 b \tag{42}$$

$$b = e t_3 \tag{43}$$

$$e = b t_4 \tag{44}$$

Para verificar a existência do elemento inverso, note que

$$e = e^2 = ee \overset{(38)}{=} e(s_2 a) \overset{(35)}{=} e(s_2 ea) = (es_2 e)a$$

e que

$$e = e^2 = ee \overset{(40)}{=} (as_4)e \overset{(35)}{=} (aes_4)e = a(es_4 e)$$

portanto

$$(es_2 e)a = e = a(es_4 e)$$

Seja, daí, $c = es_4 e$ e $d = es_2 e$, logo $c, d \in S^1$ e $da = e = ac$. No entanto

$$\begin{aligned} c &= es_4 e \\ &= e^2 s_4 e \\ &= (ee)(s_4 e) \\ &= e(es_4 e) \\ &= ec \qquad (45) \\ &= (da)c \\ &= d(ac) \\ &= de \qquad (46) \\ &= (es_2 e)e \\ &= es_2 e^2 \\ &= es_2 e \\ &= d \end{aligned}$$

logo

$$c = d \tag{47}$$

e, consequentemente,

$$ca = e = ac \tag{48}$$

Falta, agora, mostrar que $c \in \mathcal{H}_e$, e assim concluiremos que c é o elemento inverso de $a \in \mathcal{H}_e$, ou seja, $c = a^{-1}$. Como $c \overset{(45)}{=} ec$, $e \overset{(48)}{=} ac$ então $(c, e) \in \mathcal{R}$. Como $c \overset{(46)}{=} de \overset{(47)}{=} ce$, $e \overset{(48)}{=} ca$ então $(c, e) \in \mathcal{L}$. Portanto $(c, e) \in \mathcal{H}$, ou seja, $c \in \mathcal{H}_e$. Isto é, existe $c \in \mathcal{H}_e$ tal que $ac = ca = e$. Como a foi tomado arbitrariamente, então para todo elemento de $\mathcal{H}_e$ existe elemento inverso.

Agora, provaremos que $\mathcal{H}_e$ é o subgrupo maximal de S com e identidade. Para tanto vamos tomar G um subgrupo qualquer de S com identidade e e vamos provar que $G \subseteq \mathcal{H}_e$. Tome, assim, $g \in G$ qualquer, então $g = eg$ e $e = g^{-1}g$, logo $(g, e) \in \mathcal{R}$. Também temos $g = ge$ e $e = gg^{-1}$, logo $(g, e) \in \mathcal{L}$. Portanto $(g, e) \in \mathcal{H}e$, ou seja $g \in \mathcal{H}_e$. Por consequência $G \subseteq \mathcal{H}_e$. ■

Corolário 2.2. *Sejam S um semigrupo e $a \in S$, então as seguintes afirmações são equivalentes:*

(i) a encontra-se em um subgrupo de S

(ii) existe $e \in E(S)$ tal que $a \in \mathcal{H}_e$

(iii) $\mathcal{H}_a$ é um subgrupo de S

Demonstração. Vamos demonstrar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

- $(i) \Rightarrow (ii)$: Seja G um subgrupo de S com $a \in G$. Então, pelo Teorema 2.6, $G \subseteq \mathcal{H}_e$ em que $e \in E(S)$ é a identidade de G, portanto $a \in \mathcal{H}_e$.

- $(ii) \Rightarrow (iii)$: Suponha que existe $e \in E(S)$ tal que $a \in \mathcal{H}_e$. Como $\mathcal{H}$ é uma relação de equivalência, então, pela Proposição 2.32, $\mathcal{H}_a = \mathcal{H}_e$. Como, pelo Teorema 2.6, $\mathcal{H}_e$ é um subgrupo de S, então $\mathcal{H}_a$ também.

- $(iii) \Rightarrow (i)$: Suponha que $\mathcal{H}_a$ é um subgrupo de S, como $a \in \mathcal{H}_a$, então a encontra-se em um subgrupo de S.

■

Proposição 2.45. *Sejam S um semigrupo e $e, f \in E(S)$ então*

$$(e, f) \in \mathcal{R} \iff e = fe, f = ef$$

e

$$(e, f) \in \mathcal{L} \iff e = ef, f = fe$$

Demonstração. As implicações

$$e = fe, f = ef \Rightarrow (e, f) \in \mathcal{R}$$

e

$$e = ef, f = fe \Rightarrow (e, f) \in \mathcal{L}$$

são imediatas a partir da Proposição 2.38 e da Proposição 2.37 respectivamente.

Por outro lado, $(e, f) \in \mathcal{R}$ implica, pelo Lema 2.4, que $e = fe$. Como $\mathcal{R}$ é reflexiva, então $(f, e) \in \mathcal{R} \overset{\text{Lema 2.4}}{\Rightarrow} f = ef$. Portanto, $(e, f) \in \mathcal{R} \Rightarrow e = fe, f = ef$. Analogamente, $(e, f) \in \mathcal{L} \Rightarrow e = ef, f = fe$. ■

Agora, finalmente, definiremos *semigrupo regular*.

Definição 2.54. Sejam S um semigrupo e $a \in S$, dizemos que a é um *regular*, se, e somente se, $a = axa$ para algum $x \in S$. Dizemos que S é um *semigrupo regular*, se todo elemento de S é regular.

Exemplo 2.17. O monoide $(\mathcal{M}_n(\mathbb{R}), \cdot)$ é um semigrupo regular. Isto é para todo $A \in \mathcal{M}_n(\mathbb{R})$, existe $X \in \mathcal{M}_n(\mathbb{R})$ tal que $A = AXA$. Se tomarmos, por exemplo,

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 0 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

e tentarmos resolver $AXA = A$, obtemos

$$X = \begin{bmatrix} 1 - 2\alpha & \alpha & -1 \\ \beta_1 & \beta_2 & \beta_3 \\ -2\gamma & \gamma & 1 \end{bmatrix}$$

com $\alpha, \beta_1, \beta_2, \beta_3, \gamma \in \mathbb{R}$.

Note que não precisamos, necessariamente, das relação de *Green* para definir semigrupo regular, no entanto, essas relações nos dão alguns resultados interessantes.

Proposição 2.46. *Sejam S um semigrupo e $a \in S$, então as seguintes afirmações são equivalentes:*

(i) *a é regular*

(ii) *existe $e \in E(S)$ tal que $(a, e) \in \mathcal{R}$*

(iii) *existe $f \in E(S)$ tal que $(a, f) \in \mathcal{L}$*

Demonstração. Vamos demonstrar que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$.

- $(i) \Rightarrow (ii)$: Suponha $a \in S$ regular. Então, pela Definição 2.54, existe $x \in S$ tal que $a = axa$. Tome $e = ax$, então $e^2 = (ax)(ax) = (axa)x = ax = e$, logo $e \in E(S)$. Como $e = ax$ e $a = axa = ea$, então existe $e \in E(S)$ tal que $(a, e) \in \mathcal{R}$.

- $(ii) \Rightarrow (iii)$: Suponha que existe $e \in E(S)$ tal que $(a, e) \in \mathcal{R}$. Então, pelo Lema 2.4, segue que, $ea = a$ e além disso, pela Proposição 2.38, existem $u, v \in S^1$ tais que $a = eu$, $e = av$. Assim $a = ea = (av)a = ava$. Tome $f = va$, então $f^2 = (va)(va) = v(ava) = va = f$, logo $f \in E(S)$. Daí segue que, $a = ava = af$ e que $f = va$, portanto existe $f \in E(S)$ tal que $(a, f) \in \mathcal{L}$.

- $(iii) \Rightarrow (i)$: Suponha que existe $f \in E(S)$ tal que $(a, f) \in \mathcal{L}$. Então, pelo Lema 2.4, segue que, $af = a$ e além disso, pela Proposição 2.37, existem $u, v \in S^1$ tais que $a = uf$, $f = va$. Assim $a = af = a(va) = ava$. Caso $v = 1$, então $a = ava = a1a = a^2$ e daí existe $a \in S$ tal que $a = aaa$. Caso $v \neq 1$, então existe $v \in S$ tal que $a = ava$. Consequentemente em todo caso a é regular.

■

Proposição 2.47. *Sejam S um semigrupo e a um elemento de S. Então a é regular, se, e somente se, $\mathcal{D}_a$ é regular.*

Demonstração. A recíproca é imediata. Afinal sendo $\mathcal{D}_a$ é regular e $a \in \mathcal{D}_a$, então a é regular.

Por outro lado, suponha a regular. Tome $b \in \mathcal{D}_a$, logo existe $c \in S^1$ tal que $(a, c) \in \mathcal{R}$ e $(c, a) \in \mathcal{L}$. Como a é regular, então, pelo item (ii) da Proposição 2.46, existe $e \in E(S)$ tal que $(a, e) \in \mathcal{R}$, logo $(e, a) \in \mathcal{R}$ por simetria, e consequentemente $(e, c) \in \mathcal{R}$ por transitividade, logo $(c, e) \in \mathcal{R}$ por simetria, o que, pelo item (ii) da Proposição 2.46, implica que c é regular. Pelo item (iii) da Proposição 2.46, existe $f \in E(S)$ tal que $(c, f) \in \mathcal{L}$, logo $(f, c) \in \mathcal{L}$ por simetria, e consequentemente $(f, b) \in \mathcal{L}$ por transitividade, logo $(b, f) \in \mathcal{L}$ por simetria, o que, pelo item (iii) da Proposição 2.46, implica que b é

regular. Como b é um elemento arbitrário de $\mathcal{D}_a$ então, todo elemento de $\mathcal{D}_a$ é regular, logo $\mathcal{D}_a$ é regular. ■

3 TEORIA DA COMPUTAÇÃO: LINGUAGENS E AUTÔMATOS

Neste capítulo são apresentadas algumas definições, exemplos e resultados acerca dos conceitos de *linguagens* e *autômatos* da Teoria da Computação.

Na Seção 3.1 apresentamos as definições para *alfabeto*, *strings* e *linguagens*. Esses conceitos são fundamentais para a construção dos *modelos computacionais* e as *expressões regulares* apresentados nas seções seguintes. Existem vários modelos computacionais na Teoria da Computação, certamente os mais conhecidos são as *Máquinas de Turing*. No entanto, neste capítulo apresentamos dois modelos mais simples: os *semiautômatos* na Seção 3.2 e os *autômatos* na Seção 3.3. Semiautômatos são capazes de descrever o funcionamento de dispositivos eletromecânicos simples. Autômatos são também conhecidos como *reconhecedores* pois reconhecem certas linguagens que denominamos de *linguagens regulares*.

Finalmente, na última Seção, apresentamos as expressões regulares e sua relação com autômatos e linguagens regulares.

Segundo Sipser [9, p. 31, tradução livre],

> A teoria da computação começa com uma questão: O que é um computador? Esta parece ser uma pergunta boba, afinal, todos sabem que essa coisa que eu digito é um computador. Mas esses computadores reais são bastante complicados - demais para nos permitir estabelecer uma teoria matemática gerenciável deles diretamente. Ao invés, usamos um computador idealizado chamado de *modelo computacional*. Do mesmo modo que qualquer modelo cientifico, um modelo computacional pode ser preciso em alguns aspectos mas possivelmente não em outros.

3.1 *STRINGS* E LINGUAGENS

Definição 3.1. Um *alfabeto* é um conjunto finito e não vazio de elementos chamados de *símbolos*, ou seja, um símbolo é um elemento do alfabeto.

Geralmente usa-se a letra grega sigma maiúscula (Σ) para denotar um alfabeto.

Exemplo 3.1. Alguns exemplos de alfabetos são:

$$\Sigma_1 = \{0, 1\}$$

$$\Sigma_2 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\Sigma_3 = \{0\}$$

$$\Sigma_4 = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{e}, \mathrm{f}, \mathrm{g}, \mathrm{h}, \mathrm{i}, \mathrm{j}, \mathrm{k}, \mathrm{l}, \mathrm{m}, \mathrm{n}, \mathrm{o}, \mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{s}, \mathrm{t}, \mathrm{u}, \mathrm{v}, \mathrm{w}, \mathrm{x}, \mathrm{y}, \mathrm{z}\}$$

$$\Sigma_5 = \{\alpha, \beta, \delta, \gamma\}$$

No Exemplo 3.1, Σ_4 é o conjunto de letras minúsculas de **a** a **z** do alfabeto português brasileiro. Neste caso, a Definição 3.1 corrobora com a noção intuitiva de alfabeto. Porém os alfabetos Σ_1, Σ_2 e Σ_3 não parecem com os que concebemos intuitivamente, afinal geralmente relacionamos os alfabetos a letras e não a números. Mas de acordo com a Definição 3.1 um alfabeto é simplesmente um conjunto finito e não vazio de símbolos. Então, nesse sentido, Σ_1, Σ_2 e Σ_3 inclusive, são alfabetos.

O alfabeto que contém um único símbolo, como em Σ_3 do Exemplo 3.1, é chamado de *alfabeto unário*.

Definição 3.2. Seja Σ um alfabeto. Chamamos de *string de* Σ a cadeia (ou sequência) finita de zero ou mais símbolos do alfabeto Σ. Denotamos a *string* s de Σ com um ou mais símbolos por $s =$

$s_1 s_2 \dots s_k$ com $s_i \in \Sigma$, para $1 \leq i \leq k$. A *string* formada por nenhum símbolo é a *string vazia* que denotamos por ε.

Exemplo 3.2. **letra**, **palavra**, **teoria**, **abadz**, **aaaa** são *strings* do alfabeto Σ_4 do Exemplo 3.1. **1527**, **54179**, **5** são *strings* do alfabeto Σ_2 do Exemplo 3.1. **01001**, **11001**, **01** são *strings* dos alfabetos Σ_1 e Σ_2 do Exemplo 3.1. **000**, **0000000**, **0** são *strings* dos alfabetos Σ_1, Σ_2 e Σ_3 do Exemplo 3.1. ε é uma *string* de todo e qualquer alfabeto.

Definição 3.3. Seja Σ um alfabeto e seja x uma *string* de Σ. O *comprimento* ou *tamanho* de x, denotado por $|x|$, é a cardinalidade da *string* x. Isto é, o tamanho de x é a quantidade de símbolos que formam x.

Exemplo 3.3. $|\text{letra}| = 5$, $|\text{palavra}| = 7$, $|\text{teoria}| = 6$, $|1527| = 4$, $|01| = 2$, $|0| = 1$, $|\varepsilon| = 0$.

Definição 3.4. Seja Σ um alfabeto, x uma *string* de Σ e $a \in \Sigma$. Escrevemos $|x|_a$ para o *número de ocorrências do símbolo a em x*.

Exemplo 3.4. $|\text{letra}|_{\text{a}} = 1$, $|\text{palavra}|_{\text{a}} = 3$, $|\text{teoria}|_{\text{a}} = 1$, $|1527|_1 = 1$, $|01|_1 = 1$, $|0|_1 = 0$, $|\varepsilon|_1 = 0$.

Definição 3.5. Seja Σ um alfabeto, $n \in \mathbb{N}$ e w uma *string* de Σ. Então denotamos o conjunto de todas as *strings* de Σ de tamanho n por Σ^n, isto é,

$$\Sigma^n = \{w; w \text{ é } \textit{string} \text{ de } \Sigma \text{ com } |w| = n\}$$

Exemplo 3.5. Suponha $\Sigma = \{\text{a}, \text{b}, \text{c}\}$ um alfabeto. Então

$$\Sigma^0 = \{\varepsilon\}$$

$$\Sigma^1 = \{\text{a}, \text{b}, \text{c}\} = \Sigma$$

$$\Sigma^2 = \{\text{aa}, \text{ab}, \text{ac}, \text{ba}, \text{bb}, \text{bc}, \text{ca}, \text{cb}, \text{cc}\}$$

Definição 3.6. Seja Σ um alfabeto. Denotamos o *conjunto de todas as* strings *de* Σ por

$$\Sigma^* = \bigcup_{n \in \mathbb{N}^0} \Sigma^n.$$

Assim, um elemento de Σ^* é uma *string* de Σ.

Definição 3.7. Seja Σ um alfabeto. Denotamos o conjunto de todas as *strings* de Σ com comprimento maior que zero por

$$\Sigma^+ = \bigcup_{n \in \mathbb{N}} \Sigma^n.$$

Nesse caso, $\varepsilon \notin \Sigma^+$.

Observação 3.1. Se Σ é um alfabeto com k símbolos, então para qualquer $n \in \mathbb{N}^0$, o conjunto Σ^n contém exatamente k^n *strings*, logo é finito, consequentemente enumerável. Como a união infinita de conjuntos enumeráveis é enumerável, segue que Σ^* e Σ^+ são enumeráveis.

Definição 3.8. Seja Σ um alfabeto com

$$u = u_1 u_2 \dots u_m,\ v = v_1 v_2 \dots v_n \in \Sigma^*.$$

A *concatenação de* u *com* v, ou equivalentemente, u *concatenado com* v, denotada por uv, é uma operação binária em Σ^* dada por

$$\begin{aligned} f: \quad & \Sigma^* \times \Sigma^* \longrightarrow \Sigma^* \\ & (u, v) \mapsto f(u, v) \end{aligned}$$

em que

$$f(u, v) = uv = u_1 u_2 \dots u_m v_1 v_2 \dots v_n$$

$$f(u, \varepsilon) = u\varepsilon = u = \varepsilon u = f(\varepsilon, u)$$

$$f(\varepsilon, \varepsilon) = \varepsilon\varepsilon = \varepsilon.$$

Exemplo 3.6. Sejam **abra** e **cadabra** *strings* do alfabeto Σ_4 do Exemplo 3.1, então **abra** concatenado com **cadabra** é a *string* **abracadabra**. Já **cadabra** concatenado com **abra** é a *string* **cadabraabra**.

Sejam Σ um alfabeto, $u, v, w \in \Sigma^*$ e $a \in \Sigma$, então a função concatenação tem as seguintes propriedades que seguem da Definição 3.8

(i) (associatividade) $u(vw) = (uv)w$

(ii) (elemento neutro) $\varepsilon u = u\varepsilon = u$

(iii) $|uv| = |vu| = |u| + |v|$

(iv) $|uv|_a = |vu|_a = |u|_a + |v|_a$

Do Exemplo 3.6, vemos que se o alfabeto Σ não é unário, então a concatenação de suas *strings* não é comutativa, isto é, se $u, v \in \Sigma^+$ então $uv \neq vu$. Além disso, se u, v e w forem *strings* de alfabetos diferentes ($u \in \Sigma_1$, $v \in \Sigma_2$ e $w \in \Sigma_3$) então podemos tomar $\Sigma = \Sigma_1 \cup \Sigma_2 \cup \Sigma_3$ e assim podemos construir uma função concatenação que é uma operação binária fechada para o conjunto Σ^*. Ou Seja, podemos dizer, daí, que Σ^* é um monoide não comutativo munido da operação binária de concatenação. No Capítulo 4 retomamos este monoide que recebe o nome de *monoide livre*. Sendo Σ^* um monoide, então não há ambiguidade em denotar

$$\underbrace{uuu\ldots u}_{n\text{vezes}}$$

por u^n com $n \in \mathbb{N}$. Usamos u^0 para representar a *string* vazia ε.

Exemplo 3.7. Suponha $\Sigma = \{\mathrm{a}, \mathrm{b}, \mathrm{l}\}$ um alfabeto dado e $v = \mathrm{bla}$ uma *string* de Σ. Então $v^0 = \varepsilon$, $v^1 = v = \mathrm{bla}$, $v^2 = \mathrm{blabla}$ e $v^5 = \mathrm{blablablablabla}$.

Definição 3.9. Seja Σ um alfabeto com $u, v \in \Sigma^*$,

(i) v é *fator a esquerda* ou *prefixo* de u, se existe $x \in \Sigma^*$ tal que $u = vx$; se $x \neq \varepsilon$, então dizemos que v é *fator próprio a esquerda* ou *prefixo próprio* de u;

(ii) v é *fator a direita* ou *sufixo* de u, se existe $x \in \Sigma^*$ tal que $u = xv$; se $x \neq \varepsilon$, então dizemos que v é *fator próprio a direita* ou *sufixo próprio* de u;

(iii) v é *fator* de u, se existem $x, y \in \Sigma^*$ tais que $u = xvy$; se $x \neq \varepsilon$ e $y \neq \varepsilon$, então dizemos que v é *fator próprio* de u.

Note que a *string* vazia ε é um prefixo, sufixo e fator de toda *string*. Uma *string* de tamanho n tem exatamente $n + 1$ prefixos distintos (n prefixos próprios) e $n + 1$ sufixos distintos (n sufixos próprios), mas não sabemos a priori a relação entre o número de fatores distintos de uma *string* e o seu comprimento n (Sakarovitch [8, p. 21]).

Definição 3.10. Seja Σ um alfabeto com $u \in \Sigma^*$, escrevemos

(i) $\mathrm{Pre}(u)$ para denotar o conjunto dos prefixos de u;

(ii) $\mathrm{Suf}(u)$ para denotar o conjunto dos sufixos de u;

(iii) $\mathrm{Fat}(u)$ para denotar o conjunto dos fatores de u.

Definição 3.11. Seja Σ um alfabeto com $w, u_1, u_2, \ldots, u_n \in \Sigma^*$, dizemos que a *string* $u_1u_2 \ldots u_n$ é uma *fatoração de* w, se $w = u_1u_2 \ldots u_n$. Se $u_i \neq \varepsilon$, então dizemos que $u_1u_2 \ldots u_n$ é *fatoração própria de* w.

Definição 3.12. Seja Σ um alfabeto com $s \in \Sigma^*$. Sendo s uma sequência de símbolos do alfabeto Σ, chamamos de *substring de* s a qualquer subsequência de s.

Todo fator de uma *string* é uma *substring*, no entanto a recíproca não é verdadeira.

Exemplo 3.8. Considere a *string* **palavra** do alfabeto Σ_4 do Exemplo 3.1, **alavr**, **pa** e **vra** são *substrings* e também, respectivamente, fator, prefixo e sufixo próprios de **palavra**; **aaa** e **plvr** são *substrings* de **palavra**, mas não são fatores.

Definição 3.13. Seja Σ um alfabeto com $u = u_1u_2 \dots u_n \in \Sigma^*$ com $u_i \in \Sigma$. A *imagem espelhada de u* ou *transposição de u*, denotada por u^t, é a *string*

$$u^t = u_n u_{n-1} \dots u_1.$$

Exemplo 3.9. A *string* **edadisrevinu** é a transposição da *string* **universidade** do alfabeto Σ_4 do Exemplo 3.1.

Definição 3.14. Seja Σ um alfabeto com $u \in \Sigma^*$. Dizemos que u é uma *string palíndroma*, se $u = u^t$.

Exemplo 3.10. A *string* **reviver** do alfabeto Σ_4 do Exemplo 3.1 é palíndroma.

