Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática
Programa de Mestrado Profissional
em Matemática em Rede Nacional

Classificação dos grupos gerados por autômatos de dois estados

Hiago Gomes Pereira

Brasília

2023

Hiago Gomes Pereira

Classificação dos grupos gerados por autômatos de dois estados

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos do "Programa" de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, para obtenção do grau de Mestre.

Universidade de Brasília - UnB

Departamento de Matemática - MAT

PROFMAT - SBM

Orientador: Prof. Dra. Flávia Ferreira Ramos Zapata

Brasília

2023

Posição vertical

Hiago Gomes Pereira
Classificação dos grupos gerados por autômatos de dois estados/ Hiago Gomes Pereira. – Brasília, 2023-
90 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dra. Flávia Ferreira Ramos Zapata

Dissertação de Mestrado – Universidade de Brasília - UnB
Departamento de Matemática - MAT
PROFMAT - SBM, 2023.

1. Grupos. 2. Autômatos. 3. Classificação. 4. *Lamplighter* 5. Sistemas Dinâmicos I. Prof. Dra. Flávia Ferreira Ramos Zapata. II. Universidade de Brasília. III. PROFMAT - SBM. IV. Classificação dos grupos gerados por autômatos de dois estados

CDU XYZ 02:141:005.7

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Classificação dos grupos gerados por autômatos de dois estados

por

Hiago Gomes Pereira

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 15 de fevereiro de 2023

Comissão Examinadora:

Prof. Dra. Flávia Ferreira Ramos Zapata- MAT/UnB (Orientador)

Prof. Dr. Rui Seimetz - MAT/UnB

Prof. Dr. Alex Carrazedo Dantas - MAT/UnB

Prof. Dr. Ricardo Nunes de Oliveira - IME/UFG

Dedico este trabalho a minha família e amigos que em tudo me ajudaram nesta jornada.

Agradecimentos

Agradeço primeiramente a Deus, pelo dom da vida e que em todas as dificuldades me fortaleceu.

Agradeço aos meus pais Aldemir e Fátima, que em tudo sempre se esforçaram para que tivesse acesso a uma boa educação. Também agradeço ao meu irmão Heitor, por todo suporte e compreensão.

A professora Flávia Zapata, por toda paciência e dedicação. Sou grato por todo o aprendizado e por toda sua disponibilidade, apesar da situação adversa de pandemia. Fico feliz por ter sido um de seus alunos.

Agradeço a minha família e aos meus amigos, por estarem sempre dispostos a ajudar no que fosse necessário. Ao Bruno, a Júlia.

Por fim, agradeço a toda equipe da UNB e do PROFMAT, corpo administrativo e docente que sempre foi disposto a fazer o melhor por seus alunos. Aos professores Vinícius Rispoli, Edson Júnior e Matheus Bernardini.

"Quem observa o vento nunca semeará, e o que olha para as nuvens nunca segará "

Eclesiastes, 11.4

Resumo

O teorema principal do presente trabalho classifica os grupos gerados por autômatos de dois estados sobre o alfabeto de duas letras. Existem 64 autômatos invertíveis agindo sobre um alfabeto de duas letras, mas apenas seis grupos de autômatos: o grupo trivial, o grupo de ordem 2, o grupo não cíclico de ordem 4, o grupo cíclico-infinito, o grupo diedral-infinito e, por fim, o grupo *Lamplighter*. A exposição baseia-se numa palestra de A. Zuk (Astérisque, 2008, n. 317).

Para além dessa classificação, foi proposta uma aplicação para o ensino de parte dos conceitos abordados. Optou-se pelo ensino de autômatos e máquinas de leitura para crianças cursando o Ensino Fundamental. O objetivo é fornecer a esses alunos um primeiro contato com a linguagem de máquina, uma linguagem essencial à computação moderna.

Palavras-chaves: Grupos. Autômatos. Classificação. *Lamplighter*. Sistemas Dinâmicos.

Abstract

The main theorem of the present work classifies the groups generated by two-state automata in the two-letter alphabet. There are 64 invertible automata acting on a two-letter alphabet, but only six automata groups: the trivial group, the order two group, the non-cyclic group of order 4, the infinite-cyclic group, the infinite-dihedral group and finally the *Lamplighter* group. The exposition is based on a lecture by A. Zuk (Astérisque, 2008, n. 317).

In addition to this classification, a pedagogical application for teaching part of the presented concepts is developed. Teaching automata and reading machines for children attending elementary school was chosen. The objective is to provide to these students a first contact with machine language, an essential language for modern computing.

Key-words: Groups. Automata. Classification. *Lamplighter*. Dynamical Systems.

Lista de ilustrações

Sumário

Introdução

Grupos gerados por autômatos foram formalmente introduzidos no início dos anos de 1960. Porém, levou certo tempo para que percebessem a sua importância, utilidade e complexidade. Entre 1970 e 1980 foi constatado que esses grupos fornecem exemplos de grupos de torção finitamente gerados infinitos. Desse modo, fazem uma contribuição para um dos problemas mais famosos em álgebra: o problema de Burnside [9].

Um grupo G é um conjunto não vazio com uma operação binária com as seguintes propriedades: associatividade, existência de um elemento neutro, e existência de um elemento inverso para todo elemento de G. Esse conceito foi nomeado em 1830 por E. Galois que possuía na época apenas 19 anos de idade. Galois fundou a Teoria dos Grupos com o objetivo de resolver um dos problemas mais famosos de seu tempo: a existência ou não de fórmulas para encontrar as raízes de equações polinomiais de grau superior a três. Os grupos solúveis surgiram da prova de Galois de que não existe solução geral para as equações de quinto grau [13], desde então, a Teoria dos Grupos vem evoluindo e encontrando aplicações em diversos campos do conhecimento, como o estudo de átomos por meio de grupos de simetria [15], ou por exemplo, em conexões com a Teoria de Probabilidades [16]. Diversos matemáticos se dedicaram ao estudo dessa parte da álgebra, dentre os pioneiros cita-se: Cauchy, Galois, Jordan, Frobenius, Sylow, Burnside e Lie.

Um autômato, por sua vez, em termos gerais, é uma estrutura que pode ser definida por meio de uma sêxtupla: conjunto de estados, aplicação parcial de transição de estados, aplicação parcial de saída, estado inicial, alfabeto de entrada e saída. É uma máquina capaz de ler uma palavra, quando contida no alfabeto de entrada, e gerar uma saída, contida no alfabeto de saída. Esse conceito é essencial à computação moderna, sendo parte da discussão principal deste trabalho.

Grupos gerados por autômatos podem ser interpretados como grupos de automorfismos de uma árvore regular uni-raiz $\mathcal{T}_2$. Formalmente, a conexão entre os grupos de automorfismos e autômatos ocorre através de uma correspondência natural entre os autômatos inversíveis de entrada e saída sobre o alfabeto $Y = \{0, 1\}$ e automorfismos da árvore binária $\mathcal{T}_2$, [9] [16]. Há interesse de matemáticos e cientistas da computação nesses grupos gerados por autômatos, já que esses oferecem respostas para problemas complexos. *"Grupos autossimilares"* de crescimento intermediário, são mencionados por Wolfram em [18], como exemplos de sistemas multivariados com comportamento complexo.

Dentre os principais problemas em várias áreas da matemática, estão os problemas de classificação. Esses visam classificar objetos matemáticos por sua complexidade em diferentes classes. Neste trabalho, classificou-se os grupos gerados por autômatos de dois

estados no alfabeto de duas letras, conforme o trabalho feito por Zuk [2]. De modo geral, utiliza-se o par (m, n) como parâmetro natural para a classificação, ondem m representa o número de estados e n a cardinalidade do alfabeto. No nosso caso, vamos nos restringir aos pares $(1, 2)$ e $(2, 2)$. Existem 64 autômatos invertíveis agindo sobre um alfabeto de duas letras, mas apenas seis grupos de autômatos: o grupo trivial, o grupo de ordem 2, o grupo não cíclico de ordem 4, o grupo cíclico-infinito, o grupo diedral-infinito e, por fim, o grupo *Lamplighter* [11].

No Capítulo 1 são introduzidos os conceitos básicos de Teoria dos Grupos, e são apresentados definições e conceitos introdutórios tais como: subgrupos, grupos cíclicos, classes laterais, produto direto, operadores e relações. No Capítulo 2, iniciamos o estudo da teoria básica de autômatos, explorando a construção da árvore binária para o alfabeto de duas letras. No Capítulo 3, são exploradas ideias de sistemas dinâmicos e apresentado o grupo *Lamplighter*, um dos seis grupos de autômatos citados anteriormente. Tal grupo pode ser interpretado como uma rua bi-infinita, ou seja, uma rua infinita em ambos os sentidos, com postes de lâmpadas que podem estar acesas ou apagadas.

No Capítulo 4, são demonstradas as relações entre grupos e autômatos. Classificou-se os grupos gerados por autômatos de dois estados. Sendo assim, cada um dos 64 autômatos invertíveis de dois estados foi associado ao respectivo grupo gerado. Diferentes abordagens foram utilizadas com a finalidade da facilitar a compreensão do leitor. Finalmente, no Capítulo 5, é proposta uma alternativa para o ensino de conceitos como autômatos e máquinas de leitura para crianças cursando o Ensino Fundamental. O objetivo é fornecer a esses alunos um primeiro contato com a linguagem de máquinas, linguagem essencial a computação moderna.

1 Preliminares

1.1 Grupos

Neste capítulo serão apresentados conceitos básicos relativos à Teoria dos Grupos. Os conceitos foram retirados dos livros, artigos e notas especificados na bibliografia em: [1] [2] [3] [7] [8] [13] [17] [18].

Definição 1.1.1 (Grupos)**.** *Seja G um conjunto não vazio, com uma operação binária*

$$\cdot : G\times G \longrightarrow G,$$

$$(a,b) \mapsto a\cdot b$$

onde e as seguintes condições são satisfeitas:

i. A operação é associativa:

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c;\ \forall a,b,c \in G$$

ii. Existe um elemento neutro:

$$\exists\ e \in G,\ tal\ que\ a = e\cdot a = a\cdot e,\ \forall a \in G$$

iii. Todo elemento de G possui um inverso:

$$\forall a \in G,\ \exists\ b \in G\ tal\ que,\ a\cdot b = b\cdot a = e.$$

Munido desta operação, o conjunto G é chamado de grupo e também pode ser representado pelo par $(G, \cdot)$. Além disso, caso $a\cdot b = b\cdot a$, $\forall a,b \in G$, a operação $\cdot$ é comutativa, e G é chamado de grupo abeliano (ou comutativo).

O item *ii.* garante a existência de um elemento especial no grupo: o elemento neutro. Este elemento é capaz de comutar com todos os outros elementos do grupo e sempre que operado com um elemento qualquer resulta nesse elemento qualquer. Dada essas propriedades singulares, podemos nos perguntar quantos elementos neutros existem em um grupo. Essa resposta é obtida a partir de sua própria definição. Se G é um grupo, existe um único elemento e com $e \cdot a = a = a \cdot e$ para todo $a \in G$.

Demonstração. Suponha que $e' \cdot a = a = a \cdot e'$ para todo $a \in G$. Em particular, se $a = e$, então $e' \cdot e = e$. Por outro lado, a propriedade de definição de e nos leva a $e' \cdot e = e'$ e então $e' = e$. □

Além disso, para cada $a \in G$, existe um único elemento $b \in G$ com $a \cdot b = e = b \cdot a$, ou seja para cada elemento a existe apenas um inverso.

Demonstração. Suponha que $a \cdot b = b \cdot a = e$ e $a \cdot b' = b \cdot a' = e$ para todo $a \in G$. Se multiplicarmos ambos os lados da equação $a \cdot b = a \cdot b'$, por b, obteremos que $b \cdot (a \cdot b) = b \cdot (a \cdot b')$ e $b = b'$, $\forall a \in G$. Logo o inverso de a é único. □

Exemplo 1.1.1. Considere $\mathbb{Z}$ o conjunto dos números inteiros. Este conjunto $\mathbb{Z}$ com a operação de adição usual é um grupo abeliano.

Exemplo 1.1.2. Seja S um conjunto não vazio com 3 elementos e seja $G = \{f : S \to S;$ f é função bijetiva$\}$, se $\circ$ é a operação de composição de funções, isto é:

$$\circ\colon G \times G \longrightarrow G, (g, f) \to g \circ f$$

Então G é claramente um grupo tendo a função identidade de S, $S \to S$, como elemento neutro. Esse grupo é chamado de grupo das permutações do conjunto S. Se $S = \{1, 2, ..., n\}$ denotaremos esse grupo por S_n, com $n!$ elementos. Para $S = \{1, 2, 3\}$, representaremos esse grupo por S_3, grupo com 3!, seis, elementos.

Agora vamos mostrar que o grupo S_3, é um exemplo de grupo não abeliano.

Demonstração. De fato, sejam $f, g \in S_3$ definidas como seguem:

$$f : \{1, 2, 3\} \to \{1, 2, 3\}$$
$$f(1) = 2, f(2) = 1, f(3) = 3$$
$$g : \{1, 2, 3\} \to \{1, 2, 3\}$$
$$g(1) = 2, g(2) = 3, g(3) = 1$$

Ora, como: $(g \circ f)(1) = g(f(1)) = g(2) = 3$, e $(f \circ g)(1) = f(g(1)) = f(2) = 1$, teremos que $g \circ f \neq f \circ g$. Logo S_3 não é abeliano.

□

Gauss em trabalho publicado em 1801 (*Disquisitiones Arithmeticae*), quando tinha apenas 24 anos de idade, desenvolveu a ideia de congruência. A congruência é uma relação de equivalência, ou seja, relação que apresenta transitividade, reflexividade e simetria. Se

x, y e m são inteiros ($m > 0$), dizemos que y é congruente a x módulo m se m é um divisor de $(y-x)$. Essa situação é usualmente denotada por $y \equiv x \ (mod\ m)$. As classes de congruência com a operação de adição modular podem ser analisadas sobre a perspectiva de grupos.

Exemplo 1.1.3. Denote a classe de congruência módulo m de um inteiro x por $\overline{x}$; ou seja:

$$\overline{x} = \{y \in \mathbb{Z}\colon y \equiv x \ (mod\ m)\} = \{x + km : k \in \mathbb{Z}\}.$$

O conjunto $\mathbb{Z}_m$ de todas as classes de congruência módulo m, com $m > 1$, é chamada de inteiros módulo m. A adição módulo m, definida por $\overline{x} + \overline{y} = \overline{x+y}$, é uma operação sobre $\mathbb{Z}_m$ para qual vale a associatividade e a comutatividade. Além disso, temos:

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{x}$$

e portanto, $\overline{0}$ é o elemento neutro desta operação. Mais do que isso, a classe $\overline{-x}$ é o oposto de $\overline{x} \in \mathbb{Z}_m$ na adição módulo m, pois:

$$\overline{x} + \overline{-x} = \overline{x + (-x)} = \overline{0}$$

Desse modo, ($\mathbb{Z}_m$,+) é um grupo comutativo, para todo inteiro $m > 1$, chamado grupo aditivo das classes de resto módulo m. Vale notar que a ordem (quantidade de elementos) desse grupo é m.

Caso m seja igual a dois, temos duas classes de equivalência. Pois, qualquer número divido por 2 deixa os restos 0 ou 1. Observe:

$$\overline{0} = \{y \in \mathbb{Z} : y \equiv 0 \ (mod\ 2)\} = \{0 + 2k : k \in \mathbb{Z}\}$$

$$\overline{1} = \{y \in \mathbb{Z} : y \equiv 1 \ (mod\ 2)\} = \{1 + 2k : k \in \mathbb{Z}\}.$$

$$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$$

No grupo ($\mathbb{Z}_2$,+) o elemento $\overline{1}$ é seu próprio oposto, dado que $\overline{1} + \overline{2-1} = \overline{1 + (2-1)} = \overline{2} = \overline{0}$. Repare que $\overline{0}$ é o elemento neutro deste grupo.

Caso m seja igual a três, temos três classes de equivalência. Já que os restos possíveis da divisão por 3 são $0, 1$ e 2.

$$\overline{0} = \{y \in \mathbb{Z}\colon y \equiv 0 \ (mod\ 3)\} = \{0 + 3k : k \in \mathbb{Z}\}$$

$$\overline{1} = \{y \in \mathbb{Z} : y \equiv 1 \ (mod\ 3)\} = \{1 + 3k : k \in \mathbb{Z}\}.$$

$$\overline{2} = \{y \in \mathbb{Z} \text{: } y \equiv 2 \ (mod\ 3)\} = \{2 + 3k : k \in \mathbb{Z}\}.$$

$$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$$

No grupo ($\mathbb{Z}_3$,+), o elemento $\overline{1}$ tem como oposto $\overline{2}$, já que $\overline{1} + \overline{3-1} = \overline{1+(3-1)} = \overline{3}$ $= \overline{0}$. Assim como o caso anterior, $\overline{0}$ é o elemento neutro deste grupo.