Definição 3.15. Seja Σ um alfabeto, escrevemos

$$\mathrm{Pal}(\Sigma) = \{u \in \Sigma^*; u = u^t\}$$

para denotar o conjunto das *strings* palíndromas de Σ^*.

Definição 3.16. Seja Σ um alfabeto com

$$u = u_1u_2 \dots u_m,\ v = v_1v_2 \dots v_n \in \Sigma^+.$$

Dizemos que u *é igual a* v $(u = v)$, quando $|u| = m = n = |v|$ e $u_i = v_i$ para todo $u_i, v_i \in \Sigma$ com $1 \leq i \leq n$.

Definição 3.17. Seja Σ um alfabeto. Chamamos de *linguagem sobre* Σ qualquer subconjunto de Σ^*.

Exemplo 3.11. Suponha $\Sigma = \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}, \mathrm{e}, \mathrm{i}, \mathrm{o}\}$ um alfabeto. Então $L = \{\mathrm{baba}, \mathrm{cedo}, \mathrm{cidade}, \mathrm{a}, \varepsilon\}$ é uma linguagem sobre Σ.

3.2 SEMIAUTÔMATO

Um *semiautômato* é um modelo computacional, composto por três objetos: um conjunto finito não vazio de *estados*; um conjunto finito não vazio de *entradas*; e, uma *função de transição* que descreve a mudança de um estado para outro dependendo do valor da entrada. Esse modelo pode ser usado para descrever o funcionamento de dispositivos eletromecânicos simples, como por exemplo portas automáticas, interruptores de iluminação automáticos, calculadoras, computadores, dispositivos que contam cédulas de dinheiro, centrais telefônicas, painéis de elevadores, etc (Lidl e Pilz [6, p. 342]).

Por exemplo, no caso de uma porta automática, o dispositivo deve ser capaz de identificar o *estado* da porta (se aberta ou fechada) e também uma informação de *entrada*, lida por um sensor, que indica se há presença de uma pessoa para permitir sua passagem. Dependendo do caso, a porta deve mudar seu estado:

(i) Se a porta está aberta, e

  (i) há a presença de pessoas na frente ou atrás dela, então deve permanecer aberta.

  (ii) não há a presença de pessoas na frente ou atrás dela, então deve fechar.

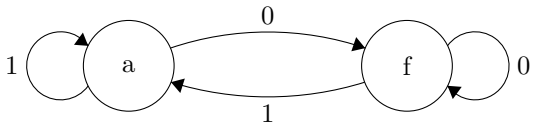
(ii) Caso contrário, se a porta está fechada, e

  (i) há a presença de pessoas na frente ou atrás dela, então deve abrir.

  (ii) não há a presença de pessoas na frente ou atrás dela, então permanecer fechada.

Para representar esta situação podemos usar o diagrama da Figura 7. Nesse caso cada estado da porta é representado por uma letra a ou f dentro de um círculo para indicar se a porta está aberta ou fechada, respectivamente. Os valores de entrada são representados pelos números um ou zero e indicam a presença ou não de pessoas na frente ou atrás da porta. Esses valores de entrada rotulam setas que indicam a transição de estados da porta.

Figura 7 – Representação do funcionamento de uma porta automática



Como podemos notar na Figura 7, graficamente, um semiautômato pode ser representado por um grafo orientado que chamamos de *diagrama de estados do semiautômato* em que:

(i) cada nó representa um estado;

(ii) as setas do grafo são rotuladas com símbolos do alfabeto de entrada e representam a função transição.

3.2.1 Semiautômato Determinístico

Note que o funcionamento da porta automática, representado na Figura 7, é um semiautômato que varia seus estados de modo bem determinado para cada entrada, isto é, para todo estado e toda entrada existe um único estado alcançado. Nesse caso, cada símbolo do alfabeto rotula uma única seta com origem em um estado (nó) e

destino em outro no seu diagrama de estados. Isso nos motiva a definir formalmente um *semiautômato determinístico* da seguinte maneira:

Definição 3.18. Um *semiautômato determinístico* é uma tripla (Q, Σ, δ) em que

(i) Q é um conjunto finito e não vazio de elementos chamados de *estados*;

(ii) Σ é um alfabeto de símbolos chamados de *entradas*;

(iii) $\delta : Q \times \Sigma \longrightarrow Q$ é a *função transição* que descreve como acontece a mudança de estado dependendo da entrada.

Exemplo 3.12. O semiautômato representado na Figura 7 é um semiautômato determinístico $P = (Q, \Sigma, \delta)$ em que $Q = \{\text{a}, \text{f}\}$, $\Sigma = \{0, 1\}$ e para todo $q \in Q$ e todo $u \in \Sigma$, δ é dada por

$$\delta(q, u) = \begin{cases} \text{a, se } u = 1 \\ \text{f, se } u = 0 \end{cases}$$

Seja $S = (Q, \Sigma, \delta)$ semiautômato determinístico com $Q = \{q_1, q_2, q_3, \ldots, q_n\}$ e $u \in \Sigma$, então podemos denotar a função transição δ para o símbolo u por

$$\delta_u = \begin{pmatrix} q_1 & q_2 & q_3 & \cdots & q_n \\ \delta(q_1, u) & \delta(q_2, u) & \delta(q_3, u) & \ldots & \delta(q_n, u) \end{pmatrix} \in \mathcal{T}_Q.$$

Assim temos que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$, em que $\mathcal{T}_Q$ é o conjunto de todas as funções em Q, conforme descrevemos na Equação (2.5) da Seção 2.5.

Exemplo 3.13. Para o semiautômato determinístico P do Exemplo 3.12 temos que

$$\delta_0 = \begin{pmatrix} \text{a} & \text{f} \\ \text{f} & \text{f} \end{pmatrix} \qquad\qquad \delta_1 = \begin{pmatrix} \text{a} & \text{f} \\ \text{a} & \text{a} \end{pmatrix}.$$

Logo $\delta = \{\delta_0, \delta_1\}$.

Um semiautômato é frequentemente descrito por uma *tabela de transição*: os estados ficam dispostos na primeira linha da tabela, as entradas na primeira coluna e os elementos internos da tabela são o resultado da transição do elemento da primeira coluna com o elemento da primeira linha respectivamente. Assim, o semiautômato determinístico P do Exemplo 3.12 pode ser representado pela seguinte tabela de transição:

Tabela 6 – Tabela de transição do semiautômato P

P	a	f
0	f	f
1	a	a

3.2.2 Semiautômato Não Determinístico

Imaginemos agora uma outra porta automatizada que além de possuir um sensor para identificar a presença de pessoas, também possui sensores capazes de medir a temperatura corporal e de detectar se o indivíduo veste uma máscara facial de pano cobrindo boca e nariz. Após identificar a presença do indivíduo, os sensores de temperatura e de uso de máscara devem ser acionados simultaneamente. Um quarto sensor é usado para aguardar o retorno dos sensores de uso de máscara e temperarura. Por fim, a porta só poderá abrir, se for medida uma temperatura menor que $37,5$ graus Celsius e o individuo estiver usando uma máscara facial de pano com boca e nariz cobertos. Assim, o dispositivo tem um conjunto finito de estados

$$Q = \{f, t, m, w, a\},$$

são eles:

(f) porta está fechada;

(t) verificando temperatura;

(m) verificando uso de máscara;

(w) aguardando;

(a) e porta está aberta.

Além disso, os sensores fornecem um alfabeto de entradas

$$\Sigma = \{0, 1, 2, 3, 4, 5, 6\}$$

que são:

(0) não há presença de pessoa;

(1) há presença de pessoa;

(2) temperatura menor que $37,5$ graus Celcius;

(3) temperatura maior ou igual a $37,5$ graus Celcius;

(4) usando máscara corretamente;

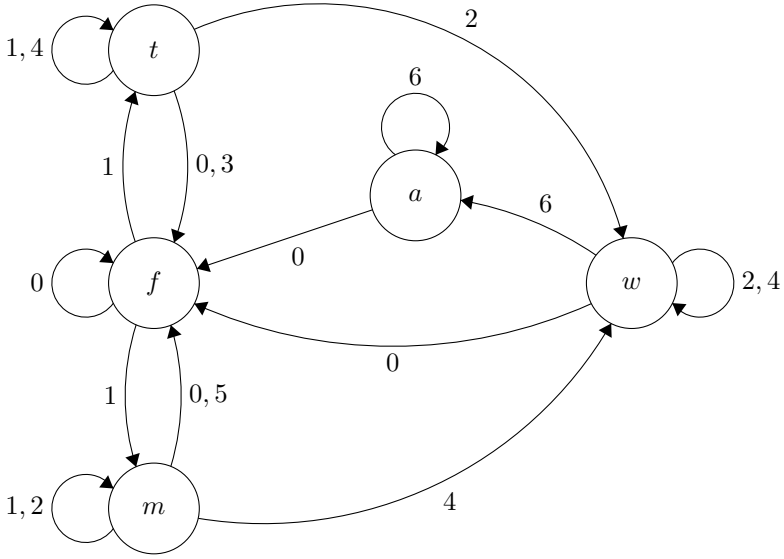
(5) não usando ou uso incorreto de máscara;

(6) temperatura e uso de máscara validados para permitir a passagem.

Do mesmo modo que em um semiautômato determinístico, em que temos os conjuntos de estados e entradas, também teremos a função de transição. No entanto, ela tem uma sutil diferença que ilustraremos usando o diagrama do semiautômato na Figura 8. Agora, se a porta está fechada e há a presença de um indivíduo na frente dela, então o dispositivo deve simultaneamente verificar sua temperatura

corporal e o uso da máscara facial. Nesse caso, quando o dispositivo está no estado "porta está fechada" (f) e recebe a entrada "há presença de pessoa" (1), ele muda ao mesmo tempo para os estados "verificando temperatura" (t) e "verificando uso de máscara" (m). Por outro lado, se a porta automática está no estado "aguardando" (w) e recebe a entrada "há presença de pessoa" (1), então não existe um estado definido para o qual deve mudar.

Figura 8 – Representação do funcionamento de uma porta automática com sensores que verificam temperatura corporal e uso de máscara facial



Enquanto que em um semiautômato determinístico para todo estado e toda entrada existe um único estado alcançado, no semiautômato representado na Figura 8, para todo estado e toda entrada

podem existir nenhum, um único ou mais estados alcançados, isto é, um subconjunto de estados. Nesse caso, cada símbolo do alfabeto rotula nenhuma, uma ou mais setas com origem em um estado (nó) e destino e outro em seu diagrama de estados. Assim, a imagem da função de transição é o conjunto das partes do conjunto de estados, o que justifica a seguinte definição:

Definição 3.19. Um *semiautômato não determinístico* é uma tripla (Q, Σ, δ) em que

(i) Q é um conjunto finito e não vazio de elementos chamados de *estados*;

(ii) Σ é um alfabeto de símbolos chamados de *entradas*;

(iii) $\delta : Q \times \Sigma \longrightarrow \mathcal{P}(Q)$ é a *função transição* que descreve como acontece a mudança de estado dependendo da entrada.

Exemplo 3.14. O dispositivo representado na Figura 8 é um semiautômato não determinístico $N = (Q, \Sigma, \delta)$ em que $Q = \{f, t, m, w, a\}$, $\Sigma = \{0, 1, 2, 3, 4, 5, 6\}$ e δ é dada pela seguinte tabela de transição

Tabela 7 – Tabela de transição do semiautômato N

N	f	t	m	w	a
0	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$	$\{f\}$
1	$\{t, m\}$	$\{t\}$	$\{m\}$	$\emptyset$	$\emptyset$
2	$\emptyset$	$\{w\}$	$\{m\}$	$\{w\}$	$\emptyset$
3	$\emptyset$	$\{f\}$	$\emptyset$	$\emptyset$	$\emptyset$
4	$\emptyset$	$\{t\}$	$\{w\}$	$\{w\}$	$\emptyset$
5	$\emptyset$	$\emptyset$	$\{f\}$	$\emptyset$	$\emptyset$
6	$\emptyset$	$\emptyset$	$\emptyset$	$\{a\}$	$\{a\}$

Analogamente com o que acontece nos semiautômatos determinísticos, podemos representar a função transição dos semiautômatos não determinísticos por $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{B}_Q$, em que $\mathcal{B}_Q$ é o conjunto de todas as relações binárias em Q.

Exemplo 3.15. Para o semiautômato não determinístico N do Exemplo 3.14 temos que

$$\delta_0 = \begin{pmatrix} f & t & m & w & a \\ f & f & f & f & f \end{pmatrix}, \qquad \delta_1 = \begin{pmatrix} f & f & t & m \\ t & m & t & m \end{pmatrix},$$
$$\delta_2 = \begin{pmatrix} t & m & w \\ w & m & w \end{pmatrix}, \qquad \delta_3 = \begin{pmatrix} t \\ f \end{pmatrix},$$
$$\delta_4 = \begin{pmatrix} t & m & w \\ t & w & w \end{pmatrix}, \qquad \delta_5 = \begin{pmatrix} m \\ f \end{pmatrix},$$
$$\delta_6 = \begin{pmatrix} w & a \\ a & a \end{pmatrix}.$$

Logo $\delta = \{\delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6\}$.

Os semiautômatos determinísticos são usados para descrever o comportamento de dispositivos que executam tarefas de modo sequencial, enquanto que os semiautômatos não determinísticos são capazes de descrever o comportamento de dispositivos que executam mais que uma tarefa paralelamente.

Diversos processos podem ser descritos por um semiautômato. Além dos Exemplos 3.12 e 3.14, relacionados com portas automáticas, podemos usar um semiautômato para descrever o processo de aprendizagem das proposições e teoremas desse trabalho. Para tanto tomemos o conjunto de as proposições e teoremas como o conjunto de estados do semiautômato e os processos “aprendendo” e “aprendido” as entradas de seu alfabeto.

3.3 AUTÔMATO

Semiautômatos são capazes de descrever procedimentos que mudam seu estado dependendo de um valor de entrada. No entanto, não são capazes de descrever mecanismos que possuem um estado inicial

e geram saídas como resultado de algum processamento. Para tanto, outros modelos computacionais são necessários, como, por exemplo, os *autômatos*, também chamados de *reconhecedores* e, assim como os semiautômatos, podem ser determinísticos ou não determinísticos.

3.3.1 Autômato Determinístico

Definição 3.20. Um *autômato determinístico* é uma quíntupla

$$(Q, \Sigma, \delta, q_0, F)$$

em que

(i) Q é um conjunto finito e não vazio de elementos chamados de *estados*;

(ii) Σ é um alfabeto de símbolos chamados de *entradas*;

(iii) $\delta : Q \times \Sigma \longrightarrow Q$ é a *função transição* que descreve como acontece a mudança de estado dependendo da entrada;

(iv) $q_0 \in Q$ é o *estado inicial*;

(v) $F \subseteq Q$ é o *conjunto de estados aceitos*.

Os autômatos são conhecidos como reconhecedores pois são usados para classificar (ou reconhecer) *strings* de seu alfabeto (Ginzburg [4, p. 55]). Intuitivamente, dizemos que um autômato determinístico reconhece uma *string*, se ao final de seu processamento, terminar em um de seus estados aceitos.

Definição 3.21. Seja $M = (Q, \Sigma, \delta, q_0, F)$ um autômato determinístico e $w = w_1 w_2 \dots w_k \in \Sigma^*$ com $w_i \in \Sigma$ para $1 \leq i \leq k$. Chamamos de *computação de w em M*, ou equivalentemente dizemos que *M computa w* (ou *w é computada por M*), ou ainda dizemos que w é uma

string de entrada de M, se existe uma sequencia de estados r_0, r_1, r_2, $\ldots$, r_k, com $r_i \in Q$ para $0 \leq i \leq k$ tal que:

(i) $r_0 = q_0$;

(ii) $\delta(r_i, w_{i+1}) = r_{i+1}$ para $0 \leq i \leq k-1$.

Se, além disso, $r_k \in F$, então dizemos que M *reconhece (ou aceita)* w.

Exemplo 3.16. Considere o autômato determinístico

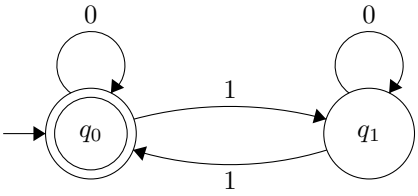
$$M_1 = (Q, \Sigma, \delta, q_0, F)$$

em que $Q = \{q_0, q_1\}$, $\Sigma = \{0, 1\}$, $F = \{q_0\}$ e δ é dada por

$$\delta(q_0, 0) = q_0$$
$$\delta(q_0, 1) = q_1$$
$$\delta(q_1, 0) = q_1$$
$$\delta(q_1, 1) = q_0.$$

Note que M_1 reconhece a *string* 110000101, mas não reconhece a *string* 100000101. A Figura 9 apresenta o diagrama de estados do autômato M_1.

Figura 9 – Diagrama de estados do autômato M_1



Note que para todo estado e toda entrada o autômato M_1 do Exemplo 3.16, representado na Figura 9, existe um único estado alcançado. Assim, do mesmo modo que acontece com um semiautômato

determinístico, cada símbolo do alfabeto rotula uma única seta com origem em um estado (nó) e destino em outro no seu diagrama de estados. Além disso, o estado inicial é o nó marcado com uma seta sem rótulo e sem nó de origem apontando para ele; e, o estado aceito é representado por um circulo duplo.

Definição 3.22. Seja $M = (Q, \Sigma, \delta, q_0, F)$ um autômato determinístico e seja A uma linguagem sobre Σ. Se M aceita todas as *strings* de A, então dizemos que M *reconhece* A.

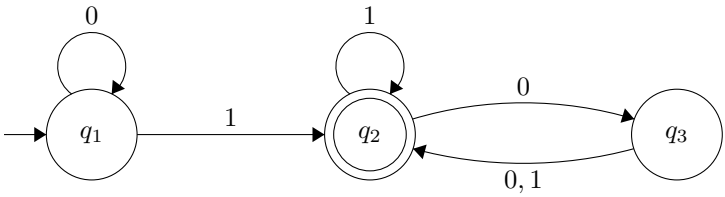
Exemplo 3.17. O autômato M_1 do Exemplo 3.16 reconhece a linguagem $A = \{11, 1111, 111111, 1100, 1010101\}$.

Definição 3.23. Seja $M = (Q, \Sigma, \delta, q_0, F)$ um autômato determinístico. Denotamos por $L(M)$ a linguagem sobre Σ de todas as *strings* aceitas por M. Se M não aceita *string* alguma, então $L(M) = \emptyset$. Chamamos $L(M)$ de *linguagem do autômato determinístico* M.

Exemplo 3.18. Considere o autômato M_1 do Exemplo 3.16, temos que $L(M_1) = \{w \in \Sigma^*; |w|_1 \equiv 0 \mod 2\}$ é a linguagem sobre Σ cujas *strings* possuem uma quantidade par de símbolos 1.

Exemplo 3.19. Considere o autômato determinístico M_2 representado através de seu diagrama de estados na Figura 10

Figura 10 – Diagrama de estados do autômato M_2

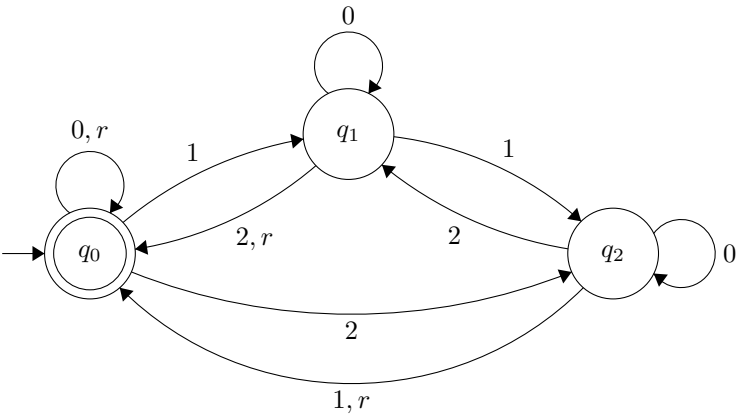


Note que

$$L(M_2) = \{w \in \Sigma^* ;\ 1 \text{ é fator de } w, \text{ e tem uma quantidade par de símbolos 0 seguindo a última ocorrência do símbolo 1 em } w\}.$$

Suponha, por exemplo um autômato determinístico $M_3 = (Q, \Sigma, \delta, q_0, F)$ em que $Q = \{q_0, q_1, q_2\}$, $\Sigma = \{\mathrm{r}, 0, 1, 2\}$ e $F = \{q_0\}$. Digamos que queremos construir M_3 de tal modo que seja capaz de verificar se a soma dos símbolos de uma *string* sobre Σ tenha resto zero na divisão por 3. Além do mais, toda vez que M_3 ler o símbolo r deve reiniciar a soma. A primeira vista, temos a impressão que não é possível resolver este problema com um autômato determinístico pois parece que necessitamos de uma quantidade ilimitada de memória uma vez que não restringimos o tamanho da *string* a ser lida, o que implica que teríamos infinitas possibilidades. No entanto basta notarmos que para qualquer número natural, o resto de sua divisão por três é sempre 0, 1 ou 2. Com este fato podemos construir o diagrama de estados para M_3 na Figura 11.

Figura 11 – Diagrama de estados do autômato M_3



Note que cada estado de M_3 representa o resto atual da divisão por 3 e cada símbolo 0, 1 ou 2 representa o valor que é adicionado ao valor acumulado. Na Tabela 8 temos a tabela de transição de M_3.

Tabela 8 – Tabela de transição do autômato determinístico M_3

M_3	q_0	q_1	q_2
r	q_0	q_0	q_0
0	q_0	q_1	q_2
1	q_1	q_2	q_0
2	q_2	q_0	q_1

Partindo de M_3 e usando as ideias para sua construção, podemos generalizá-lo e criar o autômato determinístico

$$M_i = (Q_i, \Sigma, \delta_i, q_0, F)$$

com Σ e F idênticos ao de M_3, que verifica se a soma dos símbolos de uma *string* de Σ tem resto zero na divisão por $i \in \mathbb{N}$ com $i > 0$. Sabe-se que a divisão de um número natural qualquer por i terá um

resto r entre 0 e $i-1$ ($0 \leq r \leq i-1$). Assim, como o conjunto de estados representam os restos possíveis, temos $Q_i = \{q_0, q_1, \ldots, q_{i-1}\}$.

Note que apesar de podermos construir o diagrama de estados de M_i para qualquer $i > 0$ dado, quando i tem um valor muito grande, tal tarefa torna-se inviável, assim como a construção de uma tabela para a função δ_i. Mas podemos manter a generalização se definirmos a função δ_i por partes, para todo $q_j \in Q_i$ e todo $a \in \Sigma$, da seguinte maneira:

$$\delta_i(q_j, a) = \begin{cases} q_0 & \text{se } a = \text{r} \\ q_j & \text{se } a = 0 \\ q_{j+1} & \text{se } a = 1 \text{ e } j < i-1 \\ q_0 & \text{se } a = 1 \text{ e } j = i-1 \\ q_{j+2} & \text{se } a = 2 \text{ e } j < i-2 \\ q_0 & \text{se } a = 2 \text{ e } j = i-2 \\ q_1 & \text{se } a = 2 \text{ e } j = i-1. \end{cases}$$

Definição 3.24. Uma linguagem é chamada de *linguagem regular* se existe algum autômato determinístico que a reconhece.

Exemplo 3.20. Consideremos as seguintes linguagens sobre o alfabeto $\Sigma = \{0, 1\}$

$$\begin{aligned} L_1 =& \{w \in \Sigma^*; |w|_1 \equiv 1 \mod 2\} \\ L_2 =& \{w \in \Sigma^*; 001 \text{ é fator de } w\} \\ L_3 =& \{w \in \Sigma^*; 0 \text{ é sufixo de } w \text{ ou } |w|_1 \equiv 0 \mod 2\} \end{aligned}$$

Conseguimos construir os autômatos determinísticos D_1, D_2 e D_3, dados pelos diagramas de estados das Figuras 12, 13 e 14, que reconhecem as linguagens L_1, L_2 e L_3 respectivamente. Logo L_1, L_2 e L_3 são linguagens regulares.

Figura 12 – Diagrama de estados do autômato D_1

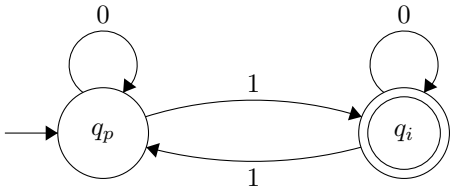


Figura 13 – Diagrama de estados do autômato D_2

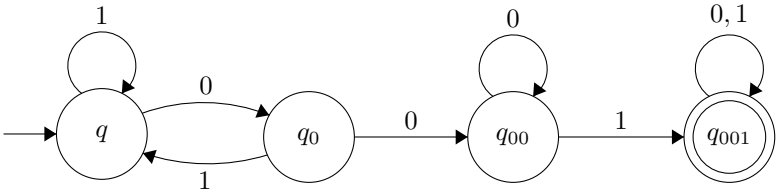
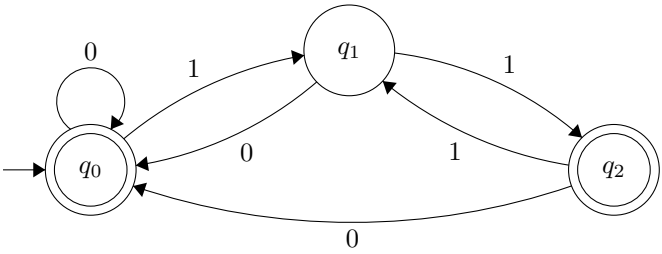


Figura 14 – Diagrama de estados do autômato D_3



3.3.2 Autômato Não Determinístico

Assim como no caso dos semiautômatos, também para os autômatos temos aqueles que são denominados como *não determinísticos*, que analogamente aos semiautômatos não determinísticos, são capazes de computar uma mesma *string* de seu alfabeto por mais de um estado simultaneamente.

Definição 3.25. Um *autômato não determinístico* é uma quíntupla $(Q, \Sigma, \delta, q_0, F)$ em que

(i) Q é um conjunto finito e não vazio de elementos chamados de *estados*;

(ii) Σ é um alfabeto de símbolos chamados de *entradas*;

(iii) $\delta : Q \times \Sigma_\varepsilon \longrightarrow \mathcal{P}(Q)$ é a *função transição* que descreve como acontece a mudança de estado dependendo da entrada com $\Sigma_\varepsilon = \Sigma \cup \{\varepsilon\}$ em que ε é um símbolo não pertencente ao alfabeto Σ chamado de *símbolo nulo* (ou *símbolo em branco*);

(iv) $q_0 \in Q$ é o *estado inicial*;

(v) $F \subseteq Q$ é o *conjunto de estados aceitos*.

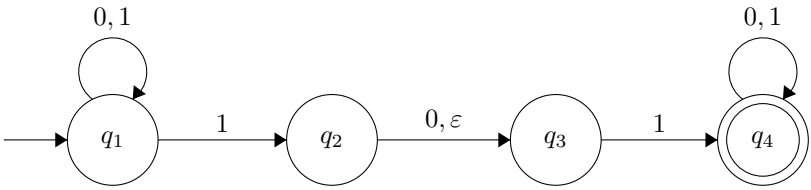
No caso de um autômato determinístico, dado um símbolo do alfabeto e um estado do conjunto de estados, a função transição nos retorna exatamente um determinado estado. Já o autômato não determinístico, retorna um subconjunto de estados. Além disso, o domínio de sua função transição possui o símbolo nulo unido ao alfabeto Σ em $Q \times \Sigma_\varepsilon$. Veremos a "utilidade" desse símbolo através de alguns exemplos e da definição de computação de *strings* em autômatos não determinísticos.

Exemplo 3.21. Seja $N_1 = (Q, \{0,1\}, \delta, q_1, \{q_4\})$ um autômato não determinístico com $Q = \{q_1, q_2, q_3, q_4\}$ e δ dada pela Tabela 9, cujo diagrama de estados é representado na Figura 15.

Tabela 9 – Tabela de transição do autômato N_1

N_1	0	1	ε
q_1	$\{q_1\}$	$\{q_1, q_2\}$	$\emptyset$
q_2	$\{q_3\}$	$\emptyset$	$\{q_3\}$
q_3	$\emptyset$	$\{q_4\}$	$\emptyset$
q_4	$\{q_4\}$	$\{q_4\}$	$\emptyset$

Figura 15 – Diagrama de estados do autômato N_1



Note que cada estado e cada símbolo do alfabeto de entrada e o símbolo nulo ε do autômato N_1 do Exemplo 3.21, cujo diagrama de estados está representado na Figura 15, podem existir nenhum, um ou mais estados alcançados por setas, isto é, um subconjunto de estados. Nesse caso, cada símbolo do alfabeto e o símbolo nulo ε rotula nenhuma, uma ou mais setas com origem em um estado (nó) e destino e outro em seu diagrama de estados. O estado inicial é o nó marcado com uma seta sem rótulo sem nó de origem apontando para ele; e, o estado aceito é representado por um circulo duplo.

Definição 3.26. Seja $N = (Q, \Sigma, \delta, q_0, F)$ um autômato não determinístico e $w \in \Sigma^*$. Chamamos de *computação de w em N*, ou equivalentemente dizemos que N *computa* w (ou w *é computada por* N),

ou ainda dizemos que w é uma *string de entrada* de N, se w pode ser escrito como $w = y_1 y_2 \dots y_m$ em que $y_i \in \Sigma_\varepsilon$ para $1 \leq i \leq m$ e existe uma sequencia de estados r_0, r_1, r_2, $\dots$, r_m, com $r_i \in Q$ para $0 \leq i \leq m$ tal que:

(i) $r_0 = q_0$;

(ii) $r_{i+1} \in \delta(r_i, y_{i+1})$ para $0 \leq i \leq m-1$;

Se, além disso, $r_m \in F$, então dizemos que N *reconhece (ou aceita)* w.

Definição 3.27. Seja $N = (Q, \Sigma, \delta, q_0, F)$ um autômato não determinístico e seja A uma linguagem sobre Σ. Se N aceita todas as *strings* de A, então dizemos que N *reconhece* A.

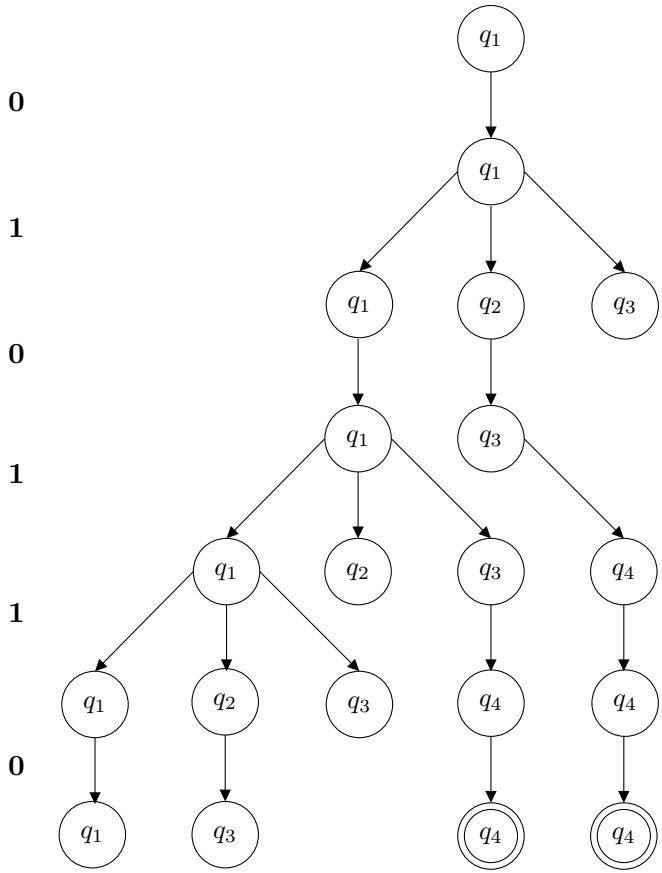
Definição 3.28. Seja $N = (Q, \Sigma, \delta, q_0, F)$ um autômato não determinístico. Denotamos por $L(N)$ a linguagem sobre Σ de todas as *strings* aceitas por N. Se N não aceita *string* alguma, então $L(N) = \emptyset$. Chamamos $L(N)$ de *linguagem do autômato não determinístico* N.

Sejam N e w da definição 3.26. Ao computar w, o autômato N pode se dividir em várias cópias dele mesmo seguindo uma execução em paralelo para cada estado retornado pela função transição δ. Se o símbolo lido não tem uma seta que aponte para outro estado então a função transição δ têm como resultado $\emptyset \subset \mathcal{P}(Q)$ e neste caso o processo paralelo termina a execução. Caso a função transição δ retorne um valor diferente de $\emptyset \subset \mathcal{P}(Q)$ para o estado atual e o símbolo nulo ε então N se dividi em várias cópias dele mesmo seguindo uma execução em paralelo para cada estado retornado pela função transição δ e mantém uma cópia no estado atual. Ao fim da leitura de w, se pelo menos uma das cópias de N terminar em um estado aceito então N aceita w.

A computação de um autômato não determinístico pode ser pensado por meio de uma árvore de decisão.

Exemplo 3.22. Tome a *string* 010110 para ser computada pelo autômato N_1 do Exemplo 3.21. Esta computação é representada na árvore de decisão da Figura 16.

Figura 16 – Computação da *string* 010110 em N_1



Como duas cópias de N_1 terminam no estado aceito q_4 então a

string 010110 é aceita. Note que

$$L(N_1) = \{a \in \{0,1\}^*; 101 \text{ ou } 11 \text{ são fatores de } a\}.$$

Definição 3.29. Seja $N = (Q, \Sigma, \delta, q_0, F)$ um autômato não determinístico e $R \subseteq Q$. Denotamos por $E(R)$ o conjunto de estados de modo que,

$$E(R) = \begin{cases} R & \text{se } \forall\, r \in R, \delta(r, \varepsilon) = \emptyset \\ R \cup E(\bigcup_{r \in R} \delta(r, \varepsilon)) & \text{se } \exists\, r \in R;\ \delta(r, \varepsilon) \neq \emptyset \end{cases}$$

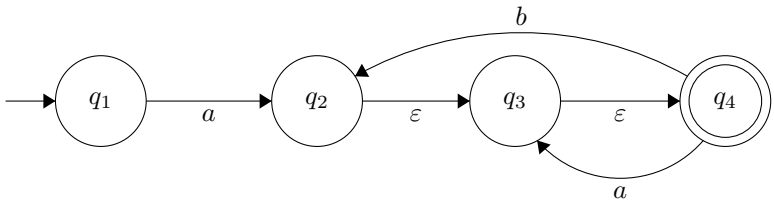
Graficamente, $E(R)$ é o conjunto de estados que podem ser alcançados a partir dos elementos de R ao longo das setas rotuladas com ε unido com conjunto R.

Exemplo 3.23. Considere o autômato não determinístico N_1 do Exemplo 3.21. Então $E(\{q_1\}) = \{q_1\}$, $E(\{q_2\}) = \{q_2, q_3\}$, $E(\{q_1, q_2\}) = \{q_1, q_2, q_3\}$ e $E(\{q_1, q_2, q_3\}) = \{q_1, q_2, q_3\}$.

Caso o autômato não determinístico tenha, em seu diagrama de estados, consecutivos estados ligados por setas rotuladas com ε partindo de um estado q qualquer, então $E(\{q\})$ retornará o conjunto de todos os estados consecutivos ligados por ε partindo de q, inclusive o próprio q. Este fato é previsto pela recursividade de $E(R)$ dado na Definição 3.29.

Exemplo 3.24. Seja N_E um autômato não determinístico com o conjunto de estados $Q_E = \{q_1, q_2, q_3, q_4\}$ representado na Figura 17.

Figura 17 – Diagrama de estados do autômato N_E



Note que $E(\{q_1\}) = \{q_1\}$ e $E(\{q_2\}) = \{q_2, q_3, q_4\}$.

3.3.3 Autômatos Equivalentes

Definição 3.30. Sejam M e N dois autômatos (determinísticos ou não determinísticos) quaisquer. Dizemos que M e N são *equivalentes* se $L(M) = L(N)$, ou seja, se reconhecem as mesmas linguagens.

Teorema 3.1. *Para todo autômato não determinístico existe um autômato determinístico equivalente.*

Demonstração. Seja $N = (Q, \Sigma, \delta, q_0, F)$ um autômato não determinístico, então devemos encontrar um autômato determinístico $D = (Q_D, \Sigma, \delta_D, q_{D0}, F_D)$ tal que $L(D) = L(N)$. Para tanto, podemos construir D da seguinte maneira:

(i) $Q_D = \mathcal{P}(Q)$: cada estado de D corresponde a um elemento de $\mathcal{P}(Q)$, isto é, cada estado de D é um subconjunto de Q. Assim, se Q tem k estados então Q_D terá 2^k estados.

(ii) Para todo $R \in Q_D$ e todo $a \in \Sigma$, $\delta_D(R, a) = \{q \in Q; q \in E(\delta(r, a)), \forall\, r \in R\} = \bigcup_{r \in R} E(\delta(r, a))$: note que como R é um estado de D, é também um subconjunto de estados de N.

(iii) $q_{D0} = E(\{q_0\})$

(iv) $F_D = \{R \in Q_D; \exists\, f \in F; f \in R\}$: assim $F_D \subseteq Q_D$ tal que para todo $R \in F_D$, R contém pelo menos um estado aceito de N.

Construído desta maneira, a cada passo de sua computação sobre uma *string* de entrada qualquer, D alcança um único estado determinado que corresponde a um subconjunto de estados de N. Logo D, de fato, é um autômato determinístico.

Como toda *string* $w \in L(N)$ é aceita por N, ela pode ser escrita como $w = y_1 y_2 \dots y_m$ em que $y_i \in \Sigma_\varepsilon$ para $1 \leq i \leq m$, existindo uma sequencia de estados r_0, r_1, r_2, $\dots$, r_m com $r_i \in Q$ para $0 \leq i \leq m$ tal que

(i) $r_0 = q_0$

(ii) $r_{i+1} \in \delta(r_i, y_{i+1})$ para $0 \leq i \leq m-1$

(iii) $r_m \in F$.

Seja k a quantidade de ocorrências do símbolo ε em $y_1 y_2 \dots y_m = w$. Assim, podemos escrever $w = w_1 w_2 \dots w_{m-k}$ em que $w_i \in \Sigma$ para $1 \leq i \leq m-k$. Façamos corresponder a cada w_i a i-ésima ocorrência de $y_j \neq \varepsilon$ com $1 \leq j \leq m$ e denotamos $y_j = w_i = y_{w_i}$. Logo $w = y_{w_1} y_{w_2} \dots y_{w_{m-k}}$. Denotamos também $r_j = r_{w_i}$ para todo índice j tal que w_i corresponde a i-ésima ocorrência de $y_j \neq \varepsilon$. Logo existe a sequencia de estados $R_0 = E(\{r_0\})$, $R_1 = E(\{r_{w_1}\})$, $R_2 = E(\{r_{w_2}\})$, $\dots$, $R_{m-k} = E(\{r_{w_{m-k}}\})$ com $R_i \in Q_D$ para $0 \leq i \leq m-k$ tal que

(i) $R_0 = E(\{q_0\} = q_{D0}$

(ii) $\delta(R_i, w_{i+1}) = R_{i+1}$ para $0 \leq i \leq m-k-1$

(iii) $R_{m-k} \in F_D$

Logo D reconhece w.

Caso $w \notin L(N)$, isto é, N não reconheça w, não conseguimos encontrar uma sequencia de estados que atenda os critérios para aceitação de w por N. Logo também não é possível encontrar uma sequencia que satisfaça os critérios de aceitação de w por D. O que implica que, neste caso, D não reconhece w.

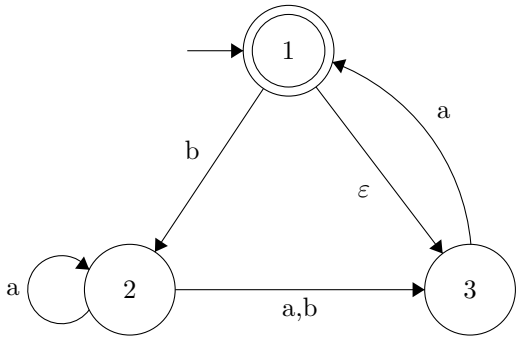
Portanto todo $w \in L(N)$ é aceita por D e toda $w \notin L(N)$ não é aceita por D logo $L(N) = L(D)$, isto é, D é equivalente a N. ■

Exemplo 3.25. Seja $N_2 = (\{1, 2, 3\}, \{\text{a}, \text{b}\}, \delta, 1, \{1\})$ um autômato não determinístico com δ dada pela Tabela 10, cujo diagrama de estados é representado na Figura 18.

Tabela 10 – Tabela de transição do autômato não determinístico N_2

N_2	a	b	ε
1	$\emptyset$	$\{2\}$	$\{1, 3\}$
2	$\{2, 3\}$	$\{3\}$	$\emptyset$
3	$\{1\}$	$\emptyset$	$\emptyset$

Figura 18 – Diagrama de estados do autômato N_2



Note que N_2 reconhece as *strings* ε, a, baba, baa mas não reconhece b, bb, babba. Usaremos este autômato não determinístico

para ilustrar o processo de construção de um autômato determinístico equivalente, conforme realizado na demonstração do Teorema 3.1. Construiremos $D_4 = (Q_{D_4}, \{\mathrm{a}, \mathrm{b}\}, \delta_{D_4}, q_{D_4 0}, F_{D_4})$ em que

(i) $Q_{D_4} = \mathcal{P}(\{1, 2, 3\})$

(ii) δ_{D_4} dada pela Tabela 11.

Tabela 11 – Tabela de transição do autômato D_4

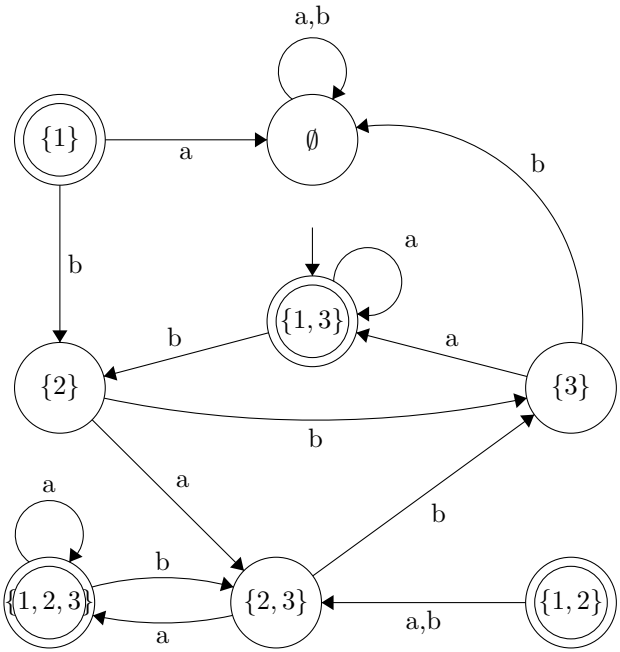
D_4	a	b
$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{2\}$
$\{2\}$	$\{2, 3\}$	$\{3\}$
$\{3\}$	$\{1, 3\}$	$\emptyset$
$\{1, 2\}$	$\{2, 3\}$	$\{2, 3\}$
$\{1, 3\}$	$\{1, 3\}$	$\{2\}$
$\{2, 3\}$	$\{1, 2, 3\}$	$\{3\}$
$\{1, 2, 3\}$	$\{1, 2, 3\}$	$\{2, 3\}$

(iii) $q_{D_4 0} = E(\{1\}) = \{1, 3\}$

(iv) $F_{D_4} = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$.

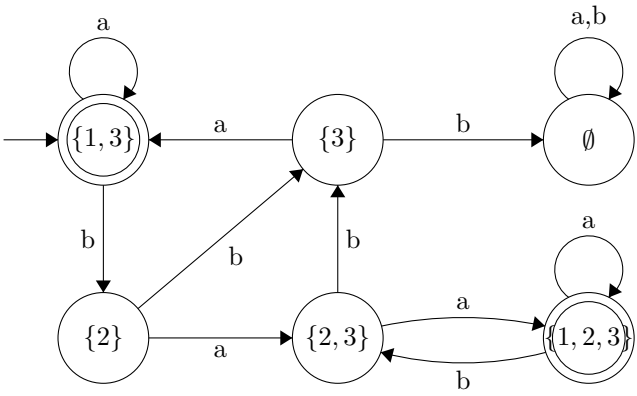
Obtendo o diagrama de estados para D_4 conforme a Figura 19.

Figura 19 – Diagrama de estados do autômato D_4



Ainda, observando o diagrama de estados do autômato D_4, na Figura 19, vemos que nenhum dos estados tem seta apontando para os estados $\{1\}$ e $\{1,2\}$, ou seja, estes estados não pertencem a imagem da função δ_{D_3}. Assim o autômato D_4 (equivalente a N_2) pode ser adaptado conforme o diagrama de estados na Figura 20.

Figura 20 – Diagrama de estados do autômato D_4 adaptado



Do mesmo modo que, de acordo com o Teorema 3.1, para todo autômato não determinístico existe um autômato determinístico equivalente, também é válido afirmar que para todo autômato determinístico existe um autômato não determinístico equivalente. Nesse caso, a prova é trivial, uma vez que todo autômato determinístico pode ser visto como um tipo particular de autômato não determinístico. Basta, para tanto, uma modificação na imagem da função transição em que cada elemento do contradomínio (conjunto de estados) é relacionado com o subconjunto do conjunto de estados que contém um único elemento.