Exemplo 1.1.4. O conjunto de simetrias de um polígono regular de n lados possui $2n$ elementos, o dobro do número de lados no caso geral. Para descrevermos essas simetrias, denotemos o número de vértices do polígono por $1, 2, ..., n$ e o conjunto de simetrias por D_{2n}.

Duas simetrias bastam para gerar D_{2n}: a rotação s de $2\pi/n$ radianos em torno do centro O do polígono, sentido anti-horário, e a reflexão t de π radianos em torno da reta x, esta passa pelo vértice P e pelo centro do polígono. A Figura 1 mostra o conjunto de simetrias em um polígono regular (quadrado PQRS).

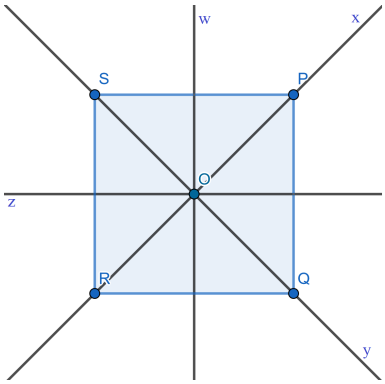

Figura 1 – Simetrias em um quadrado

Posto isso, podemos demonstrar que o conjunto de simetrias do polígono é D_{2n} $= \{s^0, s, s^2, ..., s^{n-1}, t, t \circ s, t \circ s^2, ..., t \circ s^{n-1}\}$ e que esse conjunto é um grupo com a operação de composição de transformações.

Definimos assim o Grupo Diedral D_{2n}, com $2n \geq 6$. Este grupo possui ordem $2n$ e é gerado por dois elementos s (rotação) e t (reflexão) tais que:

$$s^n = 1, t \circ t = 1 \text{ e } t \circ s \circ t = s^{-1} \tag{1.1}$$

Na Figura 2, observamos a composição de simetrias para um triângulo equilátero PQR. As retas x, y, z passam pelo baricentro do triângulo e estabelecem os eixos de

simetria. Inicialmente, aplicamos uma reflexão de π em torno da reta z. Em seguida, uma rotação de $2\pi/3$ radianos no sentido anti-horário em torno do centro O. Note que essa composição é equivalente a uma reflexão de π radianos em torno do eixo x a partir do triângulo em sua posição inicial.

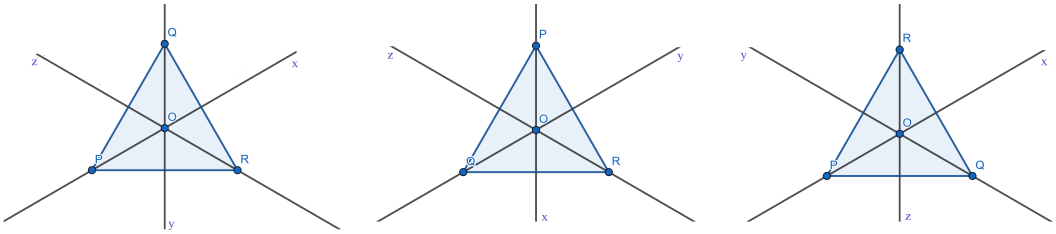

Figura 2 – Composição de simetrias no triângulo regular

O grupo de simetrias do triângulo é dado por $D_6 = \{s^0, s, s^2, t, t \circ s, t \circ s^2\}$. Ou seja, as rotações possíveis $2\pi/3$ radianos em torno de O e as reflexões sobre as retas x, y, z representam os elementos desse grupo.

A Figura 3 mostra por sua vez uma composição de simetrias para um quadrado PQRS regular. As retas x, y, z, w passam pelo centro do quadrado e correspondem aos eixos de simetria deste polígono. Inicialmente, aplicamos duas rotações de $2\pi/4$ no sentido anti-horário em torno do centro O. Em seguida, aplicamos uma reflexão de π radianos em torno da reta y. Note que essa composição é equivalente a uma reflexão de π radianos em torno do eixo x a partir do quadrado em sua posição inicial.

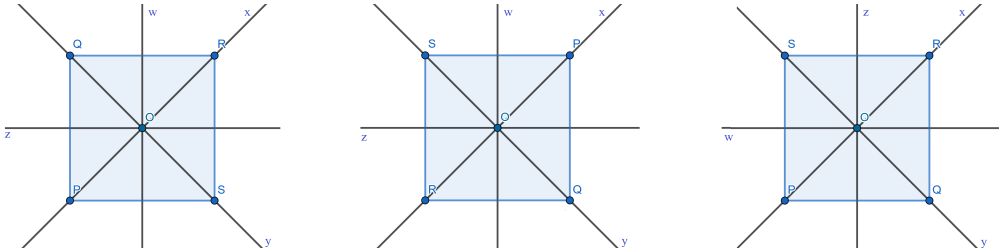

Figura 3 – Composição de simetrias no quadrado regular

O grupo de simetrias do quadrado é dado por $D_8 = \{s^0, s, s^2, s^3, t, t \circ s, t \circ s^2, t \circ s^3\}$. Ou seja, as rotações possíveis $2\pi/4$ radianos em torno de O e as reflexões sobre as retas x, y, z, w representam os elementos desse grupo. Note por fim que D_6 e D_8 não são grupos comutativos. Esse resultado pode ser estendido, D_{2n} não é abeliano para n ≥ 3.

Definição 1.1.2 (Notação Cíclica)**.** *Sejam $l_n = \{1, 2, ..., n\}$ e a_1,a_2,...,$a_r \in l_n$ inteiros distintos. Se $\sigma \in S_n$ é uma permutação tal que $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ..., $\sigma(a_{r-1}) = a_r$ e $\sigma(a_r) = a_1$ e $\sigma(x) = x$, para todo $x \in l_n$ - $\{a_1, a_2, ..., a_r\}$, então se diz que σ é um ciclo de comprimento r e que $\{a_1, a_2, ..., a_r\}$ é o conjunto de suporte de σ. Para designar*

a permutação assim definida, usaremos a notação $(a_1\ a_2\ \ldots\ a_r)$. *Se* $r = 2$, *então* σ *é chamado de transposição.*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

Como $\sigma(1) = 4$, $\sigma(4) = 2$ *e* $\sigma(2) = 1$, $\sigma(3) = 3$ *e* $\sigma(5) = 5$, *então* σ *é um ciclo de comprimento 3 cujo suporte é {1,2,4}. Portanto, podemos escrever:*

$$\sigma = (1\ 4\ 2)$$

Devemos observar que a notação cíclica não indica qual grupo S_n *o ciclo pertence. Além disso, um mesmo ciclo pode ser escrito de diferentes maneiras, por exemplo (1 4 2) = (4 2 1).*

Exemplo 1.1.5. Vamos decompor em transposições a seguinte permutação de S_8:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 8 & 3 & 7 & 5 & 2 & 4 \end{pmatrix}$$

Como $\sigma(1) = 1$, vamos começar o processo descrito na demonstração com o elemento 2:

$$\sigma(2) = 6, \sigma^2(2) = \sigma(\sigma(2)) = \sigma(6) = 5, \sigma(5) = 7, \sigma(7) = 2$$

Portanto:

$$\sigma_1 = (2\ 6\ 5\ 7)$$

Repetimos o processo a partir do 3:

$$\sigma(3) = 8, \sigma(8) = 4, \sigma(4) = 3$$

Portanto:

$$\sigma_2 = (384) \text{ e } \sigma = \sigma_1\sigma_2 = (2657)(384)$$

Neste trabalho, ao analisarmos a composição de funções (ou produto de dois ciclos) a leitura será feita da esquerda para a direita.

Exemplo 1.1.6. Tome o grupo S_4 das permutações de quatro elementos. Apresentaremos o grupo de Klein.

O grupo de Klein é um grupo de quatro elementos formado por todos os produtos possíveis de transposições disjuntas em quatro elementos.

$$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$

O grupo de Klein pode ser descrito como o grupo de simetrias de um retângulo não quadrado (com os três elementos de não identidade sendo reflexão horizontal e vertical e rotação de 180 graus).

1.2 Subgrupos

Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se H for ele próprio um grupo com a mesma operação de G. Assim, para que H seja um subgrupo de G são necessárias as condições:

i. $e \in H$

ii. se $a, b \in H$ então $ab \in H$.

Em geral, essas duas condições não são suficientes para que H seja um subgrupo de G ($H = \mathbb{N} \subset \mathbb{Z} = G$ satisfaz as duas condições acima onde a operação é a soma, porém não é um subgrupo de $(\mathbb{Z}, +)$). Provaremos agora uma proposição que fornece as condições necessárias e suficientes para que um subconjunto H de um grupo G seja um subgrupo de G. Se H for um subgrupo de G denotaremos $H \leq G$.

Proposição 1.2.1. *Sejam G um grupo e H um subconjunto de G. As seguintes condições são equivalentes:*

i. H é um subgrupo de G.

ii. a) e ∈ H

b) $\forall a,b \in H$ temos $ab \in H$.

c) $\forall a \in H$ temos $a^{-1} \in H$.

iii. $H \neq \varnothing$ e $\forall a, b \in H$ temos $ab^{-1} \in H$.

Demonstração. $(i) \Rightarrow (ii)$: Segue imediatamente das definições e da unicidade da identidade e da unicidade do inverso de cada elemento de G.

$(ii) \Rightarrow (i)$: Basta observar que a condição (b) (H é fechado para a operação de G) nos diz que a operação será também associativa pois a operação é associativa em G.

$(ii) \Rightarrow (iii)$: Primeiramente, se $e \in H$ então $H \neq \varnothing$, e se $b \in H$ então $b^{-1} \in H$ por (c).

Assim, se $a, b \in H$, temos $a, b^{-1} \in H$ e por (ii) segue $ab^{-1} \in H$ como queríamos demonstrar.

$(iii) \Rightarrow (ii)$: Se $H \neq \varnothing$, então $\exists a \in H$. Logo, $e = aa^{-1} \in H$. Agora, se $a \in H$ segue $a^{-1} = ea^{-1} \in H$, e finalmente se $a, b \in H$ temos $a, b^{-1} \in H$ e daí teremos $ab = a(b^{-1})^{-1} \in H$ e isto termina a demonstração da Proposição 1.2.1.

□

A seguir observamos alguns exemplos de subgrupos e como eles se encaixam na definição e proposição previamente estabelecidas. Iniciaremos a análise com os subgrupos mais simples. Estes são o $\{e\}$ e o próprio G.

Exemplo 1.2.1. Se G é um grupo, então $\{e\}$ e G são subgrupos de G.

Demonstração. No primeiro caso, notamos que $e \in \{e\}$, além disso $e \cdot e = e$. Temos também que $e^{-1} = e$, logo $e \cdot e \in \{e\}$, assim como $e^{-1} \in \{e\}$. Concluímos que $\{e\}$ é um subgrupo de G. No segundo caso observamos que G por ser um grupo, automaticamente satisfaz as condições de subgrupo. □

Exemplo 1.2.2. $H = m\mathbb{Z} = \{rm : r \in \mathbb{Z}\}$, $m \in \mathbb{Z}$, é um subgrupo do grupo aditivo dos inteiros. É possível observar que $r0 = 0$, logo $0 \in H$. Temos também que se $rn \in m\mathbb{Z}$, $r(m + n) \in m\mathbb{Z}$. Pois $rm + rn = r(m + n)$, e $(m + n) \in \mathbb{Z}$. Por último, notamos que para cada $rm \in m\mathbb{Z}$, temos um inverso $-rm$ para a operação de adição. Essa afirmação é válida, pois $-rm + rm = 0$, com $-r \in \mathbb{Z}$ e $-rm \in m\mathbb{Z}$.

Dado o grupo multiplicativo dos números reais também é possível estabelecer um subgrupo H composto por reais positivos.

Exemplo 1.2.3. O conjunto $H = \{x \in \mathbb{R}^* \mid x > 0\}$ é um subgrupo multiplicativo dos números reais não nulos $(\mathbb{R}^*, \cdot)$. De fato, se $a, b \in H$, então $a, b \in \mathbb{R}$, $a > 0$ e $b > 0$. Mas, se $b > 0$, então $b^{-1} > 0$. Logo $ab^{-1} > 0$, pois o produto de dois números reais estritamente positivos também é estritamente positivo. De onde $ab^{-1} \in H$.

1.2.1 Subgrupo gerado por um subconjunto

Fixemos inicialmente algumas notações. Se H e K são subconjuntos de um grupo G (em particular, se H e K são subgrupos de G), o conjunto $\{hk \mid h \in H \text{ e } k \in K\}$ será denotado por HK, e o conjunto $\{h^{-1} \mid h \in H\}$ será denotado por H^{-1}. Em geral HK não é um subgrupo de G, mesmo quando H e K são subgrupos de G.

Se X é um subconjunto não-vazio do grupo G, o conjunto $\{a_1a_2...a_n \mid n \in \mathbb{N}, a_i \in X \text{ ou } a_i \in X^{-1}\}$ será denotado por $\langle X\rangle$. Quando o conjunto é finito, digamos $X = \{a_1, a_2, ..., a_r\}$, utilizaremos a notação $\langle a_1, a_2, ..., a_r\rangle$ para designar o conjunto $\{a_1a_2...a_n \mid n \in \mathbb{N}, a_i \in X \text{ ou } a_i \in X^{-1}\}$. Observe que se $g \in G$, então $\langle g\rangle = \{..., (g^{-1})^2, g^{-1}, e, g, g^2, ...)\}$; com frequência, quando $r \in \mathbb{N}$, escreveremos g^{-r} para denotar o elemento $(g^{-1})^r$; assim, com estas notações, temos $\langle g\rangle = \{g^t | t \in \mathbb{Z}\}$.

Proposição 1.2.2. *Sejam G um grupo e X um subconjunto não vazio de G. Então o conjunto $\langle X\rangle$ é um subgrupo de G.*

Demonstração. Observe que:

1. $\forall x, y \in \langle X\rangle$, temos $xy \in \langle X\rangle$.
2. $\forall x \in \langle X\rangle$, temos $x^{-1} \in \langle X\rangle$.

Sejam $x, y \in \langle X\rangle$. Temos:

$$x = a_1a_2...a_n, \text{ com } a_i \in X \text{ ou } a_i \in X^{-1}, \forall i$$
$$y = b_1b_2...b_m, \text{ com } b_j \in S \text{ ou } b_j \in X^{-1}, \forall j$$

Logo, $xy = a_1a_2...a_nb_1b_2...b_m$ e $x^{-1} = {a_n}^{-1}{a_{n-1}}^{-1}...{a_2}^{-1}{a_1}^{-1}$ estão também em $\langle X\rangle$. □

Definição 1.2.1. *Sejam G um grupo e X um subconjunto não vazio de G. Então $\langle X\rangle$ é o subgrupo gerado por X.*

1.3 Grupos Cíclicos

Grupos cíclicos são grupos gerados por um único elemento. Esses estão presentes em vários campos na teoria dos grupos. Alguns dos grupos já apresentados são cíclicos, nesta seção essa constatação ficará evidente.

Definição 1.3.1 (Grupo Cíclico)**.** *Se G é um grupo e $a \in G$, então o grupo cíclico gerado por a, denotado por $\langle a\rangle$, é o conjunto de todas as potências de a. Um grupo G é chamado de cíclico se existe um $a \in G$ com $G = \langle a\rangle$; ou seja, G consiste em todas as potências de a.*

Exemplo 1.3.1. O Grupo S_3 das permutações não é cíclico, pois nenhum dos seus elementos gera um grupo de ordem 6. Mas, observe que o subgrupo $H = \{(1), (123), (132)\}$, do grupo das permutações S_3, é cíclico, já que H é gerado por (123). Observe que $(123)^2 = (132), (123)^3 = (1), (132)^2 = (123)$.

Os grupos cíclicos, como vimos anteriormente, são gerados por apenas um elemento. Apesar disso, note que H também poderia ser gerado por (132). Em outras palavras, dentre os diferentes elementos de um grupo, pode ser que haja mais de um gerador. O exemplo 1.3.2 a seguir demonstra esse fato para o caso particular de ($\mathbb{Z}$,+).

Exemplo 1.3.2. Para todo número m, o grupo aditivo $\mathbb{Z}$ dos números inteiros é cíclico, pois $\mathbb{Z}_m = \langle\bar{1}\rangle$. Em outras palavras, todos os seus elementos são múltiplos de 1 ou de -1. De fato, $\mathbb{Z} = \{m \cdot 1 \mid m \in \mathbb{Z}\}$ ou $\mathbb{Z} = \{m \cdot (-1) \mid m \in \mathbb{Z}\}$. Portanto, $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$. Os números 1 e -1 são, na verdade, os únicos geradores de $\mathbb{Z}$.

Exemplo 1.3.3. Notemos que se G é um grupo cíclico gerado por um elemento a e $x = a^m$, $y = a^n \in G$, então $xy = a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m = yx$, portanto G é abeliano.