Corolário 3.1. *Uma linguagem é regular se, e somente se, existe algum autômato não determinístico que a reconhece.*

Demonstração. Pela Definição 3.24, uma linguagem é regular se, e somente se, existe algum autômato determinístico que a reconhece, mas o autômato determinístico é um tipo particular de autômato não

determinístico. Logo exite uma autômato não determinístico que a reconhece.

Reciprocamente, seja N um autômato não determinístico que reconhece a linguagem $A \subseteq L(N)$. Pelo Teorema 3.1, existe um autômato determinístico D equivalente a N. Portanto $A \subseteq L(N) = L(D)$. Consequentemente D reconhece A. Logo A é uma linguagem regular. ■

Notação 3.1. Sejam A e B linguagens. Denotamos

(i) a *união* de A com B pelo conjunto $A \cup B = \{x; x \in A \text{ ou } x \in B\}$;

(ii) a *concatenação* de A com B pelo conjunto $AB = \{xy; x \in A \text{ e } y \in B\}$;

(iii) A *estrela* pelo conjunto $A^* = \{\varepsilon\} \cup \{x_1 x_2 \dots x_k; k \in \mathbb{N}, x_k \in A\}$.

Exemplo 3.26. Seja $\Sigma = \{\mathrm{a}, \mathrm{b}, \dots, \mathrm{z}\}$ o alfabeto português com 26 letras minúsculas. E sejam $A = \{\text{flor}, \text{casa}\}$ e $B = \{\text{azul}, \text{bonita}\}$ linguagens sobre Σ, então

(i) $A \cup B = \{\text{flor}, \text{casa}, \text{azul}, \text{bonita}\}$

(ii) $AB = \{\text{florazul}, \text{florbonita}, \text{casaazul}, \text{casabonita}\}$

(iii) $A^* = \{\varepsilon, \text{flor}, \text{casa}, \text{florcasa}, \text{florflor}, \text{casaflor}, \text{casacasa}, \dots\}$

Note que se L e $\emptyset$ são linguagens ($\emptyset$ é a linguagem vazia), então $L\emptyset = \emptyset = \emptyset L$ e que $\emptyset^* = \{\varepsilon\}$.

Teorema 3.2. *Se A e B são linguagens regulares então $A \cup B$ é linguagem regular.*

Demonstração. Tome os autômatos não determinísticos

$$N_1 = (Q_1, \Sigma_1, \delta_1, q_1, F_1)$$

e

$$N_2 = (Q_2, \Sigma_2, \delta_2, q_2, F_2)$$

que reconhecem as linguagens A e B respectivamente. Do Corolário 3.1 se existir um autômato não determinístico que reconheça a união de A com B, então $A \cup B$ é uma linguagem regular.

Construímos o autômato não determinístico

$$N_U = (Q, \Sigma, \delta, q_0, F)$$

que reconhece $A \cup B$ da seguinte maneira

(i) $Q = \{q_0\} \cup Q_1 \cup Q_2$

(ii) $\Sigma = \Sigma_1 \cup \Sigma_2$

(iii) q_0 é o estado inicial de N_U

(iv) $\forall\, q \in Q$ e $\forall\, a \in \Sigma_\varepsilon$

$$\delta(q,a) = \begin{cases} \delta_1(q,a) & \text{se } q \in Q_1 \\ \delta_2(q,a) & \text{se } q \in Q_2 \\ \{q_1, q_2\} & \text{se } q = q_0 \text{ e } a = \varepsilon \\ \emptyset & \text{se } q = q_0 \text{ e } a \neq \varepsilon \end{cases}$$

(v) $F = F_1 \cup F_2$

■

Afim de elucidar a ideia da demonstração do Teorema 3.2, faremos os esquemas dos diagramas de estados dos autômatos N_1 e N_2 e partindo deles montaremos o esquema do diagrama de estados do autômato N_U conforme a demonstração.

Figura 21 – Esquema do diagrama de estados do autômato N_1

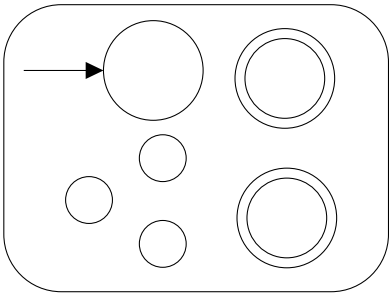
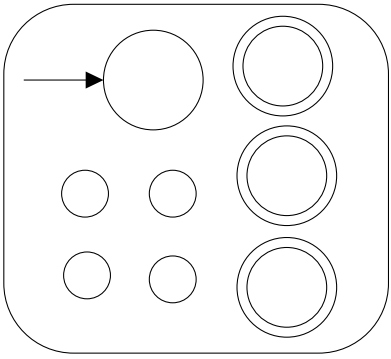
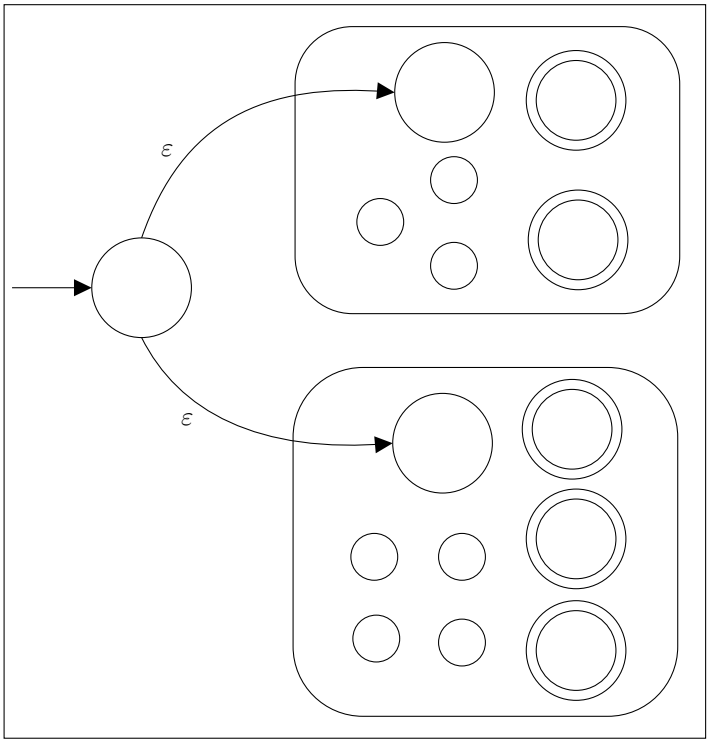


Figura 22 – Esquema do diagrama de estados do autômato N_2



O autômato não determinístico N_U que reconhece a linguagem $A \cup B$ do Teorema 3.2 é construído de acordo com a demonstração conforme a Figura 23.

Figura 23 – Esquema do diagrama de estados do autômato N_U



Assim toda *string* computada por N_U executa simultaneamente a computação da mesma *string* em N_1 e N_2. Note que toda $s \in A \cup B$ é aceita por N_1 ou por N_2, portanto é aceita por N_U. Logo N reconhece $A \cup B$, o que implica que $A \cup B$ é uma linguagem regular.

Teorema 3.3. *Se A e B são linguagens regulares então AB é linguagem regular.*

Demonstração. Tome os autômatos não determinísticos

$$N_1 = (Q_1, \Sigma_1, \delta_1, q_1, F_1)$$

e

$$N_2 = (Q_2, \Sigma_2, \delta_2, q_2, F_2)$$

que reconhecem as linguagens A e B respectivamente. Do Corolário 3.1 se existir um autômato não determinístico que reconheça a concatenação de A com B, então AB é uma linguagem regular.

Construímos o autômato não determinístico

$$N_C = (Q, \Sigma, \delta, q_1, F_2)$$

que reconhece AB da seguinte maneira

(i) $Q = Q_1 \cup Q_2$

(ii) $\Sigma = \Sigma_1 \cup \Sigma_2$

(iii) q_1 é o estado inicial de N_C

(iv) $\forall\, q \in Q$ e $\forall\, a \in \Sigma_\varepsilon$

$$\delta(q,a) = \begin{cases} \delta_1(q,a) & \text{se } q \in Q_1 - F_1 \\ \delta_1(q,a) & \text{se } q \in F_1 \text{ e } a \neq \varepsilon \\ \delta_1(q,a) \cup \{q_2\} & \text{se } q \in F_1 \text{ e } a = \varepsilon \\ \delta_2(q,a) & \text{se } q \in Q_2 \end{cases}$$

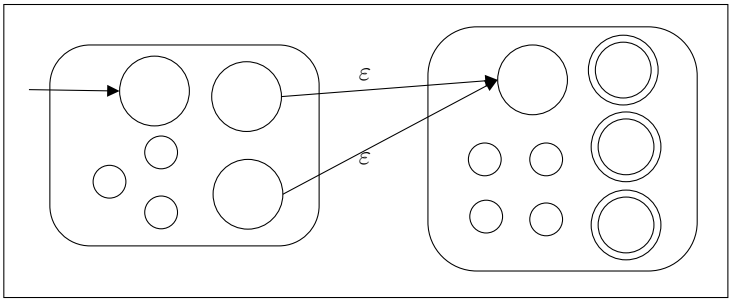
(v) F_2 é o conjunto de estados aceitos de N

■

Sejam A e B as linguagens regulares reconhecidas pelos autômatos não determinísticos N_1 e N_2 da demonstração do Teorema 3.3 respectivamente, então a *string* $s \in AB$ pode ser escrita como $s = s_1 s_2$

em que $s_1 \in A$ e $s_2 \in B$, isto é, N_1 aceita s_1 e N_2 aceita s_2. Portanto, pode-se concluir que a "quebra" de s ocorre em algum estado aceito de N_1 na computação de s. Usando os esquemas dos diagramas de estados dos autômatos N_1 e N_2 apresentados nas Figuras 21 e 22 respectivamente, pode-se construir o autômato não determinístico N_C do Teorema 3.3 conforme o esquema da Figura 24.

Figura 24 – Esquema do diagrama de estados do autômato N_C



Teorema 3.4. *Se A é linguagem regular então A^* é linguagem regular.*

Demonstração. Tome o autômato não determinístico

$$N_1 = (Q_1, \Sigma_1, \delta_1, q_1, F_1)$$

que reconhece a linguagem A. Do Corolário 3.1 se existir um autômato não determinístico que reconheça A^*, então A^* é uma linguagem regular.

Construímos o autômato não determinístico

$$N_E = (Q, \Sigma, \delta, q_0, F)$$

que reconhece A^* da seguinte maneira

(i) $Q = Q_1 \cup \{q_0\}$

(ii) Σ é o alfabeto de N_E

(iii) q_0 é o estado inicial de N_E

(iv) $\forall\, q \in Q$ e $\forall\, a \in \Sigma_\varepsilon$

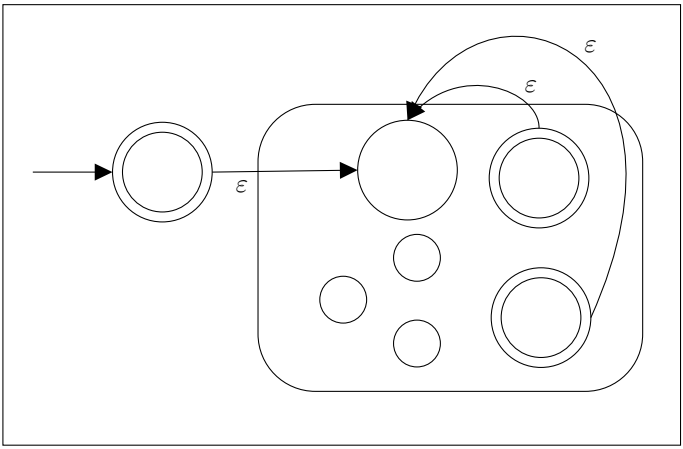
$$\delta(q,a) = \begin{cases} \delta_1(q,a) & \text{se } q \in Q_1 - F_1 \\ \delta_1(q,a) & \text{se } q \in F_1 \text{ e } a \neq \varepsilon \\ \delta_1(q,a) \cup \{q_1\} & \text{se } q \in F_1 \text{ e } a = \varepsilon \\ \{q_1\} & \text{se } q = q_0 \text{ e } a = \varepsilon \\ \emptyset & \text{se } q = q_0 \text{ e } a \neq \varepsilon \end{cases}$$

(v) $F = F_1 \cup \{q_0\}$

■

Seja A a linguagem regular reconhecida pelo autômato não determinístico N_1 da demonstração do Teorema 3.4, então a *string* $s \in A^*$ pode ser escrita como $s = x^n$ em que $x \in A$ e $n \in \mathbb{N}^0$, ou seja, N_1 aceita x. Assim, analogamente ao caso da concatenação, a "quebra" de s ocorre em algum estado aceito de N_1 na computação de s. Além disso, para algum autômato não determinístico aceitar s, deve aceitar também a *string* vazia ε, uma vez que $\varepsilon \in A^*$. Por fim, usando o esquema do diagrama de estados do autômato N_1 apresentados na Figura 21, pode-se construir o autômato não determinístico N_E do Teorema 3.4 conforme o esquema da Figura 25.

Figura 25 – Esquema do diagrama de estados do autômato N_E



3.4 EXPRESSÕES REGULARES

Definição 3.31. Seja Σ um alfabeto. Dizemos que R é uma *expressão regular sobre* Σ se R é

(i) $a \in \Sigma$;

(ii) $\varepsilon \in \Sigma^*$;

(iii) $\emptyset \subset \Sigma^*$;

(iv) $R_1 \cup R_2$ com R_1 e R_2 expressões regulares;

(v) $R_1 R_2$ com R_1 e R_2 expressões regulares;

(vi) R_1^* com R_1 expressão regular.

Denotamos por $L(R)$ a *linguagem descrita por* R. Nos itens (i) e (ii), as expressões regulares a e ε descrevem as linguagens $\{a\}$ e $\{\varepsilon\}$ (conjunto unitário da *string* vazia), respectivamente, ou seja, $L(a) = \{a\}$ e $L(\varepsilon) = \{\varepsilon\}$. No item (iii), a expressão regular $\emptyset$ descreve a linguagem vazia, ou seja, $L(\emptyset) = \emptyset$. Nos itens (iv) e (v), as expressões regulares descrevem as linguagens obtidas tomando a união e a concatenação das linguagens descritas por R_1 e R_2, respectivamente, ou seja, $L(R_1 \cup R_2) = L(R_1) \cup L(R_2)$ e $L(R_1 R_2) = L(R_1)L(R_2)$. Finalmente, no item (vi) a expressão regular R_1 descreve a linguagem obtida da operação estrela, isto é, $L(R_1^*) = L(R_1)^*$.

Grosso modo, uma expressão regular nada mais é que uma maneira sucinta para descrever linguagens. Um exemplo de expressão regular é $(0 \cup 1)0^*$. Esta expressão regular representa todas as *strings* que iniciam com 0 ou 1 seguido por uma sequência de zero ou mais 0. Ou seja, $(0 \cup 1)0^* = (\{0\} \cup \{1\})\{0\}^*$. É convencionada a ordem da aplicação das operações regulares: primeiro aplica-se a operação estrela, depois a concatenação e por fim a união, salvo quando há parenteses alterando esta ordem.

Exemplo 3.27. Seja $\Sigma = \{0, 1\}$ um alfabeto. Abaixo temos alguns exemplos de expressões regulares sobre Σ e as linguagens descritas pelas mesmas.

(i) $L(0^*10^*) = \{w \in \Sigma^*; w \text{ contém um único símbolo } 1\}$

(ii) $L(\Sigma^*1\Sigma^*) = \{w \in \Sigma^*; 1 \text{ é fator de } w\}$

(iii) $L(\Sigma^*001\Sigma^*) = \{w \in \Sigma^*; 001 \text{ é fator de } w\}$

(iv) $L(1^*(01^+)^*) =$
$\{w \in \Sigma^*;$ todo 0 em w é seguido por ao menos um $1\}$

(v) $L((\Sigma\Sigma)^*) = \{w \in \Sigma^*; |w| \equiv 0 \mod 2\}$

(vi) $L((\Sigma\Sigma\Sigma)^*) =$
$\{w \in \Sigma^*; |w| \equiv 0 \mod 3\}$

(vii) $L(01 \cup 10) = \{01, 10\}$

(viii) $L(0\Sigma^*0 \cup 1\Sigma^*1 \cup 0 \cup 1) =$
$\{w \in \Sigma^*; w$ começa e termina com o mesmo símbolo$\}$

(ix) $L((0 \cup \varepsilon)1^*) = L(01^* \cup 1^*)$

(x) $L((0 \cup \varepsilon)(1 \cup \varepsilon)) = \{\varepsilon, 0, 1, 01\}$

(xi) $L(1^*\emptyset) = \emptyset$

(xii) $L(\emptyset^*) = \{\varepsilon\}$

3.4.1 Autômato não determinístico generalizado

Notação 3.2. Denotamos por $\mathcal{R}(\Sigma)$ o conjunto de todas as expressões regulares sobre o alfabeto Σ.

Definição 3.32. Um *autômato não determinístico generalizado* é uma quíntupla $(Q, \Sigma, \delta, q_s, q_a)$ em que

(i) Q é um conjunto finito e não vazio de elementos chamados de *estados*;

(ii) Σ é um alfabeto de símbolos chamados de *entradas*;

(iii) $\delta : (Q - \{q_a\}) \times (Q - \{q_s\}) \longrightarrow \mathcal{R}(\Sigma)$ é a *função transição*;

(iv) $q_s \in Q$ é o *estado inicial*;

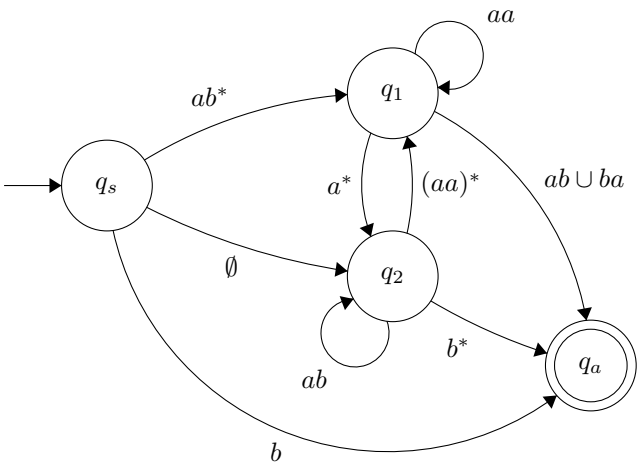
(v) $q_a \in Q$ é o *estado aceito*.

Exemplo 3.28. Seja $G_1 = (Q, \{a, b\}, \delta, q_s, q_a)$ um autômato não determinístico generalizado com $Q = \{q_s, q_1, q_2, q_a\}$ e δ dada pela Tabela 12, cujo diagrama de estados está representado na Figura 26.

Tabela 12 – Tabela de transição do autômato G_1

G_1	q_1	q_2	q_a
q_s	ab^*	$\emptyset$	b
q_1	aa	a^*	$ab \cup ba$
q_2	$(aa)^*$	ab	b^*

Figura 26 – Diagrama de estados do autômato G_1



Note que para todo $r \in Q$, $\delta(r, q_s)$ e $\delta(q_a, r)$ não estão definidos. Graficamente, o *diagrama de estados do autômato não determinístico generalizado* apresenta as seguintes características:

(i) cada nó representa um estado;

(ii) as setas do grafo são rotuladas com expressões regulares sobre o alfabeto do autômato não determinístico generalizado e representam a imagem da função transição;

(iii) o nó que representa o estado inicial (q_s) tem setas apontando para todos os outros estados, mas nenhum estado tem seta apontando para o nó do estado inicial;

(iv) o nó que representa o estado aceito (q_a) recebe setas de todos os outros estados apontado para ele, mas ele não tem seta apontando para outros estados;

(v) os nós que representam os demais estados têm uma seta para cada par, inclusive para si mesmo;

(vi) o estado inicial é o nó marcado com uma seta sem rótulo sem nó de origem apontando para ele;

(vii) o estado aceito é marcado por um circulo duplo.

Definição 3.33. Seja $G = (Q, \Sigma, \delta, q_s, q_a)$ um autômato não determinístico generalizado e $w \in \Sigma^*$. Chamamos de *computação de w em G*, ou equivalentemente dizemos que G *computa* w (ou w *é computada por* G), ou ainda dizemos que w é uma *string de entrada* de G, se w pode ser escrito como $w = w_1 w_2 \dots w_m$ em que $w_i \in \Sigma^*$ para $1 \leq i \leq m$ e existe uma sequencia de estados q_0, q_1, q_2, $\dots$, q_m, com $q_i \in Q$ para $0 \leq i \leq m$ tal que

(i) $q_0 = q_s$;

(ii) $w_i \in L(R_i)$ em que $R_i = \delta(q_{i-1}, q_i)$ para $1 \leq i \leq m$;

Se, adicionalmente, $q_m = q_a$, então dizemos que G *reconhece (ou aceita)* w.

Definição 3.34. Seja $G = (Q, \Sigma, \delta, q_s, q_a)$ um autômato não determinístico generalizado e seja A uma linguagem sobre Σ. Se G aceita todas as *strings* de A, então dizemos que G *reconhece* A.

Definição 3.35. Seja $G = (Q, \Sigma, \delta, q_s, q_a)$ um autômato não determinístico generalizado. Denotamos por $L(G)$ a linguagem sobre Σ de todas as *strings* aceitas por G. Se G não aceita *string* alguma, então $L(G) = \emptyset$. Chamamos $L(G)$ de *linguagem do autômato não determinístico generalizado* G.

A Definição 3.30 também é válida para autômatos não determinísticos generalizados, isto é, Se M e N dois autômatos (determinísticos, não determinísticos ou não determinísticos generalizados) quaisquer, então dizemos que M e N são *equivalentes* se $L(M) = L(N)$. Além disso, também podemos ter expressões regulares equivalentes a autômatos.

Definição 3.36. Sejam M um autômato (determinístico, não determinístico ou não determinístico generalizado) e R uma expressão regular quaisquer. Dizemos que M e R são *equivalentes* se $L(M) = L(R)$.

Teorema 3.5. *Para todo autômato determinístico existe um autômato não determinístico generalizado equivalente.*

Demonstração. Seja $D = (Q, \Sigma, \delta, q_0, F)$ um autômato determinístico, então devemos encontrar um autômato não determinístico generalizado $G = (Q_G, \Sigma, \delta_G, q_s, q_a)$ tal que $L(D) = L(G)$. Para tanto, podemos construir G da seguinte maneira

(i) $Q_G = Q \cup \{q_s, q_a\}$;

(ii)

$$\begin{aligned}
&\delta_G(q_s, q_a) = \emptyset \\
&\delta_G(q_s, q_0) = \varepsilon \\
&\delta_G(q_s, q_j) = \emptyset \ (\forall\, q_j \in Q - \{q_0\}) \\
&\delta_G(q_i, q_a) = \varepsilon \ (\forall\, q_i \in F) \\
&\delta_G(q_i, q_a) = \emptyset \ (\forall\, q_i \in Q - F) \\
&\delta_G(q_i, q_j) = \emptyset \ (\forall\, q_i, q_j \in Q;\ \nexists\, a \in \Sigma;\ \delta(q_i, a) = q_j) \\
&\delta_G(q_i, q_j) = \bigcup a \ (\forall\, q_i, q_j \in Q;\ \exists\, a \in \Sigma;\ \delta(q_i, a) = q_j)
\end{aligned}$$

Como toda *string* $w \in L(D)$ é aceita por D, ela pode ser escrita como $w = w_1 w_2 \dots w_k$ em que $w_i \in \Sigma$ para $1 \leq i \leq k$, existindo uma sequencia de estados r_0, r_1, r_2, …, r_k com $r_i \in Q$ para $0 \leq i \leq k$ tal que:

(i) $r_0 = q_0$

(ii) $\delta(r_i, w_{i+1}) = r_{i+1}$ para $0 \leq i \leq k-1$

(iii) $r_k \in F$

Assim, podemos escrever $w = \varepsilon w_1 w_2 \dots w_k \varepsilon$, e então existe a sequencia de estados q_s, r_0, r_1, r_2, …, r_k, q_a com $r_i \in Q$ para $0 \leq i \leq k$ tal que $w_i \in L(\delta_G(r_{i-1}, r_i))$ para $1 \leq i \leq k$ e $\varepsilon = \delta_G(q_s, r_0) = \delta_G(r_k, q_a)$. Logo G aceita w.

Caso $w \notin L(D)$, isto é, D não aceite w, não conseguimos encontrar uma sequencia de estados que atenda os critérios para aceitação de w por D. Logo também não é possível encontrar uma sequencia que satisfaça os critérios de aceitação de w por G. O que implica que, neste caso, G não aceita w.

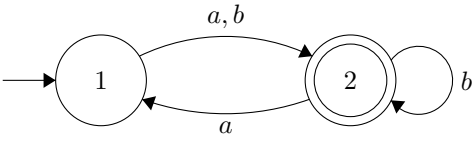
Portanto toda $w \in L(D)$ é aceita por G e toda $w \notin L(D)$ não é aceita por G logo $L(D) = L(G)$, ou seja, G é equivalente a D. ■

Exemplo 3.29. A fim de elucidar as ideias apresentadas na demonstração do Teorema 3.5, tomaremos o autômato determinístico $D_5 = (\{1, 2\}, \{a, b\}, \delta, 1, \{2\})$ com δ dada pela Tabela 13, cujo diagrama de estados é representado na Figura 27.

Tabela 13 – Tabela de transição do autômato determinístico D_5

D_5	a	b
1	2	2
2	1	2

Figura 27 – Diagrama de estados do autômato determinístico D_5

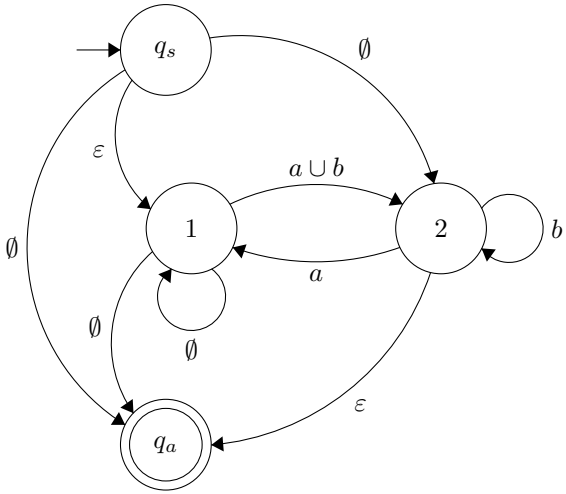


E construímos um autômato não determinístico generalizado equivalente ao autômato determinístico D_5, conforme feito na demonstração do Teorema 3.5. Tal autômato não determinístico generalizado é $G_2 = (\{q_s, 1, 2, q_a\}, \{a, b\}, \delta_G, q_s, q_a)$ com δ_G dada pela Tabela 14, cujo diagrama de estados é representado na Figura 28.

Tabela 14 – Tabela de transição do autômato não determinístico generalizado G_2

G_2	1	2	q_a
q_s	ε	$\emptyset$	$\emptyset$
1	$\emptyset$	$a \cup b$	$\emptyset$
2	a	b	ε

Figura 28 – Diagrama de estados do autômato não determinístico generalizado G_2 equivalente à D_5



3.4.2 Relação entre expressão regular e linguagem regular

A partir de agora, construiremos as ferramentas necessárias para demonstrar que uma linguagem é regular se, e somente se, existe alguma expressão regular que a descreve.

Lema 3.1. *Toda linguagem descrita por alguma expressão regular é uma linguagem regular.*

Demonstração. Seja R uma expressão regular sobre um alfabeto Σ. Sabemos que R descreve a linguagem $L(R)$. Então devemos provar que $L(R)$ é uma linguagem regular. Para tanto, basta encontrar um autômato não determinístico que reconheça $L(R)$.

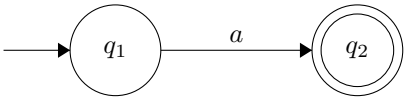
Da Definição 3.31, temos seis diferentes casos para analisarmos R e construirmos um autômato não determinístico que reconheça $L(R)$.

(i) Se $R = a \in \Sigma$, então $L(R) = \{a\}$. Logo existe o autômato não determinístico $N_3 = (\{q_1, q_2\}, \Sigma, \delta, q_1, \{q_2\})$ com

$$\delta(r, b) = \begin{cases} \{q_2\} & \text{se } r = q_1 \text{ e } b = a \\ \emptyset & \text{se } r \neq q_1 \text{ e } b \neq a \end{cases}$$

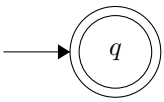
que reconhece $L(R)$, cujo diagrama de estados é representado na Figura 29.

Figura 29 – Diagrama de estados do autômato não determinístico N_3



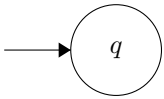
(ii) Se $R = \varepsilon \in \Sigma^*$, então $L(R) = \{\varepsilon\}$. Logo existe o autômato não determinístico $N_4 = (\{q\}, \Sigma, \delta, q, \{q\})$ com $\delta(q, b) = \emptyset$ para todo $b \in \Sigma_\varepsilon$ que reconhece $L(R)$, cujo diagrama de estados é representado na Figura 30.

Figura 30 – Diagrama de estados do autômato não determinístico N_4



(iii) Se $R = \emptyset \subset \Sigma^*$, então $L(R) = \emptyset$. Logo existe o autômato não determinístico $N_5 = (\{q\}, \Sigma, \delta, q, \emptyset)$ com $\delta(q, b) = \emptyset$ para todo $b \in \Sigma_\varepsilon$ que reconhece $L(R)$.

Figura 31 – Diagrama de estados do autômato não determinístico N_5



Os últimos três casos podem ser demonstrados indutivamente partindo dos casos anteriores. Suponha R_1 e R_2 são expressões regulares dadas conforme os casos acima. Já demonstramos daí que $L(R_1)$ e $L(R_2)$ são linguagens regulares. Daí, como $R_1 \cup R_2$ descreve $L(R_1 \cup R_2) = L(R_1) \cup L(R_2)$, temos pelo Teorema 3.2 que $R_1 \cup R_2$ descreve uma linguagem regular. Analogamente, $R_1 R_2$ e R_1^*, pelos Teoremas 3.3 e 3.4, respectivamente, descrevem linguagens regulares. ■

Exemplo 3.30. Usando diagramas de estados, o Lema 3.1 e os Teoremas 3.2, 3.3 e 3.4, construiremos um autômato não determinístico que reconhece a linguagem descrita pela expressão regular $R = (a \cup b)^* aba$ (todas as *strings* formadas pelos símbolos a e b com sufixo aba).

Figura 32 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular a

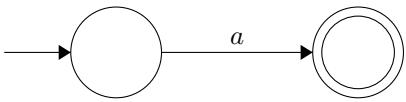


Figura 33 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular b

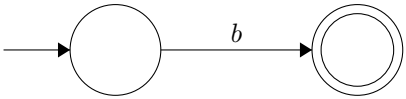


Figura 34 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular $a \cup b$

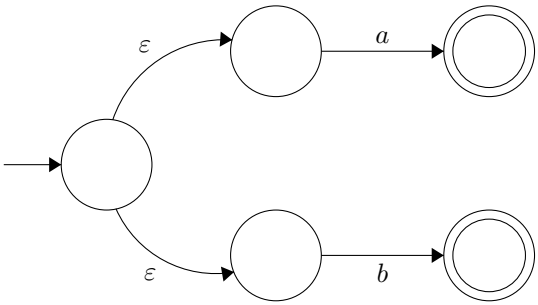


Figura 35 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular $(a \cup b)^*$

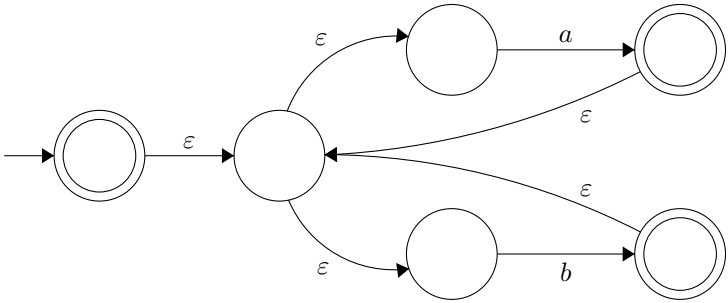


Figura 36 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular ab

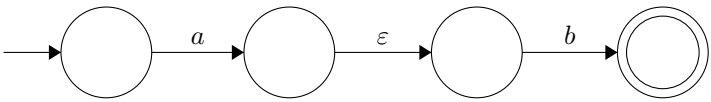


Figura 37 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular *aba*

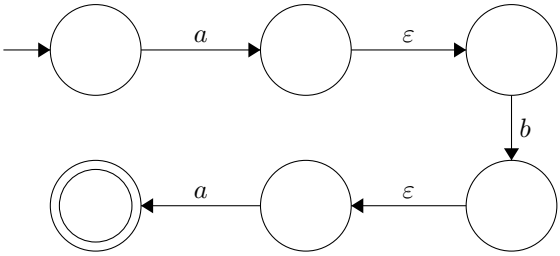
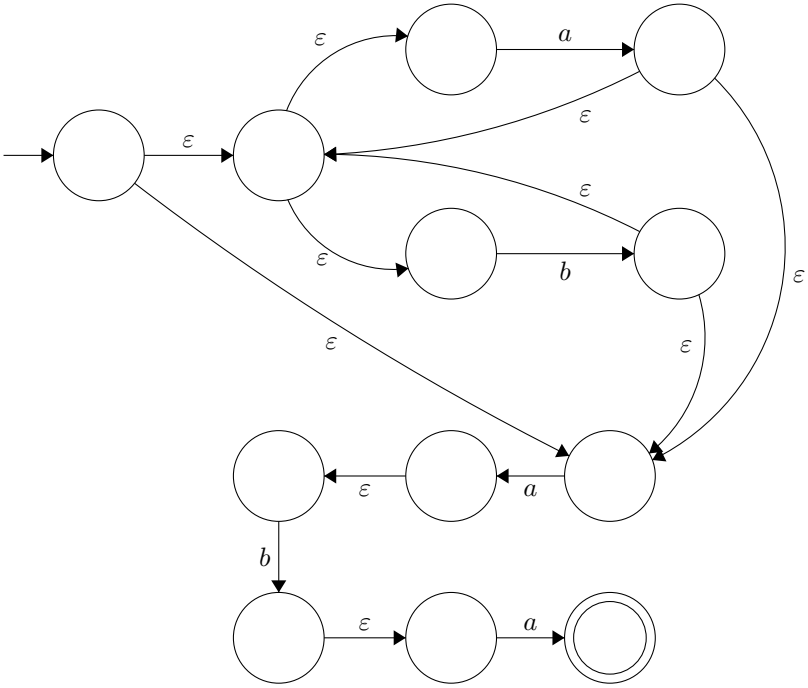


Figura 38 – Diagrama de estados do autômato não determinístico que reconhece a linguagem descrita pela expressão regular $(a \cup b)^* aba$



O Lema 3.1 nos mostra que se uma linguagem é descrita por uma expressão regular então é uma linguagem regular. Agora, construiremos algumas ferramentas para demonstrar que toda linguagem regular pode ser descrita por uma expressão regular.

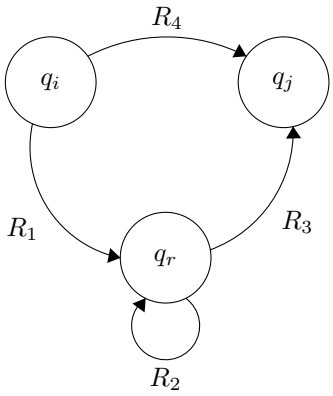
Definição 3.37. Seja $G = (Q, \Sigma, \delta, q_s, q_a)$ um autômato não determinístico generalizado com $k > 2$ estados. A *redução de* G é a função denotada por $\text{red}(G)$, que recebe como parâmetro o autômato não de-

terminístico generalizado G e retorna o autômato não determinístico generalizado G_R com $k-1$ estados.

A função red(G) funciona da seguinte maneira. Toma $q_r \in Q - \{q_s, q_a\}$ e retorna o autômato não determinístico generalizado $G_R = (Q_R, \Sigma, \delta_R, q_s, q_a)$ em que $Q_R = Q - \{q_r\}$, e para todo $q_i \in Q_R - \{q_a\}$ e todo $q_j \in Q_R - \{q_s\}$ tem-se $\delta_R(q_i, q_j) = (R_1)(R_2)^*(R_3) \cup (R_4)$ em que $R_1 = \delta(q_i, q_r)$, $R_2 = \delta(q_r, q_r)$, $R_3 = \delta(q_r, q_j)$, e $R_4 = \delta(q_i, q_j)$.

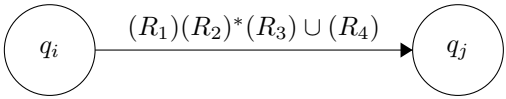
Exemplo 3.31. Suponha que tomamos $q_r, q_i, q_j \in Q$ estados particulares de um autômato não determinístico generalizado em que $q_r \in Q - \{q_s, q_a\}$, $q_i \in Q - \{q_r, q_a\}$ e $q_j \in Q - \{q_r, q_s\}$, então obtemos o diagrama de estados parcial de G conforme a Figura 39.

Figura 39 – Diagrama de estados parcial de G contendo apenas os estados q_r, q_i e q_j com $R_1 = \delta(q_i, q_r)$, $R_2 = \delta(q_r, q_r)$, $R_3 = \delta(q_r, q_j)$, e $R_4 = \delta(q_i, q_j)$



Considerando o diagrama de estados parciais da Figura 39, red(G) retorna o diagrama de estados parcial de G conforme a Figura 40.

Figura 40 – Diagrama de estados parcial de red(G)



Note que G e red(G) são equivalentes. Afinal, a expressão definida para $\delta_R(q_i, q_j)$ descreve todas as *strings* que levaria G de q_i para q_j diretamente ou via q_r.

Definição 3.38. Seja $G = (Q, \Sigma, \delta, q_s, q_a)$ um autômato não determinístico generalizado. A *conversão de G na expressão regular R* é a função denotada por convert(G), que recebe como parâmetro o autômato não determinístico generalizado G e retorna a expressão regular R. A função convert(G) é dada por

$$\text{convert}(G) = \begin{cases} \delta(q_s, q_a) & \text{se } |Q| = 2 \\ \text{convert}(\text{red}(G)) & \text{se } |Q| > 2 \end{cases}$$

Note que convert(G) é uma função recursiva. A cada passo, através da função red(G), ela reduz em um o número de estados de G até que $|Q| = 2$ retornando então a expressão regular $\delta(q_s, q_a)$

Proposição 3.1. *Todo autômato não determinístico generalizado G é equivalente a* convert(G).

Demonstração. Provaremos esta proposição por indução sobre o número de estados do autômato não determinístico generalizado $G = (Q, \Sigma, \delta, q_s, q_a)$.

Passo base: Note que a proposição vale para $|Q| = 2$. Se G tem apenas dois estados, então estes são o estado inicial e o final. Daí $\delta(q_s, q_a)$ descreve todas as *strings* aceitas por G. Logo a expressão $\delta(q_s, q_a)$ é equivalente a G.

Passo de indução: Assuma que a proposição é válida para $k-1$ estados de red(G) e usaremos esta suposição para provar que a proposição é válida para k estados de G. Primeiro mostraremos que G e red(G) reconhecem a mesma linguagem.

Suponha que G aceita uma *string* $w \in \Sigma^*$. Então, quando G computa w, existe a sequência de estados

$$q_s, q_1, q_2, q_3, \ldots, q_a$$

Se nenhum destes estados é o estado q_r removido por red(G), claramente red(G) também aceita w. A razão é que cada uma das novas expressões regulares retornadas pela função transição de red(G) contém a antiga expressão regular como parte de uma união.

Se o estado q_r removido por red(G) aparece na sequência de estados de quando G computa w acima, removemos cada estado q_r da sequência formando uma nova sequencia que faz com que w seja aceita por red(G). Os estados $q_i \in Q - \{q_r, q_a\}$ e $q_j \in Q - \{q_r, q_j\}$ tem uma nova expressão regular dada pela função transição de red(G) que descreve todas as *strings* que levaria G de q_i para q_j diretamente ou via q_r. Então, red(G) aceita w.

Por outro lado, Suponha que red(G) aceita w. Como cada par de estados q_i e q_j em red(G) descreve todas as *strings* que levam G de q_i para q_j diretamente ou via q_r, G também aceita w. Assim, G e red(G) são equivalentes.

A hipótese de indução afirma que quando a função convert(G) é executada recursivamente na entrada red(G), o resultado é uma expressão regular que é equivalente a red(G) porque red(G) tem estados $k-1$. Portanto, essa expressão regular também é equivalente a G, o que completa o passo de indução. ■

Lema 3.2. *Toda linguagem regular pode ser descrita por alguma expressão regular.*

Demonstração. Seja A uma linguagem regular, então existe o autômato determinístico D que reconhece A. Pelo Teorema 3.5, sabemos que existe algum autômato não determinístico generalizado G equivalente a D, o que implica que G reconhece A. Consequentemente A pode ser descrita pela expressão regular convert(G). ■

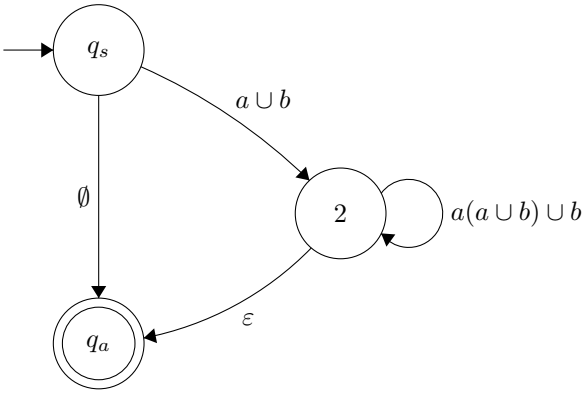
Exemplo 3.32. Tome o autômato determinístico D_5 representado na Figura 27 e seu autômato não determinístico generalizado equivalente G_2 representado na Figura 28, ilustraremos o funcionamento da função convert(G_2) obtendo a expressão regular que descreve $L(D_5)$. Ao aplicar red em G_2 eliminando o estado 1 obtemos a função transição conforme a Tabela 15 para os estados restantes.

Tabela 15 – Função transição de red(G_2) com $q_r = 1$

	2	q_a
q_s	$\varepsilon\emptyset^*(a \cup b) \cup \emptyset = a \cup b$	$\varepsilon\emptyset^*\emptyset \cup \emptyset = \emptyset$
2	$a\emptyset^*(a \cup b) \cup b = a(a \cup b) \cup b$	$a\emptyset^*\emptyset \cup \varepsilon = \varepsilon$

Como resultado obtemos o autômato não determinístico generalizado conforme o diagrama de estados da Figura 41.

Figura 41 – Diagrama de estados do autômato $G_3 = \text{red}(G_2)$

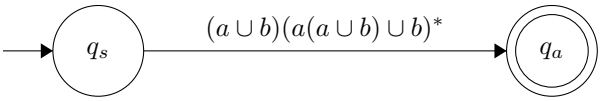


Aplicando novamente red em G_3, removendo agora o estado 2, restam apenas os estados q_s e q_a cuja função transição é dada por

$$\delta(q_s, q_a) = (a \cup b)(a(a \cup b) \cup b)^* \varepsilon \cup \emptyset = (a \cup b)(a(a \cup b) \cup b)^*;$$

Consequentemente obtemos o autômato não determinístico generalizado conforme o diagrama de estados da Figura 42.

Figura 42 – Diagrama de estados do autômato $\text{red}(G_3)$



Portanto $\text{convert}(G_2) = (a \cup b)(a(a \cup b) \cup b)^* = L(D_5)$.

Usando os Lemas 3.1 e 3.2, demonstra-se o seguinte Teorema.

Teorema 3.6. *Uma linguagem é regular se, e somente se, existe alguma alguma expressão regular que a descreve.*

Demonstração. Consequência direta dos Lemas 3.1 e 3.2. ■

4 SEMIGRUPOS E MONOIDES APLICADOS A LINGUAGENS E AUTÔMATOS

Neste último capítulo são relacionados os conteúdos dos dois capítulos anteriores. Assim atingimos o objetivo final do trabalho que é justamente relacionar a teoria de semigrupos e monoides algébrico do Capítulo 2 com os conceitos de *linguagens* e *autômatos* da teoria da computação do Capítulo 3.

Na Seção 4.1 apresentamos as linguagens Σ^+ e Σ^* sobre um alfabeto Σ, respectivamente, como o semigrupo e o monoide livre gerado por Σ. Então, munidos de ferramentas desenvolvidas no Capítulo 2, obtemos alguns resultados para caracterizar estes tipos de semigrupos. Nas Seções 4.2 e 4.3 obtemos os semigrupos relacionados com os semiautômatos e os autômatos da teoria da computação, respectivamente. Nessas Seções desenvolvemos métodos para obter o semigrupo ou monoide de um semiautômato ou autômato, bem como, a partir de um dado semigrupo ou monoide finito podemos construir um semiautômato ou autômato. Por fim, na Seção 4.4 apresentamos uma caracterização algébrica para as linguagens regulares que, como visto no Capítulo 3, são linguagens que podem ser reconhecidas por algum autômato determinístico.