1.4 Homomorfismos

Grupos diferentes, com elementos diferentes, podem apresentar estruturas algebricamente iguais. Um homomorfismo entre, os grupos G e H, é uma função entre dois conjuntos que preserva as estruturas de grupo, ou seja, é compatível com as operações. Quando esta função é bijetiva é possível estender as propriedades do primeiro grupo para o segundo.

Definição 1.4.1 (Homomorfismo)**.** *Suponha que (G,$*$) e (H,$\circ$) sejam dois grupos. Uma função f:G$\to$H é um homomorfismo se, para todos a,b $\in$ G,*

$$f(a*b)=f(a)\circ f(b).$$

Um homomorfismo sobrejetivo é chamado de epimorfismo. Já um homomorfismo injetivo é um monomorfismo. Por fim, um homomorfismo bijetivo é um isomorfismo.

Isomorfismo é uma função especial que quando construída entre dois grupos permite assegurar que o que é verdade para um elemento do primeiro grupo também é verdade para seu correspondente no segundo grupo. Não são isomorfos grupos que apresentem quantidades diferentes de elementos, que apresentem características diferentes quanto a comutatividade (abeliano e não abeliano). Dizemos que G é isomorfo a H, denotando por $G \cong H$, se existe um isomorfismo $f : G \to H$. Por último, se $f : G \to H$ é um homomorfismo bijetor, então $f^{-1} : H \to G$ é também um homomorfismo .

Teorema 1.4.1. *Seja f:(G,$\cdot$)$\to$(H,$\circ$) um homomorfismo:*

i. $f(e) = e'$, onde e' é a identidade em H.

ii. Se $a \in G$, então $f(a^{-1})=f(a)^{-1}$.

iii. Se $a \in G$ e $n \in \mathbb{Z}$, então $f(a^n)$=$f(a)^n$.

Demonstração. (i) Aplicando f a equação $e = e \cdot e$ temos $f(e) = f(e \cdot e) = f(e) \circ f(e)$. Agora podemos multiplicar cada lado da equação por $f(e)^{-1}$ para se obter $e' = f(e)$.

(ii) Aplicando f as equações $a \cdot a^{-1} = e = a^{-1} \cdot a$ temos $f(a) \circ f(a^{-1})$. Segue do Teorema 1, a unicidade do inverso, que $f(a^{-1}) = f(a)^{-1}$.

(iii) Por uma indução simples é possível mostrar que $f(a^n) = f(a)^n$ para todo $n \geq 0$, e então $f(a^{-n}) = f((a^{-1})^n) = f(a^{-1})^n = f(a)^{-n}$. □

Exemplo 1.4.1. Seja $n \in \mathbb{Z}$ fixo. Então, ϕ_n: $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$, $\phi_n(z) = nz$, é um homomorfismo. Mais geralmente, se $(G,\cdot)$ é um grupo abeliano então ϕ_n: $G \to G$, $\phi_n(g) = g^n$, é um homomorfismo.

Exemplo 1.4.2. A função denotada por υ: $\mathbb{Z} \to \mathbb{Z}_m$, definida por $\upsilon(a) = \overline{a}$, é um homomorfismo sobrejetivo, pois:

i. $\upsilon(a + b) = \overline{a + b} = \overline{a}+\overline{b}$

ii. se $y \in \mathbb{Z}_m$, então y= $\overline{a}$, para algum $a \in \{0, 1, 2, ..., m - 1\}$, e, portanto, $\upsilon(a) = \overline{a} = y$.

Dois conceitos são fundamentais na discussão acerca de homomorfismos: núcleo e imagem. Estes conjuntos desempenham um papel importante na Teoria dos Grupos por conta de suas propriedades. Algumas dessas serão exploradas mais adiante.

O núcleo de um homomorfismo é o conjunto de elementos de G que resultam no elemento neutro de H quando este homomorfismo é aplicado sobre eles.

Definição 1.4.2 (Núcleo)**.** *Dado um homomorfismo ϕ de um grupo G para um grupo H, o Núcleo de ϕ é Ker(ϕ)=$\{x \in G \mid \phi(x) = e\}$.*

Se ϕ é um monomorfismo, então o núcleo é trivial: Ker(ϕ) = $\{e\}$. Além disso, K = Ker(ϕ) é um subgrupo de G. De fato, note que $\phi(e) = e$, então $e \in K$. Além disso, se $s, t \in K$, então $\phi(s)$= $e = \phi(t)$, e também $\phi(st^{-1}) = \phi(s)\phi(t)^{-1} = e$; por isso $st^{-1} \in K$.

A imagem do homomorfismo, por sua vez, representa todos os elementos de H que são obtidos ao aplicarmos este homomorfismo sobre G.

Definição 1.4.3 (Imagem)**.** *Dado um homomorfismo ϕ de um grupo G para um grupo H, a Imagem de ϕ é definida por Im(ϕ) = $\{h \in H: h = \phi(a)$ para algum $a \in G\}$.*

Definiremos agora os automorfismos, que são isomorfismos que levam elementos de um grupo em elementos do mesmo grupo. Em alguns casos, o conjunto de automorfismos de um grupo G, é um grupo com a operação de composição de funções.

Definição 1.4.4 (Automorfismo)**.** *Um automorfismo de um grupo G é um isomorfismo $\sigma: G \to G$. O conjunto de todos os automorfismos do grupo G será denotado por:*

$$Aut(G) = \{\sigma: G \to G, \text{ onde } \sigma \text{ é um isomorfismo.}\}$$

1.5 Classes Laterais e o Teorema de Lagrange

Nesta seção, as classes laterais serão definidas e exemplificadas. Os conceitos de ordem e índice serão abordados e por fim o teorema de Lagrange será apresentado.

Classes laterais são subconjuntos de um grupo, estas podem ser à direita ou à esquerda.

Definição 1.5.1 (Classes Laterais)**.** *Se S é um subgrupo de G e se $t \in G$, então uma classe lateral à direita de S em G é o subconjunto de G*

$$St = \{st: s \in S\}.$$

De igual forma uma classe lateral à esquerda é $tS = \{ts: s \in S\}$. O elemento t é um representante de St, assim como de tS.

Exemplo 1.5.1. Seja $G = S_3$ e seja $H = \langle\tau\rangle = \{1, \tau\}$, onde $\tau = (12)$. As classes laterais à direita de H em G são

$$H = \{1, \tau\}; H(123) = \{(123), (23)\}; H(132) = \{(132), (23)\}.$$

Lema 1.5.1.1. *Se $S \leq G$, então $Sa = Sb$ se e somente se $ab^{-1} \in S$ ($aS = bS$ se e somente se $b^{-1}a \in S$).*

Demonstração. Se $Sa = Sb$, então $a = 1a \in Sa = Sb$, e então existe $s \in S$ com $a = sb$; logo, $ab^{-1} \in S$. Consequentemente, assuma que $ab^{-1} = \sigma \in S$; logo $a = \sigma b$. Para provar que $Sa = Sb$, devemos mostrar duas inclusões. Se $x \in Sa$, então $x = sa$ para algum $s \in S$, e então $x = s\sigma b$; similarmente, se $y \in Sb$, então $y' = s'b$ para algum $s' \in S$, e $y = s'\sigma^{-1}a \in Sa$. Portanto, $Sa = Sb$. □

Teorema 1.5.1. *Se $S \leq G$, então quaisquer classes laterais à direita (ou à esquerda) de S em G são idênticas ou disjuntas.*

Demonstração. Primeiro mostraremos que se existe um elemento $x \in Sa \cap Sb$, então $Sa = Sb$. Suponha um x que tenha a forma $sb = x = ta$, onde $s, t \in S$. Então, $ab^{-1} = t^{-1}s \in S$, e então a partir do Lema 1.5.1.1 concluímos que $Sa = Sb$.

□

Se $S \leq G$, então o número de classes laterais à direita de S em G é igual ao número de classes laterais à esquerda de S em G.

Temos uma bijeção $f : R \to L$, aonde R é a família de classes laterais à direita de S em G e L é a família de classes à esquerda. Se $Sa \in R$, definimos a função $f(Sa) = a^{-1}S$. Observamos que se $Sa = Sb$, então $a^{-1} = b^{-1}S$. É rotineiro mostrar que f é uma bijeção.

O índice de um grupo G em um subgrupo S se refere ao número de elementos que possuem o conjunto das classes laterais.

Definição 1.5.2 (Índice)**.** *Se $S \leq G$, então o índice de S em G, denotado por [G:S], é o número de classes laterais à direita de S em G.*

Exemplo 1.5.2. Retomando o Exemplo 1.3.1, notamos que o índice de H em S_3 é dois, pois:

$$H = \{1, \tau\}; H(123) = \{(123), (23))\}; H(132) = \{(132), (23)\}.$$

A ordem de um grupo se refere a cardinalidade desse. Ou seja, ao número de elementos que ele possui. Já a ordem de um elemento de um grupo se refere ao menor positivo m tal que $a^m = e$. Isso equivale a dizer que refere-se ao número de elementos gerados por a.

Definição 1.5.3 (Ordem de um Grupo)**.** *O número de elementos de um grupo finito G diz-se a ordem de G e representa-se por $|G|$. Um grupo com uma infinidade de elementos diz-se ter ordem infinita.*

Definição 1.5.4 (Ordem de um elemento de um grupo G)**.** *Se G é um grupo e $a \in G$, então a ordem de a é $|\langle a \rangle|$, o número de elementos de $\langle a \rangle$.*

Teorema 1.5.2. *Se G é um grupo e $a \in G$ tem ordem finita m, então m é o menor inteiro positivo tal que $a^m = e$.*

Teorema 1.5.3 (Teorema de Lagrange)**.** *Se G é um grupo finito e $H \leq G$, então $|H|$ divide $|G|$ e $[G:H] = |G|/|H|$.*

De fato, pelo Teorema 1.5.1, G pode ser particionado em classes laterais a direita:

$$G = Ht_1 \cup Ht_2 \cup \cdots \cup Ht_n,$$

e também $|G| = \sum_{i=1}^{n} |Ht_i|$. Mas é fácil reparar que f_i: $H \to Ht_i$, definida por $f_i(h) = ht_i$, é uma bijeção, de modo que $|Ht_i| = |H|$ para todos os i. Assim, $|G| = n|H|$, onde $n = [G:H]$.

Exemplo 1.5.3. Encontraremos todos os subgrupos de S_3 e suas respectivas ordens.

O grupo S_3 tem 6 elementos. Um subgrupo H de S_3, pelo Teorema de Lagrange, só pode ter $|H| \in \{1, 2, 3\}$, que são os divisores de 6. O único subgrupo de ordem 1 é $\{(1)\}$. Os subgrupos de ordem 2 são:

$$\langle(23)\rangle = \{(1), (23)\},$$
$$\langle(13)\rangle = \{(1), (13)\},$$
$$\langle(12)\rangle = \{(1), (12)\}.$$

Existe apenas um único subgrupo de ordem 3 que é $\langle(123)\rangle = \{(1), (123), (132)\} = \langle(132)\rangle$.

1.6 Apresentação de Grupos

Os grupos gerados por um elemento, os grupos cíclicos, foram facilmente abordados. Contudo, os grupos gerados por mais de um elemento são muito mais difíceis de se trabalhar e classificar. Mesmo os grupos gerados por dois elementos, podem ser extremamente complicados. (Por exemplo: existem mais pares de grupos dois gerados não isomorfos do que números naturais; cada grupo enumerável é um subgrupo de um quociente do grupo dois gerado $SL_2(\mathbb{Z})$; todo grupo simples finito pode ser gerado por dois elementos). Vamos começar nosso estudo analisando o caso de alguns grupos finitos gerados por dois elementos e introduzir o conceito de *relações* em um grupo. Nosso objetivo é chegar ao conceito de *apresentação de um grupo*. Em nossa abordagem, evitaremos tocar na demonstração rigorosa, contudo, demos enfoque a essência do conceito em si. Para uma definição formal veja a referência-padrão [5].

Exemplo 1.6.1. Considere mais uma vez o subgrupo H de S_3, onde $H = \{(1), \alpha = (123), \beta = (132)\}$. Observe que em H valem as igualdades:

$\alpha^3 = (123)^3 = (1)$

$\alpha^2 = (123)^2 = (132) = \beta$

As igualdades $\alpha^3 = (123)^3 = e$, $\alpha^2 = \beta$ são chamadas de *relações* em H. Agora vamos mostrar que a relação $\alpha^3 = e$ determina completamente H. Se G é um grupo de ordem 3 no qual existe A tal que:

$$\begin{cases} G = \langle A\rangle \\ A^3 = e \end{cases}$$

então existe um homomorfismo f entre H e G, tal que $f(\alpha) = A$. Assim, a menos de isomorfismos, o grupo H é caracterizado como sendo o grupo gerado por um elemento α que satisfaz a relação $\alpha^3 = e$, ou seja:

$$\begin{cases} G = \langle \alpha \rangle \\ \alpha^3 = e \end{cases}$$

Nesse caso, dizemos que H tem a *apresentação*: $\langle \alpha \mid \alpha^3 = e \rangle$.

Exemplo 1.6.2. Sejam $\alpha = (132)$ e $\beta = (13)$, ambos elementos de S_3 temos:

$\alpha^2 = (132)(132) = (123)$

$\alpha^3 = (132)(132)(132) = e$

$\beta^2 = (13)(13) = e$

$\beta\alpha = (13)(132) = (12)$

$\alpha^2\beta = (132)(132)(13) = (12)$

Vemos que S_3 é um grupo de ordem 6 tal que:

$$\begin{cases} S_3 = \langle \alpha, \beta \rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^2\beta. \end{cases}$$

As igualdades $\alpha^3 = e$, $\beta^2 = e$, e $\beta\alpha = \alpha^2\beta$ são relações em S_3. Agora vamos mostrar que essas relações determinam completamente S_3. Se G é um grupo de ordem 6 no qual existem A e B tais que:

$$\begin{cases} G = \langle A, B \rangle \\ A^3 = e \\ B^2 = e \\ BA = A^2B, \end{cases}$$

então existe um homomorfismo f entre S_3 e G, tal que $f(\alpha) = A$ e $f(\beta) = B$. Assim, a menos de isomorfismos, o grupo S_3 é caracterizado como sendo o grupo de ordem 6 gerado por dois elementos α e β que satisfazem as relações:

$$\begin{cases} \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^2\beta. \end{cases}$$

Nesse caso, dizemos que S_3 tem a *apresentação*: $\langle \alpha, \beta \mid \alpha^3 = e,\ \beta^2 = e,\ \alpha\beta = \alpha^2\beta \rangle$.

Exemplo 1.6.3. Similarmente, $D_8 = \{s^0,\ s,\ s^2,\ s^3,\ t,\ t \circ s,\ t \circ s^2,\ t \circ s^3\}$ é um grupo de ordem 8 tal que:

$$\begin{cases} D_8 = \langle s, t \rangle \\ s^4 = e \\ t^2 = e \\ t \circ s = s^3 \circ t. \end{cases}$$

Pois:

$s^4 = s^0$

$t^2 = s^0$

$s^{-1} = t \circ s \circ t$

$s^3 \circ t = s^{-1} \circ s \circ s^3 \circ t = s^{-1} \circ s^0 \circ t = s^{-1} \circ t = t \circ s \circ t \circ t = t \circ s \circ t^2 = t \circ s$

Para mais detalhes ver Equação 1.1.

As igualdades $s^4 = e$, $t^2 = e$, e $ts = s^3t$ são relações em D_8. Agora vamos mostrar que essas relações determinam completamente D_8. Se G é um grupo de ordem 8 no qual existem A e B tais que:

$$\begin{cases} D_8 = \langle A, B \rangle \\ A^4 = e \\ B^2 = e \\ BA = A^3B, \end{cases}$$

então existe um homomorfismo f entre D_8 e G: tal que $f(s) = A$ e $f(t) = B$. Assim, a menos de isomorfismos, o grupo D_8 é caracterizado como sendo o grupo de ordem 8 gerado por dois elementos s e t que satisfazem as relações:

$$\begin{cases} s^4 = e \\ t^2 = e \\ ts = s^3t. \end{cases}$$

Portanto, dizemos que D_8 tem a *apresentação*: $\langle s, t \mid s^4 = e,\ t^2 = e,\ t \circ s = s^3 \circ t \rangle$.

Exemplo 1.6.4. O grupo de *Klein* ou das permutações $K = \{(1), (12)(34) = \alpha, (13)(24) = \beta, (14)(23) = \alpha\beta\}$ é um grupo de ordem 4 tal que:

$$\begin{cases} K = \langle \alpha, \beta \rangle \\ \alpha^2 = e \\ \beta^2 = e \\ \beta\alpha = \alpha\beta \end{cases}$$

Pois:

$\alpha^2 = (12)(34)(12)(34) = (1)$

$\beta^2 = (13)(24)(13)(24) = (1)$

$\beta\alpha = (12)(34)(13)(24) = (14)(23)$

$\alpha\beta = (13)(24)(12)(34) = (14)(23)$

As igualdades $\alpha^2 = e$, $\beta^2 = e$, e $\alpha\beta = \beta\alpha$ são relações em K. Agora vamos mostrar que essas relações determinam completamente K. Se G é um grupo de ordem 4 no qual existem A e B tais que:

$$\begin{cases} K = \langle A, B \rangle \\ A^2 = e \\ B^2 = e \\ BA = AB \end{cases}$$

então existe um homomorfismo f entre K e G: tal que $f(\alpha) = A$ e $f(\beta) = B$. Assim, a menos de isomorfismos, o grupo K é caracterizado como sendo o grupo gerado por dois elementos α e β que satisfazem as relações:

$$\begin{cases} \alpha^2 = e \\ \beta^2 = e \\ \beta\alpha = \alpha\beta \end{cases}$$

Portanto, dizemos que o grupo de *Klein* tem a *apresentação*: $\langle \alpha, \beta \mid \alpha^2 = e, \beta^2 = e, \beta\alpha = \alpha\beta \rangle$.

De modo geral, as relações em um grupo G gerado por um conjunto finito X, são o conjunto de equações que podem ser apresentadas sobre a forma $a = b$ com $a, b \in G$, fazendo correspondência com $ab^{-1} = e$. Em casos muito particulares, grupos finitos gerados por dois elementos, $G = \langle a, b \rangle$, com elementos a e b, apresentam relações do tipo $ba = a^s b$ com $s \in \mathbb{Z}$.

Definição 1.6.1. *Um conjunto contendo as relações de G será denotado por R. Quando o conjunto X de geradores e um conjunto R de relações determinam G, a menos de isomorfismo, dizemos que G tem apresentação $G = \langle X|R \rangle$. Os elementos de X são chamados*

de geradores de G e os elementos de R são chamados de relações em G. Um grupo G é finitamente apresentado se possui uma apresentação com os conjuntos X e R finitos.

1.7 Subgrupos Normais

Definição 1.7.1 (Subgrupo Normal)**.** *Um subgrupo K de G é um subgrupo normal, denotado por $K \trianglelefteq G$, se $gKg^{-1} = K$ para todo $g \in G$.*

Se K G e $gKg^{-1} \leq K$ para todo $g \in G$, então $K \trianglelefteq G$: substituindo g por g^{-1}, temos $g^{-1}Kg \leq K$, e isso nos dá a inclusão reversa $K \leq gKg^{-1}$.

Exemplo 1.7.1. O núcleo de um homomorfismo $f : G \to H$ é um subgrupo normal. De fato, se $a \in K$, então $f(a) = 1$; se $g \in G$, então $f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)f(g)^{-1} = 1$, e então $gag^{-1} \in K$. Portanto, $gKg^{-1} \leq K$ para todo $g \in G$, e então $K \trianglelefteq G$.

Exemplo 1.7.2. $G' = \langle\ x^{-1}y^{-1}xy |\ x, y \in G\ \rangle$ é um subgrupo normal de G.

Primeiro, observe que se chamamos de S o conjunto $\{x^{-1}y^{-1}xy \mid x, y \in G\}$ e se $\alpha \in S$, então $\alpha^{-1} \in S$; consequentemente, se ξ é um elemento qualquer de $G' = \langle S \rangle$, então ξ se escreve da forma $\xi = \alpha_1 ... \alpha_n \in S$. Segundo, se $g \in G$, temos:

$$g^{-1}\xi g = g^{-1}(\alpha_1 ... \alpha_n)g = (g^{-1}\alpha_1 g)(g^{-1}\alpha_2 g)...(g^{-1}\alpha_n g)$$

e consequentemente, para ver que $g^{-1}\xi g \in G'$, basta ver que vale $g^{-1}\alpha g \in$ S quando $\alpha \in S$. Seja então $\alpha = x^{-1}y^{-1}xy$ um elemento de S; temos:

$$g^{-1}\alpha g = g^{-1}(x^{-1}y^{-1}xy)g = (g^{-1}x^{-1}g)(g^{-1}y^{-1}g)(g^{-1}xg)(g^{-1}yg) = (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \in S.$$

Definição 1.7.2 (Comutador)**.** *Se a,b ∈ G, o comutador de a em b, denotado por [a,b] é*

$$[a,b] = a^{-1}b^{-1}ab.$$

Conforme demonstrado, o subgrupo comutador (ou derivado) de G, denotado por G′, é o subgrupo gerado por todos os comutadores de G.

Definição 1.7.3 (Conjugado)**.** *Se $x \in G$, então o conjugado de x em G é um elemento da forma $a^{-1}xa$ para algum $a \in G$.*

Lema 1.7.3.1. *Se G é um grupo, então a relação "y é um conjugado de x em G", ou seja, y=$g^{-1}xg$ para algum $g \in G$, é uma relação de equivalência.*

Definição 1.7.4. *Se G é um grupo, então a classe de equivalência de $a \in G$ sobre a relação "y é um conjugado de x em G" é chamada de classe de conjugação de a, é denotada por a^G.*

Teorema 1.7.1. *Se $N \trianglelefteq G$, então as classes laterais de N em G formam um grupo, denotado G/N, de ordem [G:N].*

Para se definir um grupo, é necessário um conjunto e uma operação. O conjunto é a família das classes laterais de N em G. Das propriedades de subgrupo normal temos,

$$NaNb = Na(a^{-1}Na)b$$

$$=N(aa^{-1})Nab = NNab = Nab$$

Então produto de duas classes laterais é uma classe lateral. Como operação binária utilizaremos o produto $NaNb = Nab$. Essa operação é associativa, o elemento neutro é $N = N1$ e o inverso de Na é $N(a^{-1})$. Esse grupo é denotado por G/N, e a definição de índice nos dá $|G/N| = [G:N]$.

O centro de um grupo é um subgrupo de G formado pelas classes de conjugação com apenas um elemento. É o conjunto de elementos em G que comutam com cada elemento de G. No caso de um grupo abeliano, o centro do grupo é o próprio grupo abeliano.

Definição 1.7.5 (Centro do Grupo)**.** *O centro de um grupo G, denotado por Z(G), é o conjunto de todos $a \in G$ que comutam com cada elemento de G.*

Definição 1.7.6 (Centralizador)**.** *Se $a \in G$, então o centralizador de a em G, denotado por $C_G(a)$, é o conjunto de todos os $x \in G$ que comutam com a.*

Definição 1.7.7 (Conjugado de um Grupo)**.** *Se $H \leq G$ e $g \in G$, então o conjugado $g^{-1}Hg$ é $\{g^{-1}hg: h \in H\}$.O conjugado $g^{-1}hg$ também é denotado por H^g.*

1.8 Produto Direto e Ação de Grupos

Definição 1.8.1 (Produto Direto)**.** *Se H e K são grupos, então o produto direto deles denotado por $H \times K$, é o grupo com elementos todos ordenados em pares (h,k), onde $h \in H$ e $k \in K$, com a operação:*

$$(h,k)(h',k') = (hh',kk').$$

De fato, $H \times K$ é um grupo: a identidade é (e,e); o inverso de $(h,k)^{-1}$ é (h^{-1},k^{-1}). Note que nem H e nem K são subgrupos de $H \times K$, mas $H \times K$, continua contendo réplicas

isomorfas de cada um deles, $H \times \{e\} = \{(h,e): h \in H\}$*, assim como,* $\{e\} \times K = \{(e,k): k \in K\}$*.*

Quando os grupos H e K são abelianos, podemos nos referir ao produto direto como uma soma direta, denotada por $H \bigoplus K$, e chamar a operação de soma ao invés de produto. Somas diretas infinitas tem a restrição de que cada elemento tem apenas um número finito de entradas não nulas. Essa não é uma restrição para produtos diretos infinitos, ao impor essa restrição temos um produto direto restrito.

Exemplo 1.8.1. O grupo de *Klein* pode ser descrito como o produto direto de duas cópias de $\mathbb{Z}_2$. Sua apresentação é $K = \langle a, b | a^2 = b^2 = (ab)^2 = e \rangle$.

Exemplo 1.8.2. Considere os elementos $\alpha_0 = (\bar{0},\bar{0})$, $\alpha_1 = (\ \bar{1},\ \bar{0})$, $\alpha_2 = (\ \bar{0},\ \bar{1})$ e $\alpha_3 = (\bar{1},\bar{1})$ do grupo de *Klein* $(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Então,

$$f_i\colon \mathbb{Z}_2 \to (\mathbb{Z}_2) \times \mathbb{Z}_2$$
$$\bar{0} \to (\bar{0},\ \bar{0})$$
$$\bar{1} \to \alpha_i$$

é um homomorfismo injetivo ($\forall i = 1,2,3$).

Exemplo 1.8.3. Seja $G = \bigoplus_{i=2}^{\infty}(\mathbb{Z}_i)$ a soma direta dos grupos $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, etc, chamados de fatores diretos. Os elementos de G são sequências infinitas cujas entradas estão em $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, ..., respectivamente. Observe que cada tupla possui finitas entradas não nulas, pois se trata de uma soma direta. A operação consiste em somar entrada a entrada os elementos do respectivo grupo, usando a soma módulo i – inerente ao fator direto. (Por simplicidade vamos omitir as "barras" dos elementos $\bar{n}$ de $\mathbb{Z}_i$.)

Concretamente, se

$$x = (1, 0, 3, 4, 4, 6, 0, 0, 0, ...)$$
$$y = (0, 2, 3, 1, 5, 6, 0, 0, 0, ...),$$
$$\text{então } x + y = (1, 2, 2, 0, 3, 5, 0, 0, 0, ...).$$

Exemplo 1.8.4. Considere o grupo $\bigoplus_{i\in\mathbb{Z}}(\mathbb{Z}_2)$. Este é um grupo cujos elementos são sequências bi-infinitas (infinitas para a esquerda e para a direita) que possuem zeros e uns (módulo 2) como entradas. Destacamos que há apenas um número finito de entradas iguais a um. O elemento genérico x indica o índice das entradas:

$$x = (...x_{-4},\ x_{-3},\ x_{-2},\ x_{-1},\ x_0,\ x_1,\ x_2,\ x_3,\ x_4...)$$

Por exemplo, se

$$a = (...0, 0, 0, 0, 0, 1, 1, 0, 0...)$$

e

$$b = (...0, 0, 1, 0, 1, 1, 1, 0, 0...),$$

então

$$a + b = (...0, 0, 1, 0, 1, 0, 0, 1, 0...).$$

Note que a adição nas entradas é feita em $\mathbb{Z}_2$. Essa soma mais a frente será novamente abordada.

Definição 1.8.2 (Ação de Grupos)**.** *Se X é um conjunto e G um grupo, dizemos que G age sobre X se existe uma função α: $G \times X \to X$ (chamada ação), denotada por α:(g,x)$\mapsto$gx, tal que:*

i. 1x = x para todo $x \in X$; e

ii. g(hx) = (gh)x para todos g,h $\in$ G e $x \in X$.

Se |X| = n, então n é chamado de ordem da ação de G em X.

Teorema 1.8.1. *Se G age sobre X por meio de uma ação α, então existe um homomorfismo $\tilde{\alpha}$: $G \to S_X$ dado por $\tilde{\alpha}(g)$: $x \mapsto gx = \alpha(g,x)$. Por outro lado, todo homomorfismo ϕ:$G \to S_X$ define uma ação, isto é, $gx = \phi(g)x$, que faz com que G aja sobre X.*

Se X é um conjunto sobre o qual G age, com $g \in G$, e $x \in X$, então:

$$\tilde{\alpha}(g^{-1})\tilde{\alpha}(g)\text{: } x \to \tilde{\alpha}(g^{-1})(gx) = g^{-1}(gx) = (g^{-1}g)x = 1x = x.$$

Segue que cada $\tilde{\alpha}(g)$ é uma permutação de X com inverso $\tilde{\alpha}(g^{-1})$. Logo $\tilde{\alpha}$ é um homomorfismo de acordo com a definição de ação de grupos. O contrário também é verificável.

Definição 1.8.3 (Órbitas)**.** *Se X é um conjunto sobre o qual G age e $x \in X$, então a órbita de x é:*

$$\mathcal{O}=\{gx\text{: } g \in G\} \subset X.$$

As órbitas de G definem uma partição, já que a relação $x \equiv y$ definida por "y = gx para algum $g \in G$" é uma relação de equivalência cujas classes de equivalência são as órbitas.

Definição 1.8.4 (Estabilizador)**.** *Se X é um conjunto sobre o qual G age, então o estabilizador de x, denotado pelo grupo G_x, é o subgrupo*

$$G_x = \{g \in G: gx = x\} \leq G.$$

Teorema 1.8.2. *Se X é um conjunto sobre o qual G age e $x \in X$, então*

$$|\mathcal{O}(x)| = [G : G_x]$$

Se $x \in X$, faça G/G_x denotar a família de todas as classes laterais à esquerda de G_x em G. Defina $f : \mathcal{O}(x) \to G/G_x$ por $f(ax) = aG_x$. Agora f está bem definida: se $ax = bx$ para algum $b \in G$, então $b^{-1}ax = x$, $b^{-1}a \in G_x$, e a $G_x = bG_x$. A função f é uma injeção: se $aG_x = f(ax) = f(cx) = cG_x$ para algum $c \in G$, então $c^{-1}a \in G_x$, $c^{-1}ax = x$, e $ax = cx$; a função f é uma sobrejeção: se $a \in G$, então $aG_x = f(ax)$. Logo, f é uma bijeção e $|\mathcal{O}(x)| = |G/G_x| = [G : G_x]$.

Definição 1.8.5 (Produto Semi-Direto)**.** *Um grupo G é o produto semi-direto de seus subgrupos K e H se:*

i. $K \trianglelefteq G$

ii. $G = KH$

iii. $K \cap H = \{e\}$

Considere grupos arbitrários K e H, com H agindo sobre K via ψ, isto é:

$$\psi: H \longrightarrow Aut(K),\ h \mapsto (\psi_h: k \mapsto k^h).$$

Seja $G = \{(k,h) \mid k \in K,\ h \in H\}$ e definamos a operação:

$$(k,h)(k_1,h_1) = (kk_1{}^h, hh_1) \text{ onde } k,\ k_1 \in K, \text{ assim como, } h,\ h_1 \in H.$$

Podemos verificar que G é um grupo e além disso temos que $K_1 = \{(k, e) \mid k \in K\}$ e $H_1 = \{(e, h) \mid h \in H\}$ são subgrupos de G tais que $K_1 \trianglelefteq G$, $K_1 \cap H_1 = \{e\}$ e $G = K_1H_1$. Observamos que K_1 é isomorfo a K e H_1 é isomorfo a H. Assim G é o produto semi-direto de $K_1 \cong K$ por $H_1 \cong H$ e denotamos $G = K \rtimes H$.

Exemplo 1.8.5. O grupo Simétrico S_n, $n \leq 3$, é um produto semi-direto do grupo das permutações pares A_n pelo grupo cíclico de ordem dois $\mathbb{Z}_2$, escrevemos $S_n = A_n \rtimes \mathbb{Z}_2$.

2 Autômatos

A classe dos grupos gerados por autômatos contém vários objetos notáveis. O estudo dessa classe levou à solução de uma série de problemas importantes na teoria dos grupos, ver [9] e [16]. Suas aplicações recentes se estenderam aos campos da álgebra, geometria, análise e probabilidade. Juntamente com grupos aritméticos e hiperbólicos, grupos de autômatos dominam a paisagem moderna da Teoria dos Grupos Infinitos.

Neste capítulo serão introduzidos conceitos importantes relacionados a autômatos, conforme [14] e [3]. Entre eles, a definição básica de grafos, árvores enraizadas, que constituem uma interpretação geométrica de grupos, automorfismos em árvores, prefixos e sufixos de palavras em monoides. Por fim, será apresentada a máquina de *Mealy*, assim como exemplos variados de autômatos. Esses constituem requisitos essenciais para a discussão posterior.

2.1 Árvores enraizadas

O conceito de árvore enraizada surge a partir do conceito de grafo. A Teoria dos Grafos estuda as relações entre elementos de um determinado conjunto. Foi desenvolvida inicialmente por Leonard Euler como resposta ao famoso problema matemático das sete pontes de Königsberg. Informalmente, os grafos podem ser definidos como um conjunto de vértices conectados dois a dois por arestas. A árvore enraizada, por sua vez, possui um vértice específico (raiz), tal que existe apenas um único caminho simples para qualquer outro vértice. As definições formais são dadas a seguir.