4.1 SEMIGRUPOS E MONOIDES LIVRES

Seja Σ um alfabeto. Note que as linguagens Σ^+ e Σ^*, munidas da operação binária de concatenação, formam, respectivamente, um semigrupo e um monoide. De fato, a concatenação de *strings* de Σ é uma operação fechada e associativa, cuja *string* vazia ε se comporta como uma identidade para o monoide Σ^*. O alfabeto Σ é o conjunto gerador de Σ^+, isto é, $\langle\Sigma\rangle = \Sigma^+$. Caso Σ seja um alfabeto unário, então Σ^+ é um semigrupo monogênico. Se $|\Sigma| > 1$ então Σ^+ não é

comutativo.

Definição 4.1. Seja Σ um alfabeto, denominamos

(i) a linguagem Σ^+, munida da operação binária de concatenação de *semigrupo livre gerado por* Σ;

(ii) a linguagem Σ^*, munida da operação binária de concatenação de *monoide livre gerado por* Σ.

Definição 4.2. Seja Σ um alfabeto, chamamos de *inclusão padrão de* Σ *em* Σ^+, a função $\alpha : \Sigma \longrightarrow \Sigma^+$ que associa cada símbolo de Σ a *string* correspondente de comprimento 1 em Σ^+.

Definição 4.3. Seja Σ um alfabeto, chamamos de *inclusão padrão de* Σ *em* Σ^*, a função $\alpha : \Sigma_\varepsilon \longrightarrow \Sigma^*$ em que $\alpha(\varepsilon) = \varepsilon$ e associa cada símbolo de Σ a *string* correspondente de comprimento 1 em Σ^*.

Lema 4.1. *Sejam Σ um alfabeto, Σ^+ o semigrupo livre gerado por Σ, α a inclusão padrão de Σ em Σ^+, S um semigrupo qualquer e $\sigma_0 : \Sigma \longrightarrow S$ uma função qualquer. Então existe um único homomorfismo de semigrupos $\sigma : \Sigma^+ \longrightarrow S$ tal que $\sigma \circ \alpha = \sigma_0$.*

Demonstração. Sejam Σ uma alfabeto, S um semigrupo e $\sigma_0 : \Sigma \longrightarrow S$ uma função. Tome $\sigma : \Sigma^+ \longrightarrow S$ tal que para todo $u = u_1u_2 \dots u_n \in \Sigma^+$ com $u_i \in \Sigma$ $(1 \leq i \leq n,\, n \in \mathbb{N})$ tem-se

$$\sigma(u) = \sigma(u_1u_2 \dots u_n) = \sigma_0(u_1)\sigma_0(u_2) \dots \sigma_0(u_n).$$

Note que σ é um homomorfismo de semigrupos. De fato, se tomarmos $v = v_1v_2 \dots v_p$, $w = w_1w_2 \dots w_q \in \Sigma^+$ com $v_i, w_j \in \Sigma$ $(1 \leq i \leq p,$

$1 \leq j \leq q$, $p, q \in \mathbb{N}$), então

$$\begin{aligned}\sigma(vw) &= \sigma(v_1 v_2 \dots v_p w_1 w_2 \dots w_q) \\ &= \sigma_0(v_1)\sigma_0(v_2)\dots\sigma_0(v_p)\sigma_0(w_1)\sigma_0(w_2)\dots\sigma_0(w_q) \\ &= \sigma(v_1 v_2 \dots v_p)\sigma(w_1 w_2 \dots w_q) \\ &= \sigma(v)\sigma(w).\end{aligned}$$

Além disso, para todo $a \in \Sigma$ temos $\sigma \circ \alpha(a) = \sigma(\alpha(a)) = \sigma(a) = \sigma_0(a)$, isto é, $\sigma \circ \alpha = \sigma_0$. Por fim, tome $\delta : \Sigma^+ \longrightarrow S$ um homomorfismo de semigrupos tal que $\sigma_0 = \delta \circ \alpha$, logo para todo $a \in \Sigma$ temos $\delta \circ \alpha(a) = \delta(\alpha(a)) = \delta(a) = \sigma_0(a)$. Sendo δ um homomorfismo, segue que para todo $u = u_1 u_2 \dots u_n \in \Sigma^+$ com $u_i \in \Sigma$ ($1 \leq i \leq n$, $n \in \mathbb{N}$) tem-se $\delta(u) = \delta(u_1 u_2 \dots u_n) = \delta(u_1)\delta(u_2)\dots\delta(u_n) = \sigma_0(u_1)\sigma_0(u_2)\dots\sigma_0(u_n)$, consequentemente $\sigma = \delta$, ou seja, σ é única. ■

Teorema 4.1. *S é um semigrupo livre gerado por X se, e somente se, $X \subseteq S$ e todo elemento de S é unicamente representado como um produto de elementos de X.*

Demonstração. Suponha que $S = X^+$, isto é, S é um semigrupo livre gerado pelo alfabeto X. Como os símbolos de X se relacionam com as *strings* de X^+ de comprimento igual a um, segue que $X \subseteq S$. Além disso, pela Definição 3.16 cada *string* de X^+ é unicamente determinado como a concatenação dos elementos de X.

Por outro lado, suponha que todo elemento de S é unicamente representado como um produto de elementos de $X \subseteq S$. Tome X^+ o semigrupo livre gerado pelo alfabeto X, $\sigma_0 : X \longrightarrow S$ uma função dada por $\sigma_0(x) = x$ para todo $x \in X$ e α a inclusão padrão de X. Pelo Lema 4.1, existe um único homomorfismo $\sigma : X^+ \longrightarrow S$ tal que para

todo $u = u_1u_2 \dots u_n \in X^+$ com $u_i \in \Sigma$ $(1 \leq i \leq n,\ n \in \mathbb{N})$ tem-se

$$\begin{aligned}\sigma(u) &= \sigma(u_1u_2 \dots u_n) \\ &= \sigma_0(u_1)\sigma_0(u_2) \dots \sigma_0(u_n) \\ &= u_1u_2 \dots u_n.\end{aligned}$$

Como S é unicamente representado como um produto de elementos de X, então σ é bijetiva, consequentemente um isomorfismo, portanto $S \cong X^+$, logo S é um semigrupo livre gerado por X. ■

Corolário 4.1. *Se S é um semigrupo livre gerado pelo alfabeto X então $X = S - S^2$.*

Demonstração. Note que S^2 é conjunto de todas as *strings* de S cujo tamanho é maior que um. Como os símbolos de X se relacionam com as *strings* de S de comprimento igual a um, segue que $X = S - S^2$. ■

Lema 4.2. *Sejam S e T conjuntos, $f : S \longrightarrow T$ uma função e $A \subseteq S$. Então $f(S - A) = f(S) - f(A)$.*

Demonstração. Primeiramente suponha $S = A$, então $S - A = \emptyset$, logo $f(S-A) = f(\emptyset) = \emptyset = f(S)-f(S) = f(S)-f(A)$. Agora suponha $S \neq A$, então $A \subset S$ e consequentemente $S-A \neq \emptyset$. Tome, daí, $t \in f(S-A)$. Logo existe $u \in S - A$ tal que $t = f(u)$, ou seja, existe $u \in S$ e $u \notin A$ tal que $t = f(u)$. Assim $t \in f(S)$ e $t \notin f(A)$, portanto $t \in f(S) - f(A)$. Segue que $f(S - A) \subseteq f(S) - f(A)$. Analogamente, prova-se que $f(S) - f(A) \subseteq f(S - A)$. Portanto $f(S - A) = f(S) - f(A)$. ■

Lema 4.3. *Sejam S e T semigrupos e $f : S \longrightarrow T$ um homomorfismo de semigrupos, então $f(S^2) = f(S)^2$.*

Demonstração. Tome $t \in f(S^2)$, logo existe $u \in S^2$ tal que $t = f(u)$. Como $u \in S^2$, então existem $x, y \in S$ tal que $u = xy$, ou

seja, $t = f(xy)$. Como f é um homomorfismo de semigrupos, então $t = f(x)f(y) \in f(S)^2$, portanto $f(S^2) \subseteq f(S)^2$. Por outro lado, tome $t \in f(S)^2$, logo existem $t_1, t_2 \in f(S)$ tal que $t = t_1 t_2$. Como $t_1, t_2 \in f(S)$, então existem $x, y \in S$ tais que $t_1 = f(x)$ e $t_2 = f(y)$, ou seja, $t = f(x)f(y)$. Como f é um homomorfismo de semigrupos, então $t = f(xy) \in f(S^2)$, portanto $f(S)^2 \subseteq f(S^2)$. Consequentemente $f(S^2) = f(S)^2$. ■

Corolário 4.2. *Sejam S um semigrupo livre gerado pelo alfabeto X e T um semigrupo livre gerado pelo alfabeto Y. Se $\phi : S \longrightarrow T$ é um homomorfismo sobrejetivo de semigrupos, então $\phi(X) = Y$.*

Demonstração. Note que como ϕ é sobrejetivo, então $\phi(S) = T$. Pelo Corolário 4.1, $X = S - S^2$ e $Y = T - T^2$. Segue daí, pelos Lemas 4.2 e 4.3, que

$$\phi(X) = \phi(S - S^2) = \phi(S) - \phi(S^2) = \phi(S) - \phi(S)^2 = T - T^2 = Y.$$

■

Howie [5, p. 29-30] usa o resultado da equivalência do Teorema 4.2 para definir um semigrupo livre, isto é, assim como o Teorema 4.1, este fornece uma caracterização alternativa para definir semigrupo livre.

Teorema 4.2. *Sejam A um conjunto, S um semigrupo e $\mu : A \longrightarrow S$ uma função injetiva que relaciona cada elemento de A a um elemento do conjunto de geradores de S. Então S é um semigrupo livre gerado por $\mu(A)$ se, e somente se, para todo semigrupo T e para toda função $\nu : A \longrightarrow T$, existe um único homomorfismo $\phi : S \longrightarrow T$ tal que $\phi \circ \mu = \nu$.*

Demonstração. Suponha que S é um semigrupo livre gerado por $\mu(A)$. Como μ é injetiva, então admite função inversa à esquerda μ^{-1} :

$\mu(A) \longrightarrow A$, segue, daí, que $\mu \circ \mu^{-1} : \mu(A) \longrightarrow S$ é a inclusão padrão de $\mu(A)$ em S. Sejam T um semigrupo e $\nu : A \longrightarrow T$ uma função, então $\nu \circ \mu^{-1}$ é uma função de $\mu(A)$ em T. Então, pelo Lema 4.1, existe um único homomorfismo de semigrupos $\phi : S \longrightarrow T$ tal que $\phi \circ \mu \circ \mu^{-1} = \nu \circ \mu^{-1}$, ou seja, $\phi \circ \mu \circ (\mu^{-1} \circ \mu) = \nu \circ (\mu^{-1} \circ \mu)$, isto é, $\phi \circ \mu = \nu$.

Por outro lado, suponha que A é um conjunto e S é um semigrupo tal que exista uma função injetiva $\mu : A \longrightarrow S$ que relaciona cada elemento de um conjunto A a um elemento do conjunto de geradores de S, e que para todo semigrupo T e para toda função $\nu : A \longrightarrow T$, existe um único homomorfismo $\phi : S \longrightarrow T$ tal que $\phi \circ \mu = \nu$. Como T pode ser qualquer semigrupo, então suponha que T é o semigrupo livre gerado por $\mu(A)$. Note, daí, que $\mu(A)$ é tanto um subconjunto de S, quanto um subconjunto de T. Também, como ν é uma função qualquer, escolha $\nu : A \longrightarrow T$ tal que $\nu \circ \mu^{-1} : \mu(A) \longrightarrow T$ é a inclusão padrão de $\mu(A)$ em T. Além disso, note que $\mu \circ \mu^{-1} : \mu(A) \longrightarrow S$ é uma função de $\mu(A)$ em S, logo, pelo Lema 4.1, existe um único homomorfismo de semigrupos $\psi : T \longrightarrow S$ tal que $\psi \circ \nu \circ \mu^{-1} = \mu \circ \mu^{-1}$, ou seja, pela injetividade de μ segue que $\psi \circ \nu = \mu$. Assim, por um lado, substituindo $\mu = \psi \circ \nu$ em $\phi \circ \mu = \nu$ temos $\phi \circ (\psi \circ \nu) = \nu$, daí, compondo essa função a direita com μ^{-1} e reagrupando obtemos $(\phi \circ \psi) \circ (\nu \circ \mu^{-1}) = \nu \circ \mu^{-1}$. Sendo $\nu \circ \mu^{-1}$ a inclusão padrão de $\mu(A)$ em T segue que para todo $t_i \in \mu(A)$ temos

$$(\phi \circ \psi) \circ (\nu \circ \mu^{-1})(t_i) = \nu \circ \mu^{-1}(t_i)$$

$$(\phi \circ \psi)(t_i) = t_i$$

$$\phi(\psi((t_i)) = t_i.$$

Como ϕ e ψ são homomorfismos, então para todo $t = t_1 t_2 \dots t_n \in T$

com $t_i \in \mu(A)$ segue que

$$\begin{aligned}(\phi \circ \psi)(t) &= (\phi \circ \psi)(t_1 t_2 \dots t_n) \\ &= \phi(\psi(t_1 t_2 \dots t_n)) \\ &= \phi(\psi(t_1)\psi(t_2) \dots \psi(t_n)) \\ &= \phi(\psi(t_1))\phi(\psi(t_2)) \dots \phi(\psi(t_n)) \\ &= t_1 t_2 \dots t_n = t.\end{aligned}$$

Portanto, $\phi \circ \psi : T \longrightarrow T$ é a função identidade em T. De outro modo, substituindo $\nu = \phi \circ \mu$ em $\psi \circ \nu = \mu$ temos $\psi \circ (\phi \circ \mu) = \mu$, daí, compondo essa função a direita com μ^{-1} e reagrupando obtemos $(\psi \circ \phi) \circ (\mu = \circ \mu^{-1}) = \mu \circ \mu^{-1}$. Sendo $\mu \circ \mu^{-1}$ a função identidade em $\mu(A) \subseteq S$ segue que para todo $s_i \in \mu(A)$ temos

$$(\psi \circ \phi) \circ (\mu \circ \mu^{-1})(s_i) = \mu \circ \mu^{-1}(s_i)$$

$$(\psi \circ \phi)(s_i) = s_i$$

$$\psi(\phi((s_i)) = s_i.$$

Como ϕ e ψ são homomorfismos, então para todo $s = s_1 s_2 \dots s_n \in S$ com $s_i \in \mu(A)$ segue que

$$\begin{aligned}(\psi \circ \phi)(s_i) &= (\psi \circ \phi)(s_1 s_2 \dots s_n) \\ &= \psi(\phi(s_1 s_2 \dots s_n)) \\ &= \psi(\phi(s_1)\phi(s_2) \dots \phi(s_n)) \\ &= \psi(\phi(s_1))\psi(\phi(s_2)) \dots \psi(\phi(s_n)) \\ &= s_1 s_2 \dots s_n = s.\end{aligned}$$

Portanto, $\psi \circ \phi : S \longrightarrow S$ é a função identidade em S. Consequentemente, ϕ é a função inversa de ψ. Como ψ é um homomorfismo de semigrupos que admite inversa, então é um homomorfismo bijetivo de

semigrupos, ou seja, é um isomorfismo entre os semigrupos T e S, isto é, $T \cong S$. Contudo, sendo T um semigrupo livre gerado por $\mu(A)$, S também o é. ■

Corolário 4.3. *Sejam S um semigrupo, $A \subseteq S$ o conjunto de geradores de S e Σ um conjunto qualquer tal que $|\Sigma| \geq |A|$. Então existe uma congruência ρ em Σ^+ tal que $S \cong \Sigma^+/\rho$.*

Demonstração. Como $|\Sigma| \geq |A|$, existe uma função sobrejetiva $\sigma_0 : \Sigma \longrightarrow A$. Sendo $A \subseteq S$, segue que σ_0 é uma função de Σ em S. Segue do Lema 4.1 que existe um homomorfismo de semigrupos $\sigma : \Sigma^+ \longrightarrow S$ dado por $\sigma(u) = \sigma_0(u_1)\sigma_0(u_2)\ldots\sigma_0(u_n)$ para todo $u = u_1u_2\ldots u_n \in \Sigma^+$. Logo, como σ_0 é uma função sobrejetiva em A (conjunto de geradores de S), então σ também é uma função sobrejetiva. De fato, para todo $s = s_1s_2\ldots s_n \in S$ com $s_i \in A$ $(1 \leq i \leq n)$, existem $u_1, u_2, \ldots u_n \in \Sigma$ tais que $\sigma_0(u_i) = s_i$, logo existe $u = u_1u_2\ldots u_n \in \Sigma^+$ tal que $\sigma(u) = \sigma(u_1u_2\ldots u_n) = \sigma_0(u_1)\sigma_0(u_2)\ldots\sigma_0(u_n) = s_1s_2\ldots s_n = s$. Consequentemente $\operatorname{im}\sigma = S$. Portanto, pelo Teorema 2.4, temos $S = \operatorname{im}\sigma \cong \Sigma^+/\ker\sigma$. Como, pela Proposição 2.36, $\rho = \ker\sigma$ é uma congruência em Σ^+, então $S \cong \Sigma^+/\rho$. ■

Como sempre podemos encontrar um conjunto de geradores para um semigrupo S (se nenhum subconjunto próprio de S for um conjunto de geradores, então o próprio S o será), deduzimos, pelo Corolário 4.3, que todo semigrupo pode ser expresso através de um isomorfismo com o semigrupo quociente de um semigrupo livre por uma congruência. A expressão obviamente não é única, pois depende da função sobrejetiva dada por σ_0 (Howie [5, p. 30]).

Exemplo 4.1. Sejam $I = \{a, b, c\}$ um conjunto, $S = I \times I$ uma banda retangular (conforme o resultado do Item (iv) do Teorema 2.3) e

$$\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

um alfabeto. Note que

$$T = \{(a,a),(b,b),(c,c)\} \subset S$$

é o conjunto de geradores de S e que $10 = |\Sigma| > |T| = 3$. Tome a função sobrejetiva $\sigma_0 : \Sigma \longrightarrow T$ dada pela Tabela 16

Tabela 16 – Tabela da função σ_0

x	$\sigma_0(x)$
0	(a,a)
1	(b,b)
2	(c,c)
3	(a,a)
4	(b,b)
5	(c,c)
6	(a,a)
7	(b,b)
8	(c,c)
9	(a,a)

Segue do Lema 4.1 que existe um único homomorfismo de semigrupos $\sigma : \Sigma^+ \longrightarrow S$ dado por $\sigma(u) = \sigma_0(u_1)\sigma_0(u_2)\ldots\sigma_0(u_n) = \sigma_0(u_1)\sigma_0(u_n)$ para todo $u = u_1u_2\ldots u_n \in \Sigma^+$, pois como S é uma banda retangular, apenas os símbolos inicial e final da *string* u geram elementos distintos de S pelo homomorfismo σ. Note daí que $\rho = \ker\sigma = \{(u,v) \in \Sigma^+ \times \Sigma^+;\, \sigma(u) = \sigma(v)\} = \{(u,v) \in \Sigma^+ \times \Sigma^+;\, \sigma_0(u_1)\sigma_0(u_n) = \sigma_0(v_1)\sigma_0(v_m)\}$. Note que

$$\begin{aligned}\Sigma^+/\rho &= \{\rho_{00},\rho_{01},\rho_{02},\rho_{10},\rho_{11},\rho_{12},\rho_{20},\rho_{21},\rho_{22}\}\\ &\cong \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\} = S.\end{aligned}$$

Os resultados que obtemos para semigrupos livres nesta seção, podemos também obter para monoides livres. Basta adaptarmos os enunciados de maneira semelhante ao Lema 4.4 seguinte.

Lema 4.4. *Sejam Σ um alfabeto, Σ^* o monoide livre gerado por Σ, α a inclusão padrão de Σ em Σ^*, M um monoide qualquer com identidade $1 \in M$ e $\sigma_0 : \Sigma_\varepsilon \longrightarrow M$ uma função em que $\sigma_0(\varepsilon) = 1$. Então existe um único homomorfismo de monoides $\sigma : \Sigma^* \longrightarrow M$ tal que $\sigma \circ \alpha = \sigma_0$.*

Demonstração. Sejam Σ um alfabeto, M um monoide com identidade $1 \in M$ e $\sigma_0 : \Sigma_\varepsilon \longrightarrow M$ uma função em que $\sigma_0(\varepsilon) = 1$. Tome $\sigma : \Sigma^* \longrightarrow M$ tal que para todo $u = u_1u_2 \dots u_n \in \Sigma^*$ com $u_i \in \Sigma_\varepsilon$ $(1 \leq i \leq n,\, n \in \mathbb{N})$ tem-se

$$\sigma(u) = \sigma(u_1u_2 \dots u_n) = \sigma_0(u_1)\sigma_0(u_2) \dots \sigma_0(u_n).$$

Note que σ é um homomorfismo de monoides. De fato, se tomarmos $v = v_1v_2 \dots v_p$, $w = w_1w_2 \dots w_q \in \Sigma^*$ com $v_i, w_j \in \Sigma$ $(1 \leq i \leq p,$ $1 \leq j \leq q,\, p, q \in \mathbb{N})$, então

$$\begin{aligned}
\sigma(vw) &= \sigma(v_1v_2 \dots v_pw_1w_2 \dots w_q) \\
&= \sigma_0(v_1)\sigma_0(v_2) \dots \sigma_0(v_p)\sigma_0(w_1)\sigma_0(w_2) \dots \sigma_0(w_q) \\
&= \sigma(v_1v_2 \dots v_p)\sigma(w_1w_2 \dots w_q) \\
&= \sigma(v)\sigma(w).
\end{aligned}$$

Ademais, $\sigma(\varepsilon) = \sigma_0(\varepsilon) = 1$. Além disso, para todo $a \in \Sigma_\varepsilon$ temos $\sigma \circ \alpha(a) = \sigma(\alpha(a)) = \sigma(a) = \sigma_0(a)$, isto é, $\sigma \circ \alpha = \sigma_0$. Por fim, tome $\delta : \Sigma^* \longrightarrow M$ um homomorfismo de monoides tal que $\sigma_0 = \delta \circ \alpha$, logo para todo $a \in \Sigma_\varepsilon$ temos $\delta \circ \alpha(a) = \delta(\alpha(a)) = \delta(a) = \sigma_0(a)$. Sendo δ um homomorfismo, segue que para todo $u = u_1u_2 \dots u_n \in \Sigma^*$ com $u_i \in \Sigma_\varepsilon$ $(1 \leq i \leq n,\, n \in \mathbb{N})$ tem-se $\delta(u) = \delta(u_1u_2 \dots u_n) = \delta(u_1)\delta(u_2) \dots \delta(u_n) = \sigma_0(u_1)\sigma_0(u_2) \dots \sigma_0(u_n)$, consequentemente $\sigma = \delta$, ou seja, σ é única. ■

4.2 SEMIGRUPO DE SEMIAUTÔMATO

Nesta seção e nas seguintes usaremos o subconjunto do monoide de transformação completa em Q dado por $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$ para denotar a função transição de um (semi)autômato determinístico A com conjunto de estados $Q = \{q_0, q_1, \ldots, q_n\}$ e alfabeto de entrada Σ. Assim, para cada elemento $u \in \Sigma$ construímos a função $\delta_u : Q \longrightarrow Q$ dada por $\delta_u(q) = \delta(q, u)$.