Definição 2.1.1. *Um grafo simples* Γ *= (V,E) consiste em V, um conjunto não vazio de vértices, e E, um conjunto de pares de elementos não ordenados (não repetidos),*$\{\nu_1,\nu_2\}$ *de elementos distintos de V, chamados de arestas.*

Definição 2.1.2. *Seja* Γ *e K grafos simples com vértices nos conjuntos X e Y, respectivamente. Se existe uma função bijetiva* $\phi : X \to Y$ *tal que dois dos vértices s e t em X são adjacentes em* Γ *se, e somente se,* $\phi(s)$ *e* $\phi(t)$ *em Y são adjacentes em K, então* Γ *e K são grafos isomorfos.*

Definição 2.1.3. *Uma árvore enraizada finita é um grafo conexo simples com um vértice específico* ν_0*, designado como raiz da árvore, tal que existe um único caminho simples para qualquer outro vértice de* ν_0*.*

Nos diagramas aqui utilizados, a raiz será localizada no topo da árvore, com todos os outros vértices abaixo. Notamos que em uma árvore enraizada finita o número de

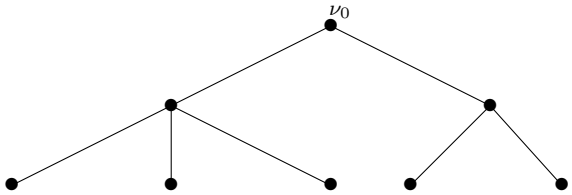

Figura 4 – Árvore Enraizada

vértices é sempre superior ao número de arestas (ver Figura 4).

Definição 2.1.4. *O nível de um vértice ν em uma árvore enraizada é o número de arestas em um caminho simples de ν para ν_0. Uma árvore sem arestas e somente com o vértice raiz, é uma árvore trivial.*

Definição 2.1.5. *A árvore binária infinita completamente enraizada $\mathcal{T}$ é uma árvore enraizada com um número infinito de níveis contáveis, onde cada vértice possui dois vértices descendentes (Figura 5).*

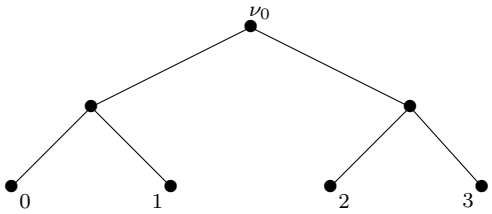

Figura 5 – Árvore Enraizada Binária

Definição 2.1.6. *Uma sub-árvore enraizada de $\mathcal{T}$ é uma árvore enraizada $\mathcal{T}'$ cuja raiz é um dos vértices de $\mathcal{T}$ e cujos vértices e arestas também pertencem a $\mathcal{T}$.*

2.2 Automorfismo em Árvores

O grupo dos automorfismos da árvore regular binária uni-raiz, Figura Figura 6, tomou notoriedade quando certos exemplos de subgrupos com as propriedades: finitamente gerado, periódico e infinito, foram construídos dentro dele. Além disso, esse grupo pode ser representado como um produto semidireto.Por conta dessas propriedades há um interesse crescente nesse grupo. Na presente seção o grupo de automorfismo da árvore enraizada será definido.

Definição 2.2.1. *Seja Y o alfabeto {0, 1}. Considere $\mathcal{M} = \mathcal{M}(Y)$ o conjunto de todas as palavras finitas formadas por elementos de Y. Com a operação de concatenação de palavras, $\mathcal{M}$ assume estrutura de monóide, isto é, um conjunto com uma operação associativa e um elemento neutro segundo esta operação. Neste caso, o elemento neutro é a palavra vazia $\varnothing$.*

Temos então que o conjunto $\mathcal{M}$ contém as palavras $\varnothing$, 0, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111 etc. Dessa forma, se a e $b \in \mathcal{M}$ então $a = a_1a_2...a_m$, onde $a_i \in Y$ e $b = b_1b_2...b_m$, onde $b_j \in Y$ e o produto (concatenação) de a por b é $a.b = ab = a_1a_2...a_nb_1b_2..b_m$. Por exemplo, se $a = 01000$ e $b = 11111000$ então $ab = 0100011111000$.

Definição 2.2.2. *Sejam u,v* $\in \mathcal{M}$*. Dizemos que u é prefixo de v se v =uw para algum w* $\in \mathcal{M}$*.*

Exemplo 2.2.1. Considere a palavra $v = 01000$. Note que tomando $u = 01$ e $w = 000$, temos que u é um prefixo possível de v.

Definição 2.2.3 (Relação de Ordem)**.** *Sejam u,v* $\in \mathcal{M}$*. Dizemos que v* $\leq$ *u se, e somente, u é prefixo de v.*

Definição 2.2.4. *O comprimento de uma palavra v* $\in \mathcal{M}$ *(o número de letras) é denotado por /v/, onde /*$\varnothing$*/ = 0. A função comprimento / / : v* $\longrightarrow$ */v/ induz uma distância entre os elementos de* $\mathcal{M}$ *dada por:*

$$d(u,v) = /u/ + /v/ - 2/w/$$

onde w é o maior prefixo comum entre u e v.

Exemplo 2.2.2. Considere $u = 011011001$ e $v = 011001$. Temos que o maior prefixo comum entre u e v é $w = 0110$. Portanto $|u| = 9$, $|v| = 6$, $|w|$ =4 e $d(u, v) = |u| + |v| - 2|w| = 9 + 6 - 2.4 = 7$.

Definição 2.2.5 (Definição de Árvore Binária Enraizada)**.** $\mathcal{M}$ *com a relação de ordem (Definição 2.2.4) é uma árvore denotada por* $\mathcal{T}_2$*. Cada palavra v de* $\mathcal{M}$*, quando vista como elemento de* $\mathcal{T}_2$*, é um vértice.*

Observe a Figura 6. A árvore é composta por diferentes níveis que representam o tamanho dos vértices. Um vértice v no primeiro nível da árvore $\mathcal{T}_2$ é uma palavra de comprimento 1 no alfabeto $Y = \{0, 1\}$. Um vértice v no segundo nível é uma palavra de comprimento dois, e assim por diante. Além disso, o vértice que dá origem aos demais, é chamado de raiz da árvore e denotado por $\varnothing$.

Um automorfismo α de $\mathcal{T}_2$ é uma bijeção $\alpha : \mathcal{T}_2 \to \mathcal{T}_2$ que preserva a distância entre os vértices. Com a operação de composição de funções, o conjunto de todos os automorfismos de $\mathcal{T}_2$ é um grupo, denotado por $\mathcal{A}_2$. Note que um automorfismo α de $\mathcal{T}_2$ fixa a raiz $\varnothing$ e preserva a adjacência dos vértices.

Considere $\sigma = (01)$ a permutação que envia 0 em 1, e 1 em 0. Podemos estendê-la a um automorfismo $\bar{\sigma}$ de $\mathcal{T}_2$, pondo:

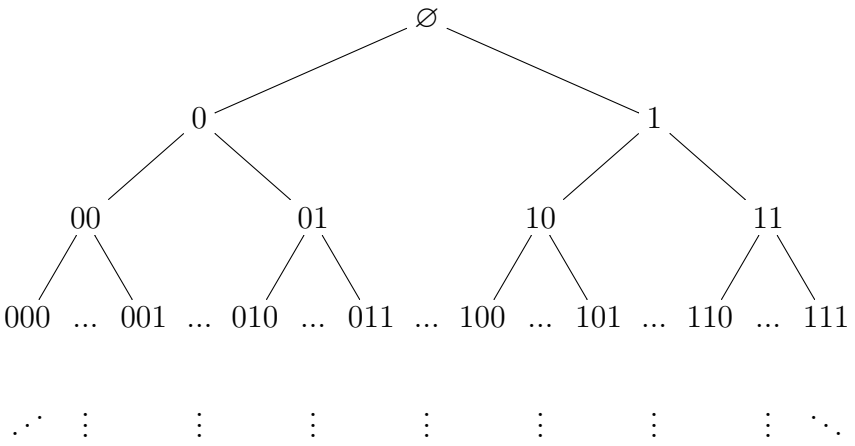

Figura 6 – Árvore Binária Enraizada $\mathcal{T}_2$

$$\bar{\sigma}(\varnothing) = \varnothing$$
$$\bar{\sigma}(yu) = \sigma(y)u$$

para todo $y \in Y$ e para todo $u \in \mathcal{T}_2$, note também que $yu \in \mathcal{T}_2$. Para simplificar a notação, vamos denotar a extensão $\bar{\sigma}$ de σ simplesmente por σ.

Por outro lado, dado um automorfismo α de $\mathcal{T}_2$, temos que α induz uma permutação $\sigma_\varnothing$ em Y. Basta considerar $\sigma_\varnothing$ igual a restrição α: $Y \to Y$. Agora, podemos considerar a extensão da permutação $\sigma_\varnothing$, para um automorfismo de $\mathcal{T}_2$. Logo a composição $\alpha(\sigma_\varnothing)^{-1}$ possui ação trivial no primeiro nível da árvore $\mathcal{T}_2$, ou seja, $\alpha(\sigma_\varnothing)^{-1}(y) = y$, para todo $y \in Y$. Chamemos $\alpha(\sigma_\varnothing)^{-1} = \alpha'$. Para cada $y \in Y$, α' induz sobre a subárvore $y.\mathcal{T}_2$ um automorfismo α_y. Considerando o isomorfismo $y.\mathcal{T}_2 \to \mathcal{T}_2$ podemos identificar $y.\mathcal{T}_2$ com $\mathcal{T}_2$ e assim *identificar* α_y como um elemento de $\mathcal{A}_2$.

Desta forma, podemos olhar para a composição $\alpha' = \alpha(\sigma_\varnothing)^{-1}$ como:

$$\alpha(\sigma_\varnothing)^{-1} = \alpha' = (\alpha_0, \alpha_1) \tag{2.1}$$

onde cada α_y, com $y = 0$ ou $y = 1$, é um automorfismo da árvore $\mathcal{T}_2$. Em outras palavras, $(\alpha_0, \alpha_1) \in (\mathcal{A}_2 \times \mathcal{A}_2)$. Da igualdade (2.1), concluímos que $\alpha = (\alpha_0, \alpha_1)\sigma_\varnothing$. Fazendo a mesma análise para α_0 e α_1 temos que $\alpha_0 = (\alpha_{00}, \alpha_{01})\sigma_0$ e $\alpha_1 = (\alpha_{10}, \alpha_{11})\sigma_1$, onde α_{00}, α_{01}, α_{10},α_{11} $\in \mathcal{A}_2$ e σ_0, $\sigma_1 \in S_2$ ($S_2 = S_y$, grupo cíclico de ordem 2). Então, $\mathcal{A}_2 \cong (\mathcal{A}_2 \times \mathcal{A}_2) \rtimes S_2$, onde S_2 age permutando as cópias de $\mathcal{A}_2$. Dessa forma, temos a função que dado um automorfismo de α e um elemento de Y, associa um outro automorfismo. Ou seja:

$$f : \mathcal{A}_2 \times Y \to \mathcal{A}_2$$
$$(\alpha, 0) \mapsto \alpha_0,$$
$$(\alpha, 1) \mapsto \alpha_1.$$

Temos também a função l:

$$l : \mathcal{A}_2 \times Y \to Y$$
$$(\alpha, 0) \mapsto \sigma_\varnothing(0),$$
$$(\alpha, 1) \mapsto \sigma_\varnothing(1).$$

Dito de uma maneira resumida, podemos ver o grupo de automorfismo da árvore binária como o produto semidireto $\mathcal{A}_2 \cong (\mathcal{A}_2 \times \mathcal{A}_2) \rtimes S_2$, usando o isomorfismo que associa α ao automorfismo $(\alpha_0, \alpha_1)\sigma_\varnothing$. Contudo, vamos simplificar a notação fazendo uma *identificação* de $\mathcal{A}_2$ com sua cópia isomorfa $(\mathcal{A}_2 \times \mathcal{A}_2) \rtimes S_2$ e escreveremos

$$\mathcal{A}_2 = (\mathcal{A}_2 \times \mathcal{A}_2) \rtimes S_2.$$

Usando esta identificação temos $\alpha = (\alpha_0, \alpha_1)\sigma_\varnothing$, onde a ação de α em $\mathcal{T}_2$ é dada por:

$$\alpha(yu) = \sigma_\phi(y)\alpha_y(u), \forall y \in Y, \forall u \in \mathcal{T}_2.$$

Exemplo 2.2.3. Tome $y = 1$ e $u = 01$, então $yu = 101$. Como $\alpha = (\alpha_0, \alpha_1)\sigma_\varnothing$, temos $\alpha(yu) = \sigma_\varnothing(1)\alpha_1(01)$. Se a palavra for 01001, então $\alpha(01001) = \sigma_\varnothing(0)\alpha_0(1001)$.

Em suma, podemos repetir para α_y o mesmo processo de descrição visto para α, assim $\alpha_y = (\alpha_{y0}, \alpha_{y1})\sigma_y$ e novamente repetimos esse processo para cada α_{yx}, onde $x \in Y$. Sucessivos desenvolvimentos produzem $\alpha_u = (\alpha_{ui})_{i \in Y}.\sigma_u$. Podemos então considerar o conjunto $Q(\alpha) = \{\alpha_u | u \in \mathcal{T}_2\}$. Os automorfismos α_u, $u \in \mathcal{T}_2$ são chamados de estados de α. Um estado α_u de α é dito ser ativo se $\sigma_u \neq e$, caso contrário, ele é denominado inativo. Observe que cada σ_u de α depende de α. Temos então a seguinte definição:

Definição 2.2.6. *Seja $\alpha = (\alpha_0, \alpha_1)\sigma_\varnothing$ um automorfismo de $\mathcal{T}_2$. O conjunto de estados de α é definido por:*

$$Q(\alpha) = \{\alpha_u \mid u \in \mathcal{T}_2\},$$

ou recursivamente por:

$$Q(\alpha) = \{\alpha, \alpha_0, \alpha_1\} \cup Q(\alpha_0) \cup Q(\alpha_1).$$

Um elemento $\alpha_u \in Q(\alpha)$ é chamado de estado de α. O conjunto $Q(\alpha)$ será melhor abordado mais adiante.

Exemplo 2.2.4. Seja $\beta = (e,\ e)\sigma$, onde $\sigma = (01)$. Observe que $\beta = (\beta_0,\ \beta_1)\sigma_\varnothing$, donde $\beta_0 = e$, $\beta_1 = e$ e $\sigma_\varnothing = \sigma$. Temos então que este automorfismo é considerado ativo. Além disso, $e = (e, e)$, e o conjunto dos estados de β podem ser representados por $Q(\beta) = \{\beta,\ \beta_0,\ \beta_1\} \cup Q(\beta_0) \cup Q(\beta_1) = \{\beta, e\}$.

Exemplo 2.2.5. Seja $\gamma = (\gamma,\ \beta)\sigma$, onde $\sigma = (01)$ e $\beta = (e,\ e)\sigma$ é o automorfismo do Exemplo 2.2.4. Usando a propriedade da Definição 2.2.6 temos que:

$$\mathrm{Q}(\gamma) = \{\gamma,\ \beta\} \cup \mathrm{Q}(\gamma) \cup Q(\beta) = \{\gamma, \beta, e\}.$$

Exemplo 2.2.6. Observe que pela descrição de $\beta = (\beta_0, \beta_1)\sigma_\varnothing = (e, e)\sigma$, onde $\beta_0 = e$, $\beta_1 = e$, $\sigma_\varnothing = \sigma$. Sendo $yu = 101$, onde $y = 1$, como no Exemplo 2.2.3, temos:

$$\beta(yu) = \sigma_\varnothing(y)\beta_y(u) = \sigma(1)\beta_1(01) = \sigma(1)e(01).$$

Para uma palavra $v = 01001$, temos:

$$\beta(01001) = \sigma_\varnothing(0)\beta_0(1001) = \sigma(0)e(1001).$$

Exemplo 2.2.7. Seja $\gamma_0 = (\gamma, \beta)\sigma$, onde $\gamma_0 = \gamma$, $\gamma_1 = \beta$ e $\sigma_\varnothing = \sigma$. Sendo $yu = 101$, Exemplo 2.2.3, temos:

$$\gamma(yu) = \gamma(101) = \sigma_\varnothing(1)\gamma_1(01) = \sigma(0)\beta(1001).$$

Já para a palavra $v = 01001$, temos:

$$\gamma(01001) = \sigma_\varnothing(0)\gamma_0(1001) = \sigma(0)\gamma(1001).$$

2.3 Autômatos

Os autômatos são máquinas de estados, que a partir de uma palavra em um alfabeto de entrada, geram uma palavra em um alfabeto de saída. Além disso, a cada estado percorrido uma saída é gerada, assim como definido o próximo estado. Por conta de suas características, os autômatos são extensivamente usados na ciência da computação.

As máquinas são utilizadas desde em sistemas complexos a casos mais simples, como um sistema de trocos em uma máquina de vendas. Neste caso, o autômato determinaria quais tipo de moedas são aceitas (alfabeto de entrada), as quantidades e possíveis trocos (alfabeto de saída). Para que uma máquina desse tipo funcionasse, também seria necessário se definir quais etapas subsequentes deveriam ser tomadas. Ou seja, escolher um conjunto de estados possíveis e uma aplicação parcial que determina a transição de

estados. Em outras palavras, se João quer comprar um refrigerante que custa 5 reais e insere uma nota de 10 reais, quais passos a máquina deveria tomar para computar o troco? Por último, devemos definir a aplicação parcial de saída, que é o resultado de cada leitura realizado pela máquina.

Um autômato é capaz de ler uma palavra binária finita, um caractere de cada vez, lendo da esquerda para a direita. O domínio de um autômato consistirá de palavras binárias finitas - não os números binários representados por essas palavras, mas a própria palavra. Por exemplo, a palavra 00 é uma palavra diferente da palavra 000. Começaremos listando de forma geral os requisitos de um autômato determinístico de finitos estados:

- Possui um número finito de estados.
- Um de seus estados é designado como seu estado inicial.
- Ele pode ler apenas um conjunto finito de caracteres definido, chamado alfabeto, um de cada vez.
- Suas palavras de entrada devem ter comprimento finito.
- Dado um estado e um caractere possível, um conjunto de instruções determina a resposta (esta é a parte determinística de seu nome).
- Ele pode ler que a palavra chegou ao fim, momento em que entra em seu estado inicial ou para.

Os estados ajudam a determinar como o autômato se comporta. A medida que a palavra é inserida no autômato, este é configurado em seu estado inicial (indicado em um diagrama por linhas tracejadas), e lê o primeiro caractere. Quando o autômato faz a leitura de um caractere, ele responde em duas maneiras: (1) imprime um caractere binário; e (2) entra em um novo estado. Em seguida, lê o próximo caractere da palavra e responde a ele. Quando o último caractere é lido, o autômato retorna ao seu estado inicial. Por fim termina de imprimir a saída associada a entrada dada. Observe que o comprimento da palavra de saída sempre é igual ao comprimento da palavra de entrada. Começaremos com uma máquina de funções extremamente simples, A_z, chamada de "autômato zero." A regra da função será: para qualquer caractere da palavra de entrada fornecida, será impresso o caractere 0.

Na Figura 7 o diagrama deste autômato é ilustrado. O círculo rotulado z representa o estado inicial (e único), e o 1|0 no topo instrui o autômato, para imprimir um 0 quando lê um 1, enquanto a seta direciona o autômato para retornar ao estado z. O 0|0 à direita instrui o autômato a imprimir um 0 quando lê um 0, enquanto a seta direciona o autômato novamente para retornar ao estado z.

Por exemplo, quando aplicamos a palavra 101 em A_z, movendo da esquerda para a direita, A_z lê 1 e retorna 0, lê o próximo caractere 0 e retorna 0, por fim lê 1 e retorna 0. Logo a palavra de saída é 000.

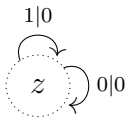

Figura 7 – Autômato zero A_z

Embora A_z sirva como um simples exemplo de autômato, a função produzida não nos é interessante porque não atua como uma "máquina de automorfismo". Neste contexto, estamos interessados em autômatos que representam máquinas de automorfismo; mais especificamente, estamos interessados nas "máquinas de automorfismo da árvore binária completa infinita".

Se queremos que nossos autômatos atuem como máquinas de automorfismo, suas regras codificadas devem produzir uma função que é uma bijeção cujo domínio é o mesmo que sua imagem, ou seja, as palavras que são saídas devem vir do mesmo conjunto das palavras que são permitidas como entrada. O autômato zero não produz uma bijeção, portanto não é um automorfismo. Após essa discussão introdutória, podemos definir formalmente os autômatos:

Definição 2.3.1. *Um autômato é uma sêxtupla A_q = (Q, Σ, Γ, f, l, q_0) onde:*

- *Q é um conjunto finito de estados;*
- *Σ é o alfabeto finito de entrada;*
- *Γ é o alfabeto finito de saída;*
- *f: $Q \times \Sigma \to Q$ é a aplicação parcial de transição de estados;*
- *l: $Q \times \Sigma \to \Gamma$ é a aplicação parcial de saída;*
- *q_0 é o estado denominado inicial.*

É importante lembrar, que no nosso caso $\Gamma = \Sigma = Y$.

Exemplo 2.3.1. Examinemos o automorfismo $\beta = (e, e)\sigma$. Este fora inicialmente apresentado no Exemplo 2.2.4.

$$f : Q \times Y \to Q$$
$$f(\beta, 0) = \beta_0 = e, f(\beta, 1) = \beta_1 = e,$$
$$f(e, 0) = e_0 = e, f(e, 1) = e_1 = e.$$

A função l é aplicação parcial de saída:

$$l : Q \times Y \to Y$$
$$l(\beta, 0) = \sigma_0 = 1, l(\beta, 1) = \sigma_1 = 0,$$
$$l(e, 0) = e_0 = 0, l(e, 1) = e_1 = 1.$$

O autômato β é representado na Figura 8.

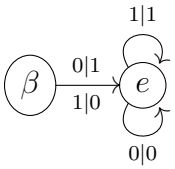

Figura 8 – Autômato $\beta = (e,\, e)\sigma$

Exemplo 2.3.2. Seja $\alpha = (\alpha,\, \beta)$. Como $\beta = (e,\, e)\sigma$. Logo o conjunto dos estados de α é $Q(\alpha) = \{\alpha, \beta, e\}$.

O alfabeto de entrada é $Y = \{0, 1\}$, já o alfabeto de saída também é Y. A função f, essa determina o estado seguinte dado o estado atual e a respectiva entrada:

$$f : Q \times Y \to Q$$
$$f(\alpha, 0) = \alpha_0 = \alpha, f(\alpha, 1) = \alpha_1 = \beta,$$
$$f(\beta, 0) = \beta_0 = e, f(\beta, 1) = \beta_1 = e,$$
$$f(e, 0) = e_0 = e, f(e, 1) = e_1 = e.$$

A função l é aplicação parcial de saída:

$$l : Q \times Y \to Y$$
$$l(\alpha, 0) = \sigma_0 = e_0 = 0, l(\alpha, 1) = \sigma_0 = e_1 = 1,$$
$$l(\beta, 0) = \sigma_0 = 1, l(\beta, 1) = \sigma_1 = 0,$$
$$l(e, 0) = e_0 = 0, l(e, 1) = e_0 = 1.$$

O autômato α é representado na Figura 9.

Exemplo 2.3.3. Seja $\tau = (e,\, \tau)\sigma$. Então, $\sigma_\phi = \sigma$, $\tau_0 = e$, por último, $\tau_1 = \tau$.

O alfabeto de entrada é $Y = \{0, 1\}$. De igual modo, o alfabeto de saída Y é {0,1}. Além disso, o conjunto de estados é $Q = \{e, \tau\}$. Observemos agora a função f, essa determina o estado seguinte dado o estado atual e a respectiva entrada:

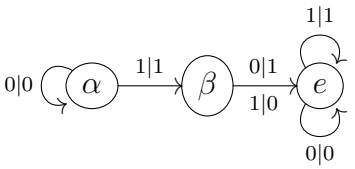

Figura 9 – Autômato $\alpha = (\alpha, \beta)$

$$f : Q \times Y \to Q$$
$$f(\tau, 0) = \tau_0 = e, f(\tau, 1) = \tau_1 = \tau.$$

Por sua vez, a função l é aplicação parcial de saída:

$$l : Q \times Y \to Y$$
$$l(\tau, 0) = \sigma(0) = 1, l(\tau, 1) = \sigma(1) = 0$$

Observe que essa retorna apenas zero ou um.

Considere agora $u = 101$ e $v = 01001$. Apliquemos τ a essas palavras:

$$\tau(u) = \tau(101) = \sigma(1)\tau(01) = 0\sigma(0)e(1) = 011$$
$$\tau(v) = \tau(01001) = \sigma(0)e(1001) = 11001.$$

Note que ao aplicarmos τ sobre uma palavra qualquer, obtemos um resultado idêntico a adicionar 1 à esquerda módulo 2. Por isso, o autômato τ também é conhecido como a máquina de adição binária.

Proposição 2.3.1. *Sendo τ = (e,τ)σ , onde $\sigma = (01)$. Então $\tau^\theta \neq (e, e)$, para todo θ inteiro não nulo.*

Demonstração. Podemos decompor esse problema em dois casos, a depender da paridade do expoente. Se θ é ímpar, este pode ser escrito na forma $\theta = 2n + 1$, com $n \geq 0$ e $n \in \mathbb{N}$. Desse modo, $\tau^\theta = \tau^{2n+1} = (\tau^n,\tau^{n+1})\sigma$ e claramente $\tau^\theta \neq (e, e)$.

De modo semelhante, para um θ par, podemos escrever $\theta = 2n$. Então, $\tau^\theta = \tau^{2n}$ $= (\tau^n,\tau^n)$, com $n \geq 1$ e $n \in \mathbb{N}$. Para $n = 1$, temos que $\tau^2 = (\tau,\tau)$. Como $\tau = (e, \tau)$ $\sigma \neq$ (e, e), segue que $\tau^2 = (\tau,\tau) \neq (e, e)$. Suponha agora que para $\forall n \in \mathbb{N}$, com $1 \leq n \leq k$, a expressão $\tau^{2n} = (\tau^n,\tau^n) \neq (e, e)$ seja válida. Sendo assim, para $n = k+1$, temos que $\tau^{2(k+1)}$ $= (\tau^{k+1},\tau^{k+1}) = (\tau^k,\tau^k)\cdot(\tau,\tau) = \tau^{2k}\cdot\tau^2$. Segue que $\tau^{2(k+1)} = (e, e)$, se e somente se, τ^2 é o inverso de τ^{2k} para qualquer valor de n, com $1 \leq n \leq k$. Isso ocorre quando $\tau^2 = \tau^{2k}$ $= (e, e)$, mas por hipótese, $\tau^{2k} = (\tau^k,\tau^k) \neq (e, e)$. Logo $\tau^{2(k+1)} \neq (e, e)$ e $\tau^{2n} = (\tau^n,\tau^n)$ $\neq (e, e)$, para $\forall n \in \mathbb{N}$. Esse autômato é representado na Figura 10.

□

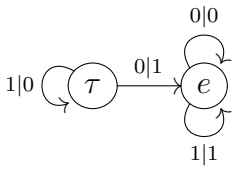

Figura 10 – Autômato $\tau = (e,\tau)\sigma$

Exemplo 2.3.4. Seja $\alpha = (\alpha^{-1}, \alpha^2)\sigma$. Então $\alpha^{-1} = (\alpha^{-2}, \alpha)\sigma$, $\alpha^2 = (\alpha, \alpha)$ e $\alpha^{-2} = (\alpha^{-1}, \alpha^{-1})$.

O alfabeto de entrada é $Y = \{0, 1\}$. De igual modo, o alfabeto de saída é $Y = \{0, 1\}$. O conjunto de estados de α é $Q(\alpha) = \{\alpha^n |\ n = -1, -2, 1, 2\}$. A função f que determina a aplicação parcial de transição de estados é:

$$f : Q \times Y \to Q$$
$$f(\alpha, 0) = \alpha_0 = \alpha^{-1}, f(\alpha, 1) = \alpha_1 = \alpha^2$$
$$f(\alpha^2, 0) = \alpha_0^2 = \alpha, f(\alpha^2, 1) = \alpha_1^2 = \alpha$$
$$f(\alpha^{-1}, 0) = \alpha_0^{-1} = \alpha, f(\alpha^{-1}, 1) = \alpha_1^{-1} = \alpha^{-2}$$
$$f(\alpha^{-2}, 0) = \alpha_0^{-2} = \alpha^{-1}, f(\alpha^{-2}, 1) = \alpha_1^{-2} = \alpha^{-1}$$

A função l é aplicação parcial de saída é dada por:

$$l : Q \times Y \to Y$$
$$l(\alpha, 0) = \sigma_0 = 1, l(\alpha, 1) = \sigma_1 = 0$$
$$l(\alpha^2, 0) = e_0 = 0, l(\alpha^2, 1) = e_1 = 1$$
$$l(\alpha^{-1}, 0) = \sigma_0 = 1, l(\alpha^{-1}, 1) = \sigma_1 = 0$$
$$l(\alpha^{-2}, 0) = e_0 = 0, l(\alpha^{-2}, 1) = e_1 = 1$$

As aplicações f e l podem ser escritas de maneira sucinta pelo autômato representado na Figura 11:

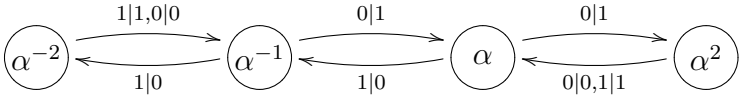

Figura 11 – Autômato $\alpha = (\alpha^{-1}, \alpha^2)\sigma$

A partir daqui iremos omitir as aplicações f e l, uma vez que o autômato as descreve completamente.

Exemplo 2.3.5. Seja $\alpha = (\alpha, \alpha^2)\sigma$. Então $\alpha^2 = (\alpha^3, \alpha^3)$, e:

$$\alpha^{2n} = (\alpha^{3n}, \alpha^{3n}),\ \alpha^{2n+1} = (\alpha^{3n+1}, \alpha^{3n+2})\sigma$$

O alfabeto de entrada é $Y = \{0, 1\}$. De igual modo, o alfabeto de saída é Y que é {0,1}. O conjunto de estados de α é $Q(\alpha) = \{\alpha^n |\ n = 1, 2, 3...\}$. Portanto, α possui infinitos estados. A Figura 12 ilustra esse autômato:

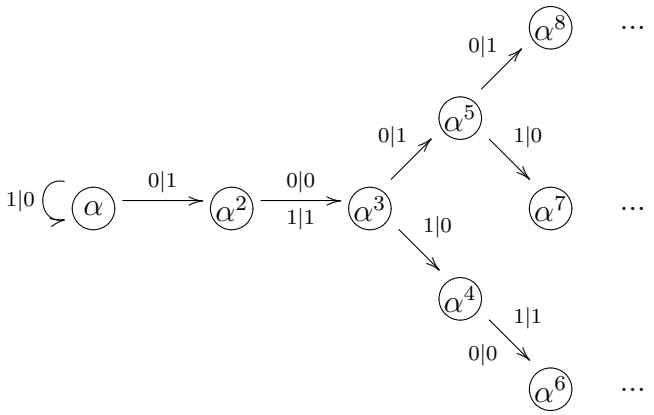

Figura 12 – Autômato $\alpha = (\alpha, \alpha^2)\sigma$

3 Grupo Lamplighter

Figura 13 – Acendedor de lampiões Bartone [6]

Lá vem o acendedor de lampiões da rua!
Este mesmo que vem infatigavelmente,
Parodiar o sol e associar-se à lua
Quando a sombra da noite enegrece o poente!
Um, dois, três lampiões, acende e continua
Outros mais a acender imperturbavelmente,
À medida que a noite aos poucos se acentua
E a palidez da lua apenas se pressente.
Triste ironia atroz que o senso humano irrita:
— Ele que doira a noite e ilumina a cidade,
Talvez não tenha luz na choupana em que habita.
Tanta gente também nos outros insinua
Crenças, religiões, amor, felicidade,
Como este acendedor de lampiões da rua!
Jorge de Lima [12]

Grupo Lamplighter

A primeira aparição do grupo $L_2 = (\bigoplus_{\mathbb{Z}} \mathbb{Z}_2) \rtimes \mathbb{Z}$ com o nome *Lamplighter* (acendedor de lampiões) ocorreu em 1983 em um artigo de Kaimanovich e Vershik, apesar de que o grupo já era conhecido desde muito antes, dado que ele é uma construção simples de um produto semidireto. Os grupos do tipo *Lamplighter* se relacionam com problemas matemáticos importantes como a conjectura de Atiyah, sendo suas representações foco de estudo, ver Dantas [4].

Uma das descrições do grupo *Lamplighter* é como um sistema dinâmico consistindo em configurações de uma rua bi-infinita (infinita para ambos os lados). Nessa rua há um número infinito de lâmpadas, onde apenas um número finito delas se encontram ligadas, e um acendedor de lâmpadas (*Lamplighter*) que é capaz de alterar a configuração [3].

Entretanto, o grupo *Lamplighter* L_2 pode ser descrito de diferentes maneiras. Além da representação como sistema dinâmico, o grupo L_2, pode ser descrito por meio da soma direta infinita ou, como será visto mais adiante, um grupo gerado por um autômato de dois estados, como mostrado por Grigorchuk e Zük [2].

Um sistema dinâmico é um objeto associado a um conjunto específico de modificações que podem ser performadas (dinamicamente) sobre este objeto. No caso do grupo *Lamplighter*, o objeto é uma rua em linha reta bi-infinita com um poste de luz a cada esquina de rua. Duas modificações são possíveis: o acendedor de lâmpadas pode caminhar qualquer distância em ambas as direções de um ponto de partida, além disso o acendedor de lâmpadas pode ligar ou desligar as lâmpadas dos postes. Em um dado momento o acendedor de lâmpadas está em um poste de luz em particular e um número finito de lâmpadas está aceso, enquanto as outras estão apagadas. Nos referimos a este momento como *configuração* da rua. Dito de maneira informal, é o "estado" (não confundir tal definição com o estado de um autômato). A *configuração* da rua se altera com o tempo, a medida que o acendedor de lâmpadas está caminhando para um poste de luz diferente, acendendo ou apagando uma lâmpada.