Como Q é um conjunto finito, podemos fazer, para todo $u \in \Sigma$,

$$\delta_u = \begin{pmatrix} q_0 & q_1 & \cdots & q_n \\ \delta(q_0, u) & \delta(q_1, u) & \ldots & \delta(q_n, u) \end{pmatrix}.$$

Segue, daí, que dados $u, v \in \Sigma$, como δ_u e δ_v são funções em Q, denotamos a composição $\delta_u \circ \delta_v$ por

$$\delta_u\delta_v = \begin{pmatrix} q_0 & q_1 & \cdots & q_n \\ \delta(\delta(q_0, v), u) & \delta(\delta(q_1, v), u) & \ldots & \delta(\delta(q_n, v), u) \end{pmatrix}.$$

Consequentemente $\langle\delta\rangle \subseteq \mathcal{T}_Q$ será o subsemigrupo do monoide de transformação completa em Q gerado por $\delta = \{\delta_u; u \in \Sigma\}$.

Além disso, note que, para toda $x = u_1u_2 \ldots u_n \in \Sigma^+$ com $u_i \in \Sigma$ $(1 \leq i \leq n,\ n \in \mathbb{N})$, a composição $\delta_{u_n} \ldots \delta_{u_2}\delta_{u_1}$ representa a computação de x em A. Ou seja, partindo do estado $q \in Q$, $\delta_{u_n} \ldots \delta_{u_2}\delta_{u_1}(q) \in Q$ será o estado final da computação de x em A.

Definição 4.4. Seja $S = (Q, \Sigma, \delta)$ semiautômato determinístico em que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$. Chamamos $\langle\delta\rangle$ de *semigrupo do semiautômato determinístico* S.

Observação 4.1. Note que o semigrupo do semiautômato determinístico $\langle\delta\rangle$ da Definição 4.4 é um semigrupo finito com no máximo $|Q|^{|Q|}$ elementos.

Definição 4.5. Sejam S, T semigrupos. Dizemos que a função $\theta : S \longrightarrow T$ é um *anti-homomorfismo de semigrupos*, se para todo $a, b \in S$, $\theta(ab) = \theta(b)\theta(a)$

Definição 4.6. Sejam S, T monoides. Dizemos que a função $\theta : S \longrightarrow T$ é um *anti-homomorfismo de monoides*, se é um anti-homomorfismo de semigrupos e, além disso, $\theta(1_S) = 1_T$, em que $1_S, 1_T$ são as identidades de S e de T, respectivamente.

Proposição 4.1. *Seja $S = (Q, \Sigma, \delta)$ semiautômato determinístico em que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$. Então existe um anti-homomorfismo de semigrupos sobrejetivo $\phi : \Sigma^+ \longrightarrow \langle\delta\rangle$ dado por $\phi(x) = \delta_{u_n}\delta_{u_{n-1}} \ldots \delta_{u_1}$ para todo $x = u_1u_2 \ldots u_n \in \Sigma^+$ ($u_i \in \Sigma$).*

Demonstração. Note que $\langle\delta\rangle$ é um subsemigrupo do monoide de transformação completa $\mathcal{T}_Q$. Seja $\phi_0 : \Sigma \longrightarrow \langle\delta\rangle$ uma função dada por $\phi_0(u) = \delta_u$ para todo $u \in \Sigma$. Pelo Lema 4.1, existe um homomorfismo de semigrupos $\phi' : \Sigma^+ \longrightarrow \langle\delta\rangle$ dado por

$$\phi'(x) = \phi_0(u_1)\phi_0(u_2) \ldots \phi_0(u_n)$$

para todo $x = u_1u_2 \ldots u_n \in \Sigma^+$. Isto é, $\phi'(x) = \delta_{u_1}\delta_{u_2} \ldots \delta_{u_n}$ para todo $x = u_1u_2 \ldots u_n \in \Sigma^+$. Além disso, como ϕ_0 é sobrejetiva, então ϕ' também é sobrejetiva. Seja $\varphi : \Sigma^+ \longrightarrow \Sigma^+$ uma função dada por $\varphi(x) = x^t$ para todo $x \in \Sigma^+$. Portanto, existe o anti-homomorfismo de semigrupos sobrejetivo $\phi : \Sigma^+ \longrightarrow \langle\delta\rangle$ dado por $\phi(x) = \phi' \circ \varphi(x)$

para todo $x \in \Sigma^+$. De fato, para todo $x, y \in \Sigma^+$

$$\begin{aligned}
\phi(xy) &= \phi' \circ \varphi(xy) \\
&= \phi'(\varphi(xy)) \\
&= \phi'((xy)^t) \\
&= \phi'(y^t x^t) \\
&= \phi'(y^t)\phi'(x^t) \\
&= \phi'(\varphi(y))\phi'(\varphi(x)) \\
&= \phi' \circ \varphi(y)\phi' \circ \varphi(x) \\
&= \phi(y)\phi(x).
\end{aligned}$$

Além disso,

$$\phi(x) = \phi'(\varphi(x)) = \phi'(x^t) = \phi'(u_n u_{n-1} \dots u_1) = \delta_{u_n}\delta_{u_{n-1}} \dots \delta_{u_1}$$

para todo $x = u_1 u_2 \dots u_n \in \Sigma^+$. ■

Observe que na Proposição 4.1, o anti-homomorfismo ϕ descreve a mudança de estados do semiautômato S para uma determinada *string* de seu alfabeto de entrada. De fato, a computação de uma *string* em um (semi)autômato ocorre, por definição, da esquerda para a direita, e a composição dos elementos de δ ocorre da mesma forma pelo anti-homomorfismo ϕ.

Notação 4.1. Denotaremos por x^S o anti-homomorfismo ϕ da Proposição 4.1 aplicado na *string* x do alfabeto de entrada Σ do semiautômato determinístico S, isto é, $x^S = \delta_{u_n}\delta_{u_{n-1}} \dots \delta_{u_1}$ para todo $x = u_1 u_2 \dots u_n \in \Sigma^+$ $(u_i \in \Sigma)$.

Além disso, note que o *kernel* do anti-homomorfismo ϕ da Proposição 4.1 é $\ker \phi = \{(a, b) \in \Sigma^+ \times \Sigma^+; a^S = b^S\}$, isto é, $(a, b) \in \ker \phi \iff a^S = b^S$.

Teorema 4.3. *Seja $S = (Q, \Sigma, \delta)$ semiautômato determinístico em que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$. Então existe uma congruência ρ em Σ^+ tal que $\langle\delta\rangle \cong \Sigma^+/\rho$.*

Demonstração. Pela Proposição 4.1, temos que existe um anti-homomorfismo de semigrupos sobrejetivo $\phi : \Sigma^+ \longrightarrow \langle\delta\rangle$ dado por $\phi(x) = \delta_{u_n}\delta_{u_{n-1}}\dots\delta_{u_1}$ para todo $x = u_1u_2\dots u_n \in \Sigma^+$. Seja $\theta : \Sigma^+ \longrightarrow \Sigma^+$ uma função dada por $\theta(x) = x^t$ para todo $x \in \Sigma^+$. Portanto, existe o homomorfismo de semigrupos sobrejetivo $\phi' : \Sigma^+ \longrightarrow \langle\delta\rangle$ dado por $\phi'(x) = \phi\circ\theta(x)$ para todo $x \in \Sigma^+$. De fato, para todo $x, y \in \Sigma^+$

$$\begin{aligned}
\phi'(xy) &= \phi\circ\theta(xy)\\
&= \phi(\theta(xy))\\
&= \phi((xy)^t)\\
&= \phi(y^tx^t)\\
&= \phi(x^t)\phi(y^t)\\
&= \phi(\theta(x))\phi(\theta(y))\\
&= \phi\circ\theta(x)\phi\circ\theta(y)\\
&= \phi'(x)\phi'(y).
\end{aligned}$$

Seja $\rho = \ker\phi'$. Portanto, pelo Teorema 2.4, $\operatorname{im}\phi' \cong \Sigma^+/\rho$. Como ϕ' é sobrejetivo, então $\langle\delta\rangle \cong \Sigma^+/\rho$. ■

Exemplo 4.2. Para o semiautômato determinístico P do Exemplo 3.12 temos

$$\delta_0 = \begin{pmatrix} \mathrm{a} & \mathrm{f}\\ \mathrm{f} & \mathrm{f}\end{pmatrix} \qquad\qquad \delta_1 = \begin{pmatrix} \mathrm{a} & \mathrm{f}\\ \mathrm{a} & \mathrm{a}\end{pmatrix}.$$

Logo $\langle\delta\rangle = \delta = \{\delta_0, \delta_1\}$. Note que $\delta_0^2 = \delta_0$, $\delta_1^2 = \delta_1$, $\delta_0\delta_1 = \delta_0$ e $\delta_1\delta_0 = \delta_1$. Assim $x^P = \delta_{u_n}\delta_{u_{n-1}}\dots\delta_{u_1} = \delta_{u_n}$ para todo $x = u_1u_2\dots u_n \in$

Σ^+. Consequentemente $\{\delta_0, \delta_1\} = \langle\delta\rangle \cong \Sigma^+/\rho = \{\rho_0, \rho_1\}$ em que $\rho_0 = \{x \in \Sigma^+; \mathrm{Suf}(x) = \{0\}\}$ e $\rho_1 = \{x \in \Sigma^+; \mathrm{Suf}(x) = \{1\}\}$.

Por outro lado, tomando um semigrupo finito qualquer, conseguimos construir um semiautômato determinístico.

Proposição 4.2. *Seja Q um semigrupo finito, então existe um semiautômato determinístico $D = (Q, \Sigma, \delta)$.*

Demonstração. Seja Q um semigrupo finito. Tome $\Sigma \subseteq Q$ em que $\langle\Sigma\rangle = Q$. Para cada $u \in \Sigma$ definimos a função $\delta_u : Q \longrightarrow Q$ dada por $\delta_u(q) = qu$ para todo $q \in Q$. Seja, daí, $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$, então $D = (Q, \Sigma, \delta)$ é um semiautômato determinístico em que, pela Definição 4.4, $\langle\delta\rangle$ é seu semigrupo. ■

Exemplo 4.3. Considere o semigrupo monogênico

$$M(4,3) = \{a, b, c, d, e, f\}$$

gerado por a com $b = a^2$, $c = a^3$, $d = a^4$, $e = a^5$ e $f = a^6$ e portanto com a tabela de Cayley dada pela Tabela 17 seguinte.

Tabela 17 – Tabela de Cayley do semigrupo monogênico $M(4,3)$

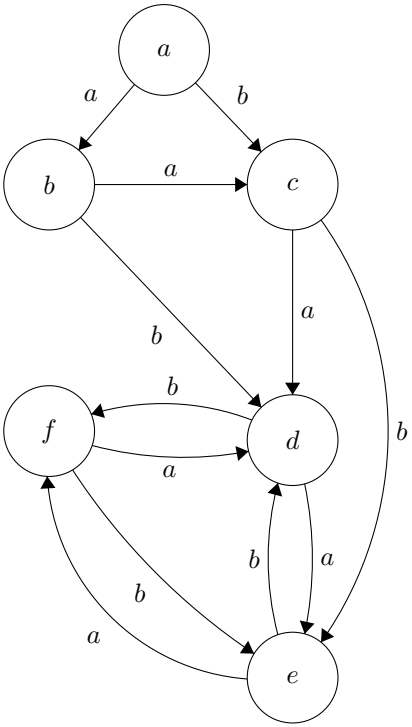
	a	b	c	d	e	f
a	b	c	d	e	f	d
b	c	d	e	f	d	e
c	d	e	f	d	e	f
d	e	f	d	e	f	d
e	f	d	e	f	d	e
f	d	e	f	d	e	f

Sejam $Q = \{a, b, c, d, e, f\}$, $\Sigma = \{a, b\}$ e $\delta = \{\delta_a, \delta_b\}$ em que

$$\delta_a = \begin{pmatrix} a & b & c & d & e & f \\ b & c & d & e & f & d \end{pmatrix}, \qquad \delta_b = \begin{pmatrix} a & b & c & d & e & f \\ c & d & e & f & d & e \end{pmatrix}.$$

Então o semiautômato determinístico $D = (Q, \Sigma, \delta)$ tem o diagrama de estados representado na Figura 43.

Figura 43 – Diagrama de estados do semiautômato D



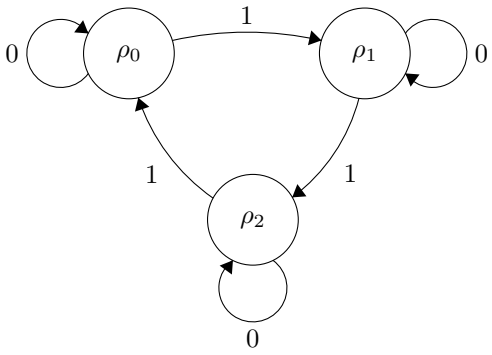
Exemplo 4.4. Seja $\Sigma = \{0, 1\}$ um alfabeto. Considere $\rho = \{(x, y) \in \Sigma^+ \times \Sigma^+; |x|_1 \equiv |y|_1 \mod 3\}$. Desse modo ρ é um relação de equivalência em Σ^+ que relaciona as *strings* de Σ^+ que possuem o mesmo resto na divisão das quantidades de ocorrências do símbolo 1 por 3, por exemplo $(0010010011, 1000) \in \rho$. Note que ρ é uma congruência em Σ^+. De fato, se $(s, t), (u, v) \in \rho$, então $|s|_1 \equiv |t|_1 \mod 3$

e $|u|_1 \equiv |v|_1 \mod 3$, logo $|s|_1 + |u|_1 \equiv |t|_1 + |v|_1 \mod 3$, o que implica em $|su|_1 \equiv |tv|_1 \mod 3$ e consequentemente $(su, tv) \in \rho$. Assim podemos construir um semiautômato $S = (Q, \Sigma, \delta)$ em que $Q = \Sigma^+/\rho = \{\rho_0, \rho_1, \rho_2\}$ com $\rho_i = \{x \in \Sigma^+; |x|_1 \equiv i \mod 3\}$ para $i \in \{0, 1, 2\}$, $\delta = \{\delta_0, \delta_1\}$ em que

$$\delta_0 = \begin{pmatrix} \rho_0 & \rho_1 & \rho_2 \\ \rho_0 & \rho_1 & \rho_2 \end{pmatrix}, \qquad \delta_1 = \begin{pmatrix} \rho_0 & \rho_1 & \rho_2 \\ \rho_1 & \rho_2 & \rho_0 \end{pmatrix}.$$

O diagrama de estados do semiautômato S é representado na Figura 44.

Figura 44 – Diagrama de estados do semiautômato S



Nesse caso, o semigrupo de S é um grupo dado por $\langle\delta\rangle = \{\delta_0, \delta_1, \delta_1^2\}$ com identidade igual a δ_0 e com $\delta_1^{-1} = \delta_1^2$.

Definição 4.7. Seja $S = (Q, \Sigma, \delta)$ semiautômato não determinístico em que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{B}_Q$. Chamamos $\langle\delta\rangle$ de *semigrupo do semiautômato não determinístico* S.

Exemplo 4.5. Para o semiautômato não determinístico N do Exemplo 3.14 temos

$$\delta_0 = \begin{pmatrix} f & t & m & w & a \\ f & f & f & f & f \end{pmatrix}, \qquad \delta_1 = \begin{pmatrix} f & f & t & m \\ t & m & t & m \end{pmatrix},$$
$$\delta_2 = \begin{pmatrix} t & m & w \\ w & m & w \end{pmatrix}, \qquad \delta_3 = \begin{pmatrix} t \\ f \end{pmatrix},$$
$$\delta_4 = \begin{pmatrix} t & m & w \\ t & w & w \end{pmatrix}, \qquad \delta_5 = \begin{pmatrix} m \\ f \end{pmatrix},$$
$$\delta_6 = \begin{pmatrix} w & a \\ a & a \end{pmatrix},$$

com $\delta = \{\delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6\}$. Logo $\langle\delta\rangle$ é o semigrupo do semiautômato não determinístico N.

Substituindo $\mathcal{T}_Q$ por $\mathcal{B}_Q$ na Proposição 4.1 e no Teorema 4.3 também provam-se os resultados para semiautômatos não determinísticos.

4.3 SEMIGRUPO DE AUTÔMATO

Dado um autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ obtemos o semiautômato determinístico $S = (Q, \Sigma, \delta)$. Em outras palavras, se tomarmos um semiautômato determinístico qualquer $S = (Q, \Sigma, \delta)$, então para cada elemento q_0 e/ou subconjunto F de Q podemos construir o autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$. Com alguns argumentos simples de contagem podemos verificar que o semiautômato determinístico S terá $|Q| \cdot 2^{|Q|-1}$ autômatos determinísticos relacionados.

De modo análogo ao que ocorre com semiautômato determinístico na Proposição 4.1, podemos encontrar um anti-homomorfismo de monoides sobrejetivo entre o conjunto das *strings* de entrada e o

semigrupo de um autômato determinístico. Note que agora falamos de anti-homomorfismo de monoides uma vez que o autômato determinístico computa elementos do monoide livre gerado por seu alfabeto de entrada.

Definição 4.8. Seja $A = (Q, \Sigma, \delta, q_0, F)$ um autômato determinístico em que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$. Chamamos $\langle \delta \cup I_Q \rangle$ de *monoide do autômato determinístico* A.

Proposição 4.3. *Seja* $A = (Q, \Sigma, \delta, q_0, F)$ *autômato determinístico em que* $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$. *Então existe um anti-homomorfismo de monoides sobrejetivo* $\phi : \Sigma^* \longrightarrow \langle \delta \rangle$ *dado por* $\phi(x) = \delta_{u_n}\delta_{u_{n-1}} \dots \delta_{u_1}$ *para todo* $x = u_1u_2 \dots u_n \in \Sigma^+$ *(*$u_i \in \Sigma$*) e* $\phi(\varepsilon) = I_Q$.

Demonstração. Considerando o semiautômato determinístico $S = (Q, \Sigma, \delta)$, pela Proposição 4.1, obtemos o anti-homomorfismo de semigrupos sobrejetivo $\phi : \Sigma^+ \longrightarrow \langle \delta \rangle$ dado por

$$\phi(x) = \delta_{u_n}\delta_{u_{n-1}} \dots \delta_{u_1}$$

para todo $x = u_1u_2 \dots u_n \in \Sigma^+$. Como $\Sigma^* = \Sigma^+ \cup \varepsilon$ e $\langle \delta \cup I_Q \rangle = \langle \delta \rangle \cup I_Q = \langle \delta \rangle^1$ podemos, partindo de ϕ, construir o anti-homomorfismo de monoides sobrejetivo $\varphi : \Sigma^* \longrightarrow \langle \delta \rangle^1$ dado por $\varphi(x) = \phi(x)$ para todo $x \in \Sigma^+$ e $\varphi(\varepsilon) = I_Q$ em que I_Q é a identidade do monoide $\langle \delta \rangle^1$ e ε é a identidade do monoide livre Σ^*. ■

Notação 4.2. Denotaremos por x^A o anti-homomorfismo φ da Proposição 4.3 aplicado na *string* x do alfabeto de entrada Σ do autômato determinístico A.

O Teorema 4.3 continua válido se substituirmos o semiautômato determinístico $S = (Q, \Sigma, \delta)$ pelo autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ e o semigrupo livre Σ^+ pelo monoide livre Σ^*, bastam algumas adaptações.

Teorema 4.4. *Seja $A = (Q, \Sigma, \delta, q_0, F)$ autômato determinístico em que $\delta = \{\delta_u; u \in \Sigma\} \subseteq \mathcal{T}_Q$. Então existe uma congruência ρ em Σ^* tal que $\langle\delta\rangle \cong \Sigma^*/\rho$.*

Demonstração. Pela Proposição 4.3, temos que existe um anti-homomorfismo de monoides sobrejetivo $\varphi : \Sigma^* \longrightarrow \langle\delta\rangle$ dado por $\varphi(x) = \delta_{u_n}\delta_{u_{n-1}}\ldots\delta_{u_1}$ para todo $x = u_1u_2\ldots u_n \in \Sigma^+$ e $\varphi(\varepsilon) = I_Q$ em que I_Q é a identidade do monoide $\langle\delta\rangle^1$ e ε é a identidade do monoide livre Σ^*. Seja $\theta : \Sigma^* \longrightarrow \Sigma^*$ uma função dada por $\theta(x) = x^t$ para todo $x \in \Sigma^+$ e $\theta(\varepsilon) = \varepsilon$. Portanto, existe o homomorfismo de monoides sobrejetivo $\varphi' : \Sigma^* \longrightarrow \langle\delta\rangle^1$ dado por $\varphi'(x) = \varphi \circ \theta(x)$ para todo $x \in \Sigma^*$. De fato, para todo $x, y \in \Sigma^*$

$$\begin{aligned}
\varphi'(xy) &= \varphi \circ \theta(xy) \\
&= \varphi(\theta(xy)) \\
&= \varphi((xy)^t) \\
&= \varphi(y^t x^t) \\
&= \varphi(x^t)\varphi(y^t) \\
&= \varphi(\theta(x))\phi(\theta(y)) \\
&= \varphi \circ \theta(x)\varphi \circ \theta(y) \\
&= \varphi'(x)\varphi'(y).
\end{aligned}$$

Seja $\rho = \ker\varphi'$. Portanto, pelo Teorema 2.4, $\operatorname{im}\varphi' \cong \Sigma^*/\rho$. Como φ' é sobrejetivo, então $\langle\delta\rangle^1 \cong \Sigma^*/\rho$. ■

Exemplo 4.6. Para o autômato determinístico M_1 do Exemplo 3.16 temos

$$\delta_0 = \begin{pmatrix} q_0 & q_1 \\ q_0 & q_1 \end{pmatrix} \qquad \delta_1 = \begin{pmatrix} q_0 & q_1 \\ q_1 & q_0 \end{pmatrix}.$$

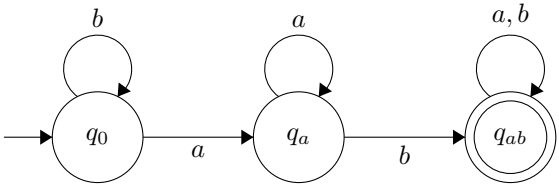
Logo $\langle\delta\rangle^1 = \delta = \{\delta_0, \delta_1\}$ uma vez que $\delta_0 = \delta_1^2 = I_Q$. Consequentemente $\{\delta_0, \delta_1\} = \langle\delta\rangle^1 \cong \Sigma^*/\rho = \{\rho_0, \rho_1\}$ em que $\rho_0 = \{x \in \Sigma^*; |x|_1 \equiv 0 \mod 2\}$ e $\rho_1 = \{x \in \Sigma^*; |x|_1 \equiv 1 \mod 2\}$.