Na Figura 14, a rua bi-infinita será representada por uma linha numerada, as lâmpadas são indexadas por números inteiros. Postes com lâmpadas acesas serão indicadas por estrelas, já as apagadas por círculos. A posição do acendedor de lâmpadas será indicada por uma seta apontando para um inteiro. O estado corrente de uma rua será chamado de *Lampstand*.

O conjunto de todos os possíveis *Lampstands* será chamado de $\mathscr{L}$. Formalizaremos agora a dinâmica da mudança de uma lâmpada especificando tarefas distintas que o acendedor de lâmpadas pode performar em cada elemento de $\mathscr{L}$.

1. δ: Mover a direita para próxima lâmpada.

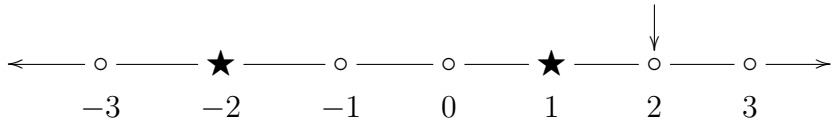

Figura 14 – *Lampstand* com duas lâmpadas acesas, o acendedor de lâmpadas está na posição 2

2. δ^{-1}: Mover a esquerda para próxima lâmpada.

3. σ: Mudar a configuração atual de cada lâmpada (acender ou apagar).

4. I: Não fazer nada.

Para qualquer configuração, o acendedor de lâmpadas realiza apenas um número finito de ações. Essas tarefas podem ser interpretadas como funções δ, σ, e I, cujo domínio e alcance são $\mathscr{L}$. Dado um *lampstand* $l \in \mathscr{L}$, $\delta(l)$ é o resultado de se realizar a primeira tarefa sobre l, $\sigma(l)$ é o resultado de se realizar a terceira tarefa em l, e $I(l)$ é o resultado de se realizar a quarta tarefa em l.

Proposição 3.0.1. *A função σ que muda a configuração atual de cada lâmpada (acende ou apaga) é uma função bijetiva.*

Demonstração. Para mostrar a sobrejetividade de σ, considere que l_1 seja qualquer *Lampstand* em $\mathscr{L}$, além disso suponha que o acendedor de lâmpadas esteja em poste de luz indexado por k. Defina l_0 como o *Lampstand* cujo acendedor de lâmpada está na lâmpada k e cujas lâmpadas estão na mesma configuração de l_1, exceto pela lâmpada k. Se k esta acesa em l_1, então está desligada em l_0; se está apagada em l_1, então está acesa em l_0. Então $\sigma(l_0) = l_1$.

A injetividade é perceptível ao supor que $\sigma(l_0) = \sigma(c_0) = l_1$, com o acendedor de lâmpadas em l_1 ficando na lâmpada k. Como σ não causa o movimento do acendedor de lâmpadas, o único efeito que ele causa em um *Lampstand* é a mudança de estado da lâmpada atual. Quaisquer que seja o estado da lâmpada k em l_1, este deve ser o oposto do estado em ambos l_0 e c_0. Todos as outras configurações de l_0 e c_0 devem ser iguais as outras configurações de l_1; então, $l_0 = c_0$. □

Se o acendedor de lâmpada está em 0 com todas as lâmpadas desligadas, essa configuração é chamada de *Lampstand* vazio e é denotado por e. (Figura 15)

Exemplo 3.0.1. Considere o *Lampstand* l_1 conforme a Figura 16 Iniciando com o estado e, aplicamos uma composição de funções δ, δ^{-1}, σ, e I para se atingir l_1.

Por exemplo, a composição $\delta\sigma\delta\delta\sigma\delta^{-1}$ ou $(\delta \circ \sigma \circ \delta \circ \delta \circ \sigma \circ \delta^{-1})$ aplicada a e leva a configuração do *Lampstand* para l_1. Mantendo-se a notação padrão para funções, a ordem

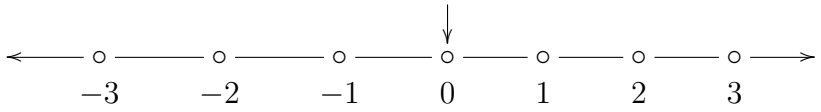

Figura 15 – *Lampstand* vazio

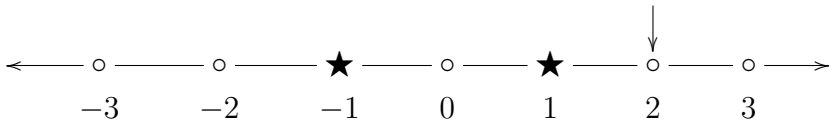

Figura 16 – Lampstand l_1

da composição é tal que δ^{-1} é aplicado e assim por diante, lendo da esquerda para a direita. A Figura 17 mostra detalhes da transformação de e em l_1.

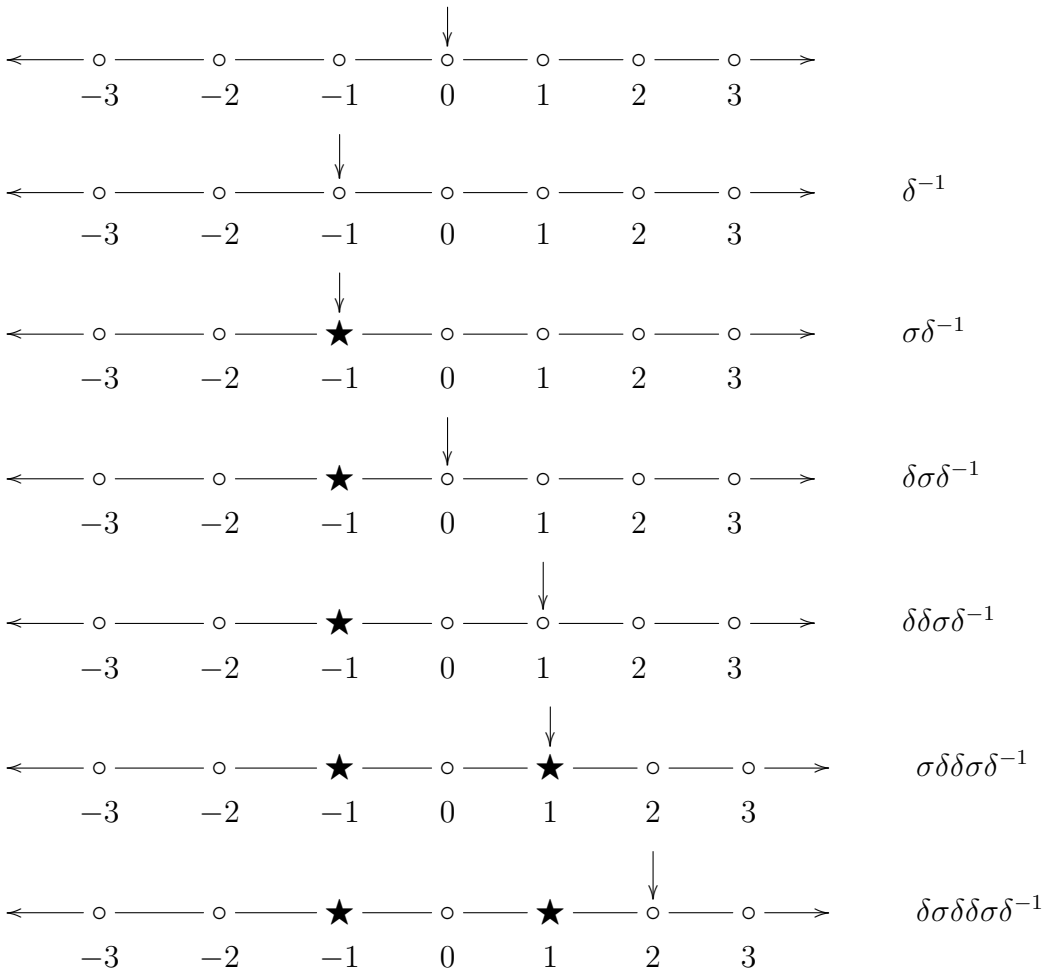

Figura 17 – Uma sequência de *Lampstands* até l_1

Para conseguir o mesmo *Lampstand* l_1, poderíamos aplicar uma função composta diferente a e, por exemplo:

$$\delta I \delta \delta I \sigma \delta^{-1} \delta^{-1} \sigma \delta.$$

Para a escolha de qualquer $l \in \mathscr{L}$ como entrada. Essas duas funções sempre terão a mesma saída:

$$\delta\sigma\delta\delta\sigma\delta^{-1}(\mathrm{l}) = \delta I\delta\delta I\sigma\delta^{-1}\delta^{-1}\sigma\delta(\mathrm{l}).$$

Não importa se há duas composições de funções representando o mesmo *Lampstand*, desde que as duas funções são definidas como a mesma função enquanto os domínios são o mesmo e as saídas são iguais. Entretanto, algumas composições de funções claramente possuem um número menor de tarefas.

Proposição 3.0.2. *O grupo L_2 (Lamplighter) é formado por elementos que representam configurações particulares da rua, um elemento de $\mathscr{L}$.*

Entretanto, os *Lampstands* podem ser identificados, bijetivamente, como o conjunto de todas as composições de funções de σ, δ e δ^{-1}, aplicadas sobre o *Lampstand* vazio (e). Além disso, $\delta(e)$ é identificado com δ, e $\sigma(e)$ é identificado com σ. A identidade é definida como $I(e)$, que poderá nesse texto ser simplificada para apenas e. A multiplicação deste grupo é a operação de composição de funções, que é bem definida dado a bijetividade das funções. Verificar a associatividade é recorrente. A Figura 18 representa as diferentes composições.

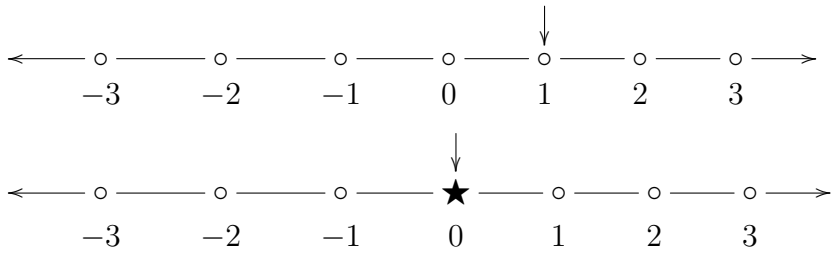

Figura 18 – Os *Lampstands* $\delta(e)$ (acima) e $\sigma(e)$ (abaixo)

L_2 é um exemplo de grupo finitamente gerado, mas não finitamente apresentado. A ordem de σ é dois, pois acender/desligar ou desligar/acender a lâmpada não altera a configuração inicial do *Lampstand*. Já δ possui ordem infinita, uma sequência de movimentos a direita é incapaz de conduzir a configuração inicial de um *Lampstand*. Lembre-se que $[\sigma^{\delta^i}, \sigma^{\delta^j}]$ é o comutador entre σ^{δ^i} e σ^{δ^j}, com $\sigma^{\delta^i} = \delta^{-i}\sigma\delta^i$ e $\sigma^{\delta^j} = \delta^{-j}\sigma\delta^j$. Além disso, a ordem de qualquer conjugado σ^{δ^i} é dois, pois:

$$\sigma^{\delta^i}\sigma^{\delta^i} = \delta^{-i}\sigma\delta^i\delta^{-i}\sigma\delta^i = \delta^{-i}\sigma\sigma\delta^i = \delta^{-i}\sigma^2\delta^i = \delta^{-i}e\delta^i = \delta^{-i}\delta^i = e.$$

Definição 3.0.1. *A apresentação de L_2 é:*

$$L_2 = \langle\ \sigma,\ \delta\ /\ \sigma^2 = 1,\ [\sigma^{\delta^i},\ \sigma^{\delta^j}\ ]\ (i, j \in \mathbb{Z})\ \rangle.$$

Além disso, é possível mostrar que o comutador $[\sigma^{\delta^i},\ \sigma^{\delta^j}\ ]$ $(i, j \in \mathbb{Z})$ pode ser obtido de $[\sigma,\ \sigma^{\delta^j}\ ]$ $(j \in \mathbb{Z})$. Da relação $\sigma^2 = 1$, conseguimos encontrar outras relações úteis:

$$(\sigma^{\delta^i})^2 = (\delta^{-i}\sigma\delta^i)(\delta^{-i}\sigma\delta^i) = (\delta^{-i}\sigma\sigma\delta^i) = (\delta^{-i}\delta^i) = e.$$

Sendo assim, podemos reescrever a apresentação de L_2 na seguinte forma:

$$L_2 = \langle\ \sigma,\ \delta \mid \sigma^2 = 1,\ [\sigma,\ \sigma^{\delta^j}\ ]\ (i, j \in \mathbb{Z})\ \rangle.$$

O grupo *Lamplighter* L_2 também pode ser representado como um par ordenado. A primeira entrada representa a localização do acendedor de lâmpadas e a segunda entrada se utiliza de uma construção a partir de uma soma infinita para indicar quais lâmpadas estão acesas. Desse modo, podemos descrever de forma consistente uma configuração particular de um *Lampstand*. Os elementos de L_2 podem ser representados por:

$$\{(n, \overrightarrow{x}) \mid n \in \mathbb{Z},\ \overrightarrow{x} \in \bigoplus_{i\in\mathbb{Z}}(\mathbb{Z}_2)\}$$

Os $\overrightarrow{x}$ são infinitas sequências cujas entradas são associados valores 0 ou 1. A partir dessa perspectiva é mais fácil visualizar o L_2 sendo $(\bigoplus_{\mathbb{Z}}\mathbb{Z}_2) \rtimes \mathbb{Z}$, como indicado no exemplo 1.8.4.

4 Classificação de Autômatos de dois estados sobre o alfabeto {0,1}

Existe interesse de lógicos e cientistas da computação em grupos de autômatos, dado que eles são importantes para a resolução de problemas complexos. Esses, por sua vez, demandam ricos conhecimentos matemáticos e intrigam pesquisadores ao redor do mundo. Os problemas de classificação estão presentes em várias áreas da matemática, podendo ser considerados dentre os principais. Se os objetos podem ser expressados como uma combinação, então é normal tentar classificá-los primeiro por classes e depois em subclasses.

Um parâmetro que pode ser utilizado para este fim é o par (m, n), onde m é o número de estados de um autômato gerando um grupo e n é a cardinalidade do alfabeto. Esse parâmetro foi o utilizado por Grigorchuk *et al.* [11], para a classificação de grupos gerados por autômatos de 3 estados no alfabeto de duas letras. Este capítulo se dedica a análise de grupos gerados por autômatos de um e dois estados com o alfabeto de duas letras, ou seja, os pares $(1, 2)$ e $(2, 2)$.

Vamos analisar, inicialmente, o par (1,2), ou seja, mostraremos que para o alfabeto binário {0,1}, o autômato com um e apenas um estado produz o grupo trivial ou o grupo cíclico de ordem dois.

Demonstração. Seja a o único estado do autômato, então $a = (a, a)$ ou $a = (a, a)\sigma$. Seja w uma palavra sobre o alfabeto Y. Se $a = (a, a)$, então $a(0w) = 0a(w)$ e $a(1w) = 1a(w)$, de onde temos que a é o automorfismo identidade. Seu autômato a é representado na Figura 19 e o grupo gerado é o trivial.

Figura 19 – Autômato gerando o grupo Trivial

Por outro lado, se $a = (a, a)\sigma$, então:

$$a^2 = (a, a)\sigma \cdot (a, a)\sigma = (a^2, a^2) \tag{4.1}$$

Logo $a^2 = (a^2, a^2)$ e pelo caso anterior um tal automorfismo é o identidade. Como a não é trivial ($a(0) = 1$), temos que $a = (a, a)\sigma$ tem ordem dois e portanto $\langle a \rangle = \mathbb{Z}_2$. Nesse último caso o autômato $a = (a, a)\sigma$ é mostrado na Figura 20.

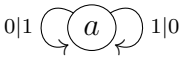

Figura 20 – Autômato gerando o grupo Cíclico de ordem dois

4.1 Resultado Principal

Vamos analisar agora os casos em que a e b são os dois estados do autômato. Para facilitar a compreensão do leitor, esta demonstração se dividirá em três partes. A primeira examinará o caso em que a e b são inativos, a segunda parte considerará que a e b são ativos e a última que a é inativo e b é ativo.

Inicialmente suponha que a e b sejam inativos, ou seja, quando aplicados em uma palavra não ocasionem a permutação 0 por 1 ou 1 por 0. Sendo assim, é possível supor que:

$$a = (a_0, a_1) \text{ e } b = (b_0, b_1), \text{ onde}$$
$$a_0 = a \text{ ou } b$$
$$a_1 = a \text{ ou } b$$
$$b_0 = a \text{ ou } b$$
$$b_1 = a \text{ ou } b$$

Além disso, ao aplicarmos qualquer combinação dos estados a e b em uma palavra, percebemos que essa não é alterada:

$$a(0w) = 0a_0(w)$$
$$a(1w) = 1a_1(w)$$
$$b(0w) = 0b_0(w)$$
$$b(1w) = 1b_1(w)$$

Esse processo poderia continuar invariavelmente a depender do comprimento da palavra w, sempre se recaindo em um dos casos básicos. Portanto, a é o automorfismo identidade. Pela mesma análise, concluímos também que b é a identidade. O grupo gerado nas condições descritas é o trivial.