Exemplo 4.7. Considere o autômato determinístico

$$A = (Q, \Sigma, \delta, q_0, F)$$

com $Q = \{q_0, q_a, q_{ab}\}$, $\Sigma = \{a, b\}$ e $F = \{q_{ab}\}$ cuja $L(A) = \{u \in \Sigma^*; ab \in \mathrm{Fat}(u)\}$, ou seja, A reconhece todas as *strings* de Σ^* que possuem o fator ab. O diagrama de estados de A é representado na Figura 45.

Figura 45 – Diagrama de estados do autômato A



Assim temos

$$\delta_\varepsilon = \begin{pmatrix} q_0 & q_a & q_{ab} \\ q_0 & q_a & q_{ab} \end{pmatrix},$$

$$\delta_a = \begin{pmatrix} q_0 & q_a & q_{ab} \\ q_a & q_a & q_{ab} \end{pmatrix} e$$

$$\delta_b = \begin{pmatrix} q_0 & q_a & q_{ab} \\ q_0 & q_{ab} & q_{ab} \end{pmatrix}.$$

Tomando $\rho = \{(x, y) \in \Sigma^* \times \Sigma^*; y^A = x^A\}$, segue que

$$\{\delta_\varepsilon,\ \delta_a,\ \delta_b,\ \delta_a\delta_b,\ \delta_b\delta_a\} = \langle\delta\rangle^1 \cong \Sigma^*/\rho = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4\}$$

em que ρ_i com $i \in \{0, 1, 2, 3, 4\}$ são linguagens reconhecidas por expressões regulares dadas por

$$\begin{aligned}
\rho_0 &= L(\varepsilon), \\
\rho_1 &= L(a^+), \\
\rho_2 &= L(b^+), \\
\rho_3 &= L(b^+a^+) \text{ e} \\
\rho_4 &= L(\Sigma^* ab \Sigma^*)
\end{aligned}$$

uma vez que

$$\begin{aligned}
\delta_a\delta_b &= \begin{pmatrix} q_0 & q_a & q_{ab} \\ q_a & q_{ab} & q_{ab} \end{pmatrix} e \\
\delta_b\delta_a &= \begin{pmatrix} q_0 & q_a & q_{ab} \\ q_{ab} & q_{ab} & q_{ab} \end{pmatrix}.
\end{aligned}$$

Note que, de fato, as Tabelas 18 e 19 mostram que as multiplicações entre os elementos do monoide quociente Σ^*/ρ e do monoide do autômato determinístico A, respectivamente, possuem a mesma estrutura, sendo que têm a mesma quantidade de elementos e que cada linha da primeira tabela corresponde à respectiva coluna da segunda tabela.

Tabela 18 – Tabela de Cayley do monoide quociente Σ^*/ρ

	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4
ρ_1	ρ_1	ρ_1	ρ_4	ρ_4	ρ_4
ρ_2	ρ_2	ρ_3	ρ_2	ρ_3	ρ_4
ρ_3	ρ_3	ρ_3	ρ_4	ρ_4	ρ_4
ρ_4	ρ_4	ρ_4	ρ_4	ρ_4	ρ_4

Tabela 19 – Tabela de Cayley do monoide do autômato determinístico A

	δ_ε	δ_a	δ_b	$\delta_a\delta_b$	$\delta_b\delta_a$
δ_ε	δ_ε	δ_a	δ_b	$\delta_a\delta_b$	$\delta_b\delta_a$
δ_a	δ_a	δ_a	$\delta_a\delta_b$	$\delta_a\delta_b$	$\delta_b\delta_a$
δ_b	δ_b	$\delta_b\delta_a$	δ_b	$\delta_b\delta_a$	$\delta_b\delta_a$
$\delta_a\delta_b$	$\delta_a\delta_b$	$\delta_b\delta_a$	$\delta_a\delta_b$	$\delta_b\delta_a$	$\delta_b\delta_a$
$\delta_b\delta_a$	$\delta_b\delta_a$	$\delta_b\delta_a$	$\delta_b\delta_a$	$\delta_b\delta_a$	$\delta_b\delta_a$

Analogamente ao que ocorre com os semiautômatos determinísticos, se tomarmos um monoide finito Q, conseguimos construir um autômato determinístico. No entanto, nesse caso, conseguimos garantir que o monoide do autômato determinístico construído é isomorfo ao monoide Q.

Proposição 4.4. *Seja Q um monoide finito, então existe um autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ tal que $Q \cong \langle\delta\rangle^1$.*

Demonstração. Sejam Q um monoide finito com identidade igual a 1 e $\Sigma \subseteq Q$ com $\langle\Sigma \cup \{1\}\rangle = Q$. Para cada $u \in \Sigma \cup \{1\}$ definimos a função $\delta_u : Q \longrightarrow Q$ dada por $\delta_u(q) = qu$ para todo $q \in Q$ (note que $\delta_1 = I_Q$). Seja, daí, $\delta = \{\delta_u; u \in \Sigma \cup \{1\}\} \subseteq \mathcal{T}_Q$, então $S = (Q, \Sigma, \delta)$ é um semiautômato determinístico. Assim para algum $q_0 \in Q$ e $F \subset Q$ obtemos o autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ cujo $\langle\delta\rangle^1$ é seu monoide. Note que $\langle\delta\rangle^1$ é um submonoide do monoide de transformação completa T_Q uma vez que $I_Q \in \langle\delta\rangle^1$. Vamos provar que $Q \cong \langle\delta\rangle^1$. Para tanto definimos a função $\varphi : Q \longrightarrow \langle\delta\rangle^1$ dada por $\varphi(q) = \delta_{u_1}\delta_{u_2}\ldots\delta_{u_n}$ para todo $q = u_1u_2\ldots u_n \in Q$ $(u_i \in \Sigma \cup \{1\})$. Assim para todo $q = u_1u_2\ldots u_n \in Q$ $(u_i \in \Sigma \cup \{1\})$ e para todo

$v \in \Sigma \cup \{1\}$ temos

$$\begin{aligned}\varphi(q)(v) &= \delta_{u_1}\delta_{u_2}\dots\delta_{u_n}(v)\\ &= vu_1u_2\dots u_n\\ &= vq\end{aligned}$$

Como $\Sigma \cup \{1\}$ é um conjunto gerador de Q, então todo elemento $q \in Q$ pode ser escrito como o produto de elementos de $\Sigma \cup \{1\}$. Logo, φ é sobrejetiva. Tome $q_1 = u_1u_2\dots u_n, q_2 = w_1w_2\dots w_m \in Q$ $(u_i, w_j \in \Sigma \cup \{1\})$ em que $\varphi(q_1) = \varphi(q_2)$, então para todo $v \in \Sigma \cup \{1\}$ temos $\varphi(q_1)(v) = \varphi(q_2)(v) \implies vq_1 = vq_2$. Em particular, para $v = 1$ temos que $vq_1 = vq_2 \implies 1q_1 = 1q_2 \implies q_1 = q_2$. Logo, φ é injetiva, consequentemente, bijetiva. Por fim, tome $q_1 = u_1u_2\dots u_n, q_2 = w_1w_2\dots w_m \in Q$ $(u_i, w_j \in \Sigma \cup \{1\})$, então

$$\begin{aligned}\varphi(q_1q_2) &= \delta_{u_1}\delta_{u_2}\dots\delta_{u_n}\delta_{w_1}\delta_{w_2}\dots\delta_{w_m}\\ &= (\delta_{u_1}\delta_{u_2}\dots\delta_{u_n})(\delta_{w_1}\delta_{w_2}\dots\delta_{w_m})\\ &= \varphi(q_1)\varphi(q_2).\end{aligned}$$

Logo, φ é um homomorfismo bijetivo, consequentemente, um isomorfismo. ■

Exemplo 4.8. Considere o monoide $W = \{1, e, f\}$ do Exemplo 2.9. Façamos $Q = W$ e $\Sigma = \{e, f\} \subset W$. Note que $\langle \Sigma \cup \{1\} \rangle = W = Q$. Agora, para cada $u \in \Sigma \cup \{1\}$ construímos a função $\delta_u : Q \longrightarrow Q$ dada por $\delta_u(q) = qu$, obtemos

$$\delta_1 = \begin{pmatrix} 1 & e & f \\ 1 & e & f \end{pmatrix} \qquad \delta_e = \begin{pmatrix} 1 & e & f \\ e & e & f \end{pmatrix} \qquad \delta_f = \begin{pmatrix} 1 & e & f \\ f & f & f \end{pmatrix}.$$

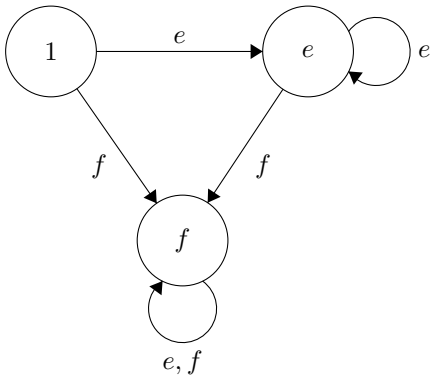
Colocando $\delta = \{\delta_1, \delta_e, \delta_f\}$ temos que $\langle \delta \rangle^1 = \delta$ com Tabela de Cayley 20.

Tabela 20 – Tabela de Cayley do monoide $\langle\delta\rangle^1$

	δ_1	δ_e	δ_f
δ_1	δ_1	δ_e	δ_f
δ_e	δ_e	δ_e	δ_f
δ_f	δ_f	δ_f	δ_f

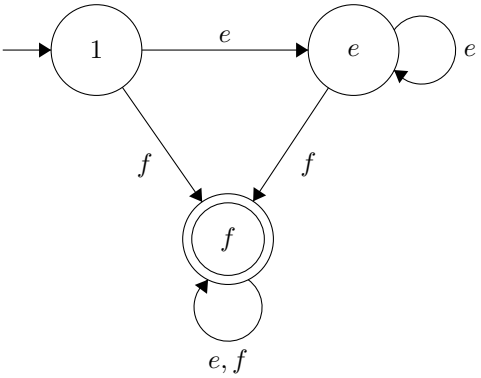
Logo $W \cong \langle\delta\rangle^1$. Assim construímos o semiautômato determinístico $S_W = (Q, \Sigma, \delta)$ cujo diagrama de estados é representado na Figura 46.

Figura 46 – Diagrama de estados do semiautômato S_W



Agora podemos selecionar quaisquer elemento e subconjunto de Q para formarmos um autômato determinístico. Por exemplo, podemos obter, a partir de S_W, o autômato determinístico $A_W = (Q, \Sigma, \delta, 1, \{f\})$ cujo diagrama de estados é representado na Figura 47 em que $L(A_W) = \{w \in \Sigma^*; |w|_f \geq 1\}$, isto é, A_W reconhece todas as *strings* do alfabeto $\Sigma = \{e, f\}$ que possuem pelo menos uma ocorrência do fator f.

Figura 47 – Diagrama de estados do autômato A_W



4.4 LINGUAGENS REGULARES

O autômato determinístico é usado para classificar (ou reconhecer) *strings* de seu alfabeto de entrada. Para essa finalidade, ele possui o estado inicial e conjunto de estados aceitos. Nesse caso as *strings* de entrada do autômato determinístico são computadas partindo do estado inicial. Se o estado final da computação de uma *string* for um estado aceito, então dizemos que a *string* é aceita ou reconhecida pelo autômato. Assim podemos dizer que uma *string* $x \in \Sigma^*$ do alfabeto de entrada do autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ é aceita (ou reconhecida) por A quando $x^A(q_0) \in F$. De fato, x^A é a notação usada para o anti-homomorfismo da Proposição 4.3, consequentemente $x^A(q_0)$ representa a computação da *string* $x \in \Sigma^*$ no autômato determinístico A partindo do estado $q_0 \in Q$. Isso prova a seguinte equivalência:

Proposição 4.5. *Sejam $A = (Q, \Sigma, \delta, q_0, F)$ um autômato determinístico e $x \in \Sigma^*$. A reconhece x se, e somente se, $x^A(q_0) \in F$.*

Segue daí que a linguagem do autômato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ pode ser escrito da seguinte maneira $L(A) = \{u \in \Sigma^*; u^A(q_0) \in F\}$. Logo "$A$ particiona Σ^* em dois subconjuntos: $L(A)$, o conjunto das *strings* reconhecidas por A, e $\Sigma^* - L(A)$, o conjunto das *strings* não reconhecidas por A" (Ginzburg [4, p. 55]).

De acordo com a Definição 3.24, o conjunto das *strings* reconhecidas por um autômato determinístico é chamada de *linguagem regular*, isto é, dizemos que uma linguagem L sobre um alfabeto Σ é regular, se, e somente se, existe um automato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ tal que para todo $x \in L$ tem-se $x^A(q_0) \in F$.

Por fim, o Teorema 4.5 caracteriza uma linguagem regular algebricamente como a união de classes de equivalência da relação de equivalência $\rho = \{(u, v) \in \Sigma^* \times \Sigma^*; u^A = v^A\}$. Note que ρ é o *kernel* do anti-homomorfismo φ da Proposição 4.3, uma vez que $\ker \varphi = \{(u, v) \in \Sigma^* \times \Sigma^*; \varphi(u) = u^A = v^A = \varphi(v)\}$, logo ρ é uma congruência em Σ^*.

Teorema 4.5. *Seja Σ um alfabeto. Segue que $L \subset \Sigma^*$ é uma linguagem regular se, e somente se, existe uma congruência ρ em Σ^* tal que*

$$\bigcup_{x \in L} \rho_x = L.$$

Demonstração. Suponha que $L \subset \Sigma^*$ é uma linguagem regular, então existe um automato determinístico $A = (Q, \Sigma, \delta, q_0, F)$ tal que para todo $x \in L$ tem-se $x^A(q_0) \in F$. Tome a congruência ρ no monoide livre Σ^* dada por

$$\rho = \{(u, v) \in \Sigma^* \times \Sigma^*; u^A = v^A\}.$$

Segue, daí, que para todo $x \in \Sigma^*$

$$\rho_x = \{y \in \Sigma^*; y^A = x^A\}.$$

Como ρ é uma relação de equivalência, temos que para todo $x \in L$, $x \in \rho_x$, logo

$$L \subseteq \bigcup_{x \in L} \rho_x.$$

Agora provaremos que $\bigcup_{x \in L} \rho_x \subseteq L$. De fato, tome $u \in \bigcup_{x \in L} \rho_x$, então existe $x \in L$ tal que $u \in \rho_x$, logo $u^A = x^A$, consequentemente $u^A(q_0) = x^A(q_0) \in F$, portanto $u \in L$. Assim

$$\bigcup_{x \in L} \rho_x = L.$$

Por outro lado, suponha que existe uma congruência ρ em Σ^* tal que

$$\bigcup_{x \in L} \rho_x = L.$$

Para cada $u \in \Sigma_\varepsilon$ definimos a função $\delta_u : \Sigma^*/\rho \longrightarrow \Sigma^*/\rho$ dada por $\delta_u(\rho_q) = \rho_{uq}$ para todo $q \in \Sigma^*/\rho$ (note que $\delta_\varepsilon = I_{\Sigma^*/\rho}$). Seja, daí, $\delta = \{\delta_u; u \in \Sigma_\varepsilon\} \subseteq \mathcal{T}_{\Sigma^*/\rho}$. Seja $F = \{\rho_x; x \in L\}$. Tome, daí, o autômato determinístico $A = (\Sigma^*/\rho, \Sigma, \delta, \rho_\varepsilon, F)$, assim para todo $x \in \Sigma^*$, $x^A = \rho_x$. Logo, para todo $x \in L$, $x^A(\rho_\varepsilon) = \rho_x\rho_\varepsilon = \rho_{x\varepsilon} = \rho_x \in F$. Portanto $L(A) = L$, consequentemente L é uma linguagem regular. ■

Exemplo 4.9. Na demonstração da recíproca do Teorema 4.5 construímos um autômato determinístico a partir de uma congruência ρ em Σ^*. Por exemplo, considere a congruência ρ do Exemplo 4.7, daí construímos o autômato determinístico

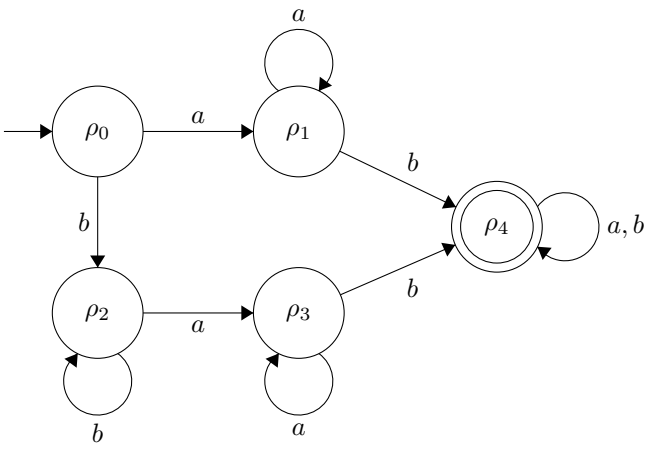
$$B = (\Sigma^*/\rho, \Sigma, \{\delta_u; u \in \Sigma_\varepsilon\}, \rho_\varepsilon, \{\rho_4\})$$

em que

$$\delta_\varepsilon = \begin{pmatrix} \rho_0 & \rho_1 & \rho_2 & \rho_3 & \rho_4 \\ \rho_0 & \rho_1 & \rho_2 & \rho_3 & \rho_4 \end{pmatrix},$$
$$\delta_a = \begin{pmatrix} \rho_0 & \rho_1 & \rho_2 & \rho_3 & \rho_4 \\ \rho_1 & \rho_1 & \rho_3 & \rho_3 & \rho_4 \end{pmatrix} e$$
$$\delta_b = \begin{pmatrix} \rho_0 & \rho_1 & \rho_2 & \rho_3 & \rho_4 \\ \rho_2 & \rho_4 & \rho_2 & \rho_4 & \rho_4 \end{pmatrix}.$$

O diagrama de estados de B é representado na Figura 48.

Figura 48 – Diagrama de estados do autômato B



Note que $L(B) = \rho_4 = L(\Sigma^* ab \Sigma^*)$ é igual a linguagem reconhecida pelo autômato determinístico A do Exemplo 4.7, ou seja, ainda que não tenham a mesma representação no diagrama de estados, os autômatos A e B reconhecem a mesma linguagem.

5 CONCLUSÃO

O desenvolvimento deste trabalho possibilitou o contato com os conteúdos de semigrupos e monoides algébricos e de linguagens e autômatos da teoria da computação que não fazem parte do currículo do curso de Licenciatura em Matemática da UFSC - Blumenau.

Para o desenvolvimento deste trabalho de conclusão de curso, foram necessários conhecimentos adquiridos durante toda a graduação, desde estratégias para demonstração de proposições e teoremas, habilidades de escrita de textos e principalmente os conteúdos das disciplinas de Álgebra, onde vimos algumas estruturas algébricas: anéis, corpos e grupos. Outro fator indispensável para elaboração deste trabalho foram as iniciações científicas. Afinal, foi ao longo das pesquisas da iniciação científica que surgiram as primeiras ideias relacionadas a este assunto.

Os objetivos pretendidos pelo trabalho foram atingidos uma vez que aplicamos a teoria de semigrupos e monoides algébricos a linguagens e autômatos da teoria da computação. Para tanto, usamos as ideias de monoide de transformação completa e o teorema fundamental do homomorfismo para semigrupos e monoides para caracterizar os semigrupos e monoides livres, bem como os semiautômatos e autômatos da teoria da computação, uma vez que a função transição que caracteriza estes objetos, pode ser descrita por meio de funções em seu respectivo conjunto de estados. Além disso, mostramos que todo semiautômato e autômato tem um semigrupo ou monoide associado, bem como, dado um semigrupo ou monoide finito qualquer podemos construir um semiautômato ou autômato. Finalizamos o trabalho, demonstrando um teorema que caracteriza linguagem regular partindo da ideia congruência e classes de equivalência. O uso de tais estruturas algébricas para descrever linguagens e autômatos possibilita que

estudemos estes mesmos objetos sob outro ponto de vista, podendo até mesmo obter novos resultados, tanto na teoria algébrica quanto na teoria da computação.

Por meio das pesquisas realizadas para o desenvolvimento deste texto, observamos que tanto a teoria de semigrupos e monoides algébricos quanto a teoria da computação são extensas. Abrem-se portanto oportunidades de novas pesquisas em ambas as áreas. Por exemplo, investigar se as máquinas de *Turing* podem ser descritas por alguma estrutura algébrica, ou ainda pode-se estudar as linguagens regulares por meio de expressões regulares com operações algébricas, ou ainda é possível aplicar a teoria de semigrupos à álgebra linear, uma vez que as matrizes quadradas sobre o corpo dos números reais com a operação binária de multiplicação matricial formam um semigrupo regular. Enfim, várias possibilidades de novas pesquisas podem surgir a partir das ideias apresentadas neste trabalho.

REFERÊNCIAS

[1] A. H. Clifford e G. B. Preston. *The Algebraic Theory of Semigroups*. 2ª ed. Vol. 1. American Mathematical Society, 1964. ISBN: 0-8218-0271-2.

[2] Hygino H. Domingues e Gelson Iezzi. *Álgebra Moderna*. 4ª ed. Av. Marquês de São Vicente, 1697, Barra Funda, São Paulo, SP 01139-904, BRA: Saraiva, 2003. ISBN: 85-357-0401-9.

[3] Vicky G. *Semigroup Theory*. 2019. Disp. em: `https://www.math.arizona.edu/~jaytaylor/files/york/SemigroupTheory.pdf` (acesso em 10/05/2019).

[4] Abraham Ginzburg. *Algebraic Theory of Automata*. 111 Fifth Avenue, New York, New York 10003: Academic Press, 1968.

[5] John M. Howie. *Fundamentals of Semigroup Theory*. Oxford University Press, 1995. ISBN: 0-19-851194-9.

[6] Rudolf Lidl e Günter Pilz. "Applied Abstract Algebra". Em: 2ª ed. 175 Fifth Avenue, New York, NY 10010, USA: Springer, 1998. Cap. 7. ISBN: 0-387-98290-6.

[7] Mathcha.io. *Mathcha - Online Math Editor*. 2019. Disp. em: `https://www.mathcha.io/` (acesso em 07/12/2019).

[8] Jacques Sakarovitch. *Elements of automata theory*. Cambridge University Press, 2009. ISBN: 978-0-521-84425-3.

[9] Michael Sipser. *Introduction to the Theory of Computation*. 3ª ed. 20 Channel Center Street, Boston, MA 02210, USA: Cengage Learning, 2013. ISBN: 978-1-133-18779-0.

[10] Evan Wallace. *Finite State Machine Designer*. 2010. Disp. em: `http://madebyevan.com/fsm/` (acesso em 07/02/2021).