Suponha agora que ambos a e b sejam ativos. Neste caso, a ação de a ou b na palavra causa a permutação de 1 por 0 ou 0 por 1. Sendo assim, é possível supor que:

$$a = (a_0, a_1)\sigma \text{ e } b = (b_0, b_1)\sigma, \text{ onde}$$
$$a_0 = a \text{ ou } b$$
$$a_1 = a \text{ ou } b$$

$$b_0 = a \text{ ou } b$$

$$b_1 = a \text{ ou } b.$$

Vamos mostrar que a e b nessas condições coincidem com o automorfismo $\theta = (\theta, \theta)\sigma$ (autômato equivalente ao apresentado na Figura 20). Procederemos por indução sobre o comprimento de uma palavra w qualquer. Se $|w| = 1$, $w = 0$ ou $w = 1$. Observe o conjunto de equações a seguir:

$$a(0) = \sigma(0) = 1 = \theta(0)$$

$$a(1) = \sigma(1) = 0 = \theta(1)$$

$$b(0) = \sigma(0) = 1 = \theta(0)$$

$$b(1) = \sigma(1) = 0 = \theta(1)$$

Logo $a(w) = \theta(w) = b(w)$ para toda palavra w de comprimento 1. Suponha agora que $a(w) = \theta(w) = b(w)$ vale para toda palavra w de comprimento n, inteiro positivo. Tome uma palavra u de comprimento $n + 1$. Então $u = w0$ ou $u = w1$ para alguma palavra w tal que $|w| = n$. Se $u = w0$:

$$a(u) = a(w0) = a(w)a_w(0) \overset{hip.ind}{=} \theta(w)a_w(0) = \theta(w)\sigma(0) \overset{eq1}{=} \theta(w)\theta_w(0) = \theta(w0) = \theta(u)$$
$$b(u) = b(w0) = b(w)b_w(0) \overset{hip.ind}{=} \theta(w)b_w(0) = \theta(w)\sigma(0) \overset{eq1}{=} \theta(w)\theta_w(0) = \theta(w0) = \theta(u).$$

Por outro lado se $u = w1$:

$$a(u) = a(w1) = a(w)a_w(1) \overset{hip.ind}{=} \theta(w)a_w(1) = \theta(w)\sigma(1) \overset{eq1}{=} \theta(w)\theta_w(1) = \theta(w1) = \theta(u)$$
$$b(u) = b(w1) = b(w)b_w(1) \overset{hip.ind}{=} \theta(w)b_w(1) = \theta(w)\sigma(1) \overset{eq1}{=} \theta(w)\theta_w(1) = \theta(w1) = \theta(u).$$

Concluímos que $a = \theta = b$. Como $\theta \neq e$, e:

$$\theta^2 = (\theta^2, \theta^2) = e. \tag{4.2}$$

Temos que a ordem de θ é dois e o grupo gerado por a e b é o cíclico de ordem dois ($\mathbb{Z}_2$).

Por fim, analisaremos os casos aonde um dos estados, digamos a, é inativo e o outro estado, digamos b, é ativo.

Com essa restrição temos que as possibilidades de a são: $a = (a, a)$, $a = (b, b)$, $a = (a, b)$ ou $a = (b, a)$. E b pode assumir: $b = (b, b)\sigma$, $b = (a, b)\sigma$, $b = (a, a)\sigma$ ou $b = (b, a)\sigma$.

i. Suponha inicialmente que $a = (a, a)$. Neste caso como já demonstrado, a corresponde à identidade do grupo.

- Se $b = (b, b)\sigma$. Conforme já demonstrado na Equação (4.2), $b = \theta$.
  Os estados $a = (a, a)$ e $a^2 = (a^2, a^2)$ são equivalentes. Decorre que a é trivial e b tem ordem dois. Podemos concluir que $G = \langle a, b\rangle = \langle b\rangle \cong \mathbb{Z}_2$, conforme a Figura 21.

Figura 21 – Autômatos gerando o grupo Cíclico de Ordem dois

- Se $b = (a, b)\sigma$
  Podemos construir o autômato para esse conjunto de estados, $Q(a) = \{a\}$ e $Q(b) = \{a, b\}$. O autômato construído é idêntico ao ilustrado na Figura 22. Repare que esse autômato é a máquina de adição binária. Como já demonstrado, o autômato $\tau = (e, \tau)\sigma$ de dois estados possui um elemento de ordem infinita, neste caso representado por b, e um elemento identidade, neste caso representado por a.

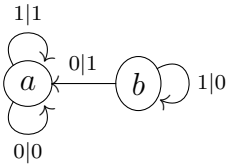

Figura 22 – Autômato representativo para $b = (e, b)\sigma$

  Dessa forma, temos que $G = \langle a, b\rangle = \langle b\rangle \cong \mathbb{Z}$, ou seja, G é o grupo cíclico infinito.

- Se $b = (a, a)\sigma$
  Temos que $a = e$ e :

  $bb = b^2 = (a, a)\sigma \cdot (a, a)\sigma = (a, a) \cdot (a, a)\sigma^2 = (a, a) \cdot (a, a) = (a^2, a^2) = e.$

  Temos então que $a = b^2 = e$. Dessa forma, podemos concluir que $G = \langle a, b\rangle = \langle b\rangle \cong \mathbb{Z}_2$.

- Se $b = (b, a)\sigma$, como $a = e$, $b = (b, e)\sigma$
  Temos que $b^2 \neq e$, pois:

  $bb = b^2 = (b, a)\sigma \cdot (b, a)\sigma = (b, a) \cdot (a, b)\sigma^2 = (ba, ab)$
  $ab = (a, a) \cdot (b, a)\sigma = (ab, a^2)\sigma$
  $ba = (b, a)\sigma \cdot (a, a) = (b, a) \cdot (a, a)\sigma = (ba, a^2)\sigma.$

  Observe que a estrutura do autômato identificado na Figura 23 é bastante semelhante a apresentada anteriormente na Figura 22 para o caso da máquina

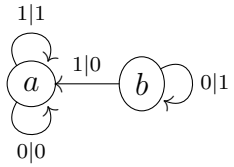

Figura 23 – Autômato representativo para $b = (b, e)\sigma$

de adição binária: $a = (a, a)$ e $b = (a, b)\sigma$. De fato, se trocarmos 0 por 1 no alfabeto, temos a máquina binária: $\tau = (\tau, e)\sigma$. Onde a é a identidade e b representa τ. Logo, com uma análise análoga é possível concluir que $G = \langle a, b\rangle = \langle b\rangle \cong \mathbb{Z}$.

ii. $a = (b, b)$

Como no caso anterior, para $a = (b, b)$, possuímos quatro possibilidades de b: $b = (a, a)\sigma$, $b = (b, b)\sigma$, $b = (a, b)\sigma$ ou $b = (b, a)\sigma$.

- Se $b = (a, a)\sigma$

  Temos que:

  $ab = (b, b) \cdot (a, a)\sigma = (ba, ba)\sigma$
  $aa = a^2 = (b, b) \cdot (b, b) = (b^2, b^2)$
  $ba = (a, a)\sigma \cdot (b, b) = (a, a) \cdot (b, b)\sigma = (ab, ab)\sigma$
  $bb = b^2 = (a, a)\sigma \cdot (a, a)\sigma = (a, a) \cdot (a, a)\sigma^2 = (a, a) \cdot (a, a) = (a^2, a^2)$.

  Concluímos que:

  $$a^2 = b^2 = e. \tag{4.3}$$

  Assim como:

  $$ab = ba \neq a. \tag{4.4}$$

  Note na Figura 24 que a ordem dos elementos a e b são ambas iguais a dois.

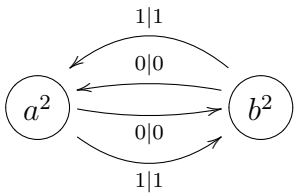

Figura 24 – Autômato $b^2 = (a^2, a^2)$

E pela análise do autômato $ab = (ba, ba)\sigma$, Figura 25, temos que $ab = ba$.

As Equações 4.3 e 4.4 obtidas mostram que o grupo G gerado por esse autômato de dois estados é comutativo e possui quatro elementos (e, a, b, ab). Dessa forma, concluímos que $G = \langle a, b\rangle \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$, ou seja, G é isomorfo ao grupo de *Klein*. Esse grupo fora previamente abordado no Exemplo 1.8.2.

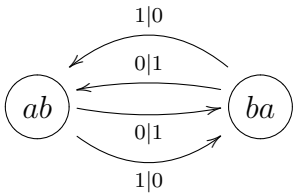

Figura 25 – Autômato $ab = (ba, ba)\sigma$

- $b = (b, b)\sigma$

  $aa = a^2 = (b, b) \cdot (b, b) = (b^2, b^2) = e$
  $bb = b^2 = (b, b)\sigma \cdot (b, b)\sigma = (b, b) \cdot (b, b)\sigma^2 = (b, b) \cdot (b, b) = (b^2, b^2) = e$
  $ab = (b, b) \cdot (b, b)\sigma = (b^2, b^2)\sigma$
  $ba = (b, b)\sigma \cdot (b, b) = (b, b) \cdot (b, b)\sigma = (b^2, b^2)\sigma$

  Através dessas expressões concluímos que a e b têm ordem dois:

  $$a^2 = b^2 = e. \tag{4.5}$$

  Além disso, o grupo G é abeliano pois:

  $$ab = (b^2, b^2)\sigma = ba. \tag{4.6}$$

  Observando as Equações 4.5 e 4.6, constatamos que G é isomorfo ao grupo de *Klein*, ou seja $G = \langle a, b\rangle \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

- $b = (a, b)\sigma$

  Temos que:

  $ab = (b, b) \cdot (a, b)\sigma = (ba, b^2)\sigma$ (Eq1)
  $ba = (a, b)\sigma \cdot (b, b) = (a, b) \cdot (b, b)\sigma = (ab, b^2)\sigma$ (Eq2)
  $bb = b^2 = (a, b)\sigma \cdot (a, b)\sigma = (a, b) \cdot (b, a)\sigma^2 = (a, b) \cdot (b, a) = (ab, ba)$
  $b^2a = (ab, ba) \cdot (b, b) = (ab^2, bab)$

  De onde:

  $$ab = (ba, b^2)\sigma \overset{Eq1}{=} ((ab, b^2)\sigma, b^2)\sigma \tag{4.7}$$

  e

  $$ba = (ab, b^2)\sigma \overset{Eq2}{=} ((ba, b^2)\sigma, b^2)\sigma. \tag{4.8}$$

  Pelas Equações 4.7 e 4.8 temos que: $ab = ba$ (como indicado no autômato da Figura 26). Portanto G é abeliano .
  Observe que $b^2a = e$, pois $b^2a = (b^2a, b^2a)$ devido a comutatividade (Figura 27). Logo $b^2 = a^{-1}$ e o grupo gerado é cíclico. Sendo assim, $G = \langle a, b\rangle = \langle b\rangle$.

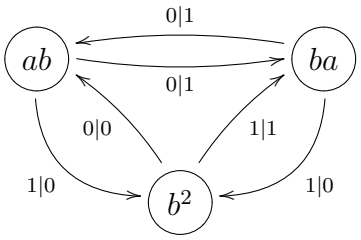

Figura 26 – Autômato $ab = (ba, b^2)\sigma = (ab, b^2)\sigma = ba$

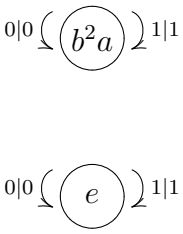

Figura 27 – Autômato b^2a e o autômato identidade são iguais

Por fim, suponha que n seja a ordem de a. Logo:

$a^n = e$

$a^{-n} = e^{-1} = e$

$a^{-n} = (a^{-1})^n = e$

$b^{2n} = a^{-n} = e$

Segundo essa relação, a ordem de b é o dobro da ordem de a. Mas por outro lado note que $a = (b, b)$, segundo essa relação a e b possuem a mesma ordem. A partir dessa contradição, concluímos que tanto a ordem de a quanto a de b devem ser infinitas. Como a e b são não triviais implica que $G = \langle a, b\rangle = \langle b\rangle \cong \mathbb{Z}$.

- $b = (b, a)\sigma$

  Temos que:

  $ab = (b, b) \cdot (b, a)\sigma = (b^2, ba)\sigma$

  $aa = a^2 = (b, b) \cdot (b, b) = (b^2, b^2)$

  $ba = (b, a)\sigma \cdot (b, b) = (b, a) \cdot (b, b)\sigma = (b^2, ab)\sigma$

  $bb = b^2 = (b, a)\sigma \cdot (b, a)\sigma = (b, a) \cdot (a, b)\sigma^2 = (b, a) \cdot (a, b) = (ba, ab)$

  $b^2a = (ba, ab) \cdot (b, b) = (bab, ab^2)$

  O autômato mostrado na Figura 28 é semelhante ao apresentado na Figura 26. De fato, as propriedades são idênticas: comutatividade, número de elementos, ordem dos elementos e ciclicidade. Como no caso anterior é possível concluir que $G = \langle a, b\rangle = \langle b\rangle \cong \mathbb{Z}$.

iii. $a = (a, b)$

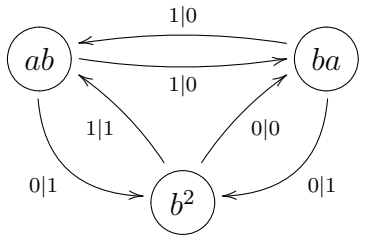

Figura 28 – Autômato $ab = (b^2, ba)\sigma$

Temos quatro possibilidades para b: $b = (b, b)\sigma$, $b = (b, a)\sigma$, $b = (a, b)\sigma$, ou $b = (a, a)\sigma$.

- $b = (b, b)\sigma$

  Temos que:

  $ab = (a, b) \cdot (b, b)\sigma = (ab, b^2)\sigma$
  $aa = a^2 = (a, b) \cdot (a, b) = (a^2, b^2)$
  $ba = (b, b)\sigma \cdot (a, b) = (b, b) \cdot (b, a)\sigma = (b^2, ba)\sigma$
  $bb = b^2 = (b, b)\sigma \cdot (b, b)\sigma = (b, b) \cdot (b, b)\sigma^2 = (b, b) \cdot (b, b) = (b^2, b^2) = (e, e)$
  $ba^{-1} = (b, b)\sigma \cdot (a^{-1}, b^{-1}) = (b, b)(b^{-1}, a^{-1})\sigma = (e, ba^{-1})\sigma$

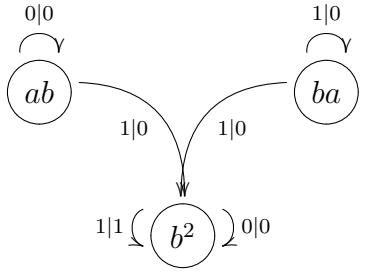

Figura 29 – Autômato $ab = (ab, b^2)\sigma$

Através de uma análise simples da Figura 29 percebemos que $ab \neq ba$, logo o grupo G gerado é não abeliano. Nota-se também que a ordem de b é dois. Agora observe que o termo ba^{-1} é a máquina de adição binária e tem, portanto, tem ordem infinita. Desse modo, o grupo G é não comutativo, gerado por dois elementos, um com ordem dois e outro de ordem infinita. Vamos mostrar que G é isomorfo ao grupo Diedral infinito. Esse grupo tem a seguinte apresentação: $D_\infty = \langle x, y \mid y^2 = 1,\ xy = yx^{-1} \rangle$.
Podemos supor que $x = ba^{-1}$ seja o elemento de ordem infinita e $y = b$ seja o elemento de ordem dois. O que nos resta é verificar a relação $xy = y^{-1}x$.

$xy = ba^{-1}b = (e, ba^{-1})\sigma \cdot (b, b)\sigma = (e, ba^{-1}) \cdot (b, b)\sigma^2 = (b, ba^{-1}b)$
$yx^{-1} = bab^{-1} = (b, b)\sigma \cdot (ab^{-1}, e)\sigma = (b, b) \cdot (e, ab^{-1})\sigma^2 = (b, bab^{-1})$

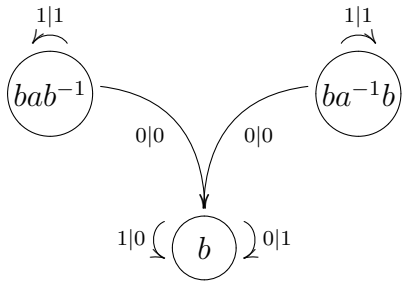

Figura 30 – Autômato $bab^{-1} = (b, ba^{-1}b)$

Repare na Figura 30 que os autômatos bab^{-1} e $ba^{-1}b$ são iguais e portanto, $G = \langle b,\, ba^{-1}\rangle \cong D_\infty$.

- $b = (a, b)\sigma$

  Temos que:

  $ab = (a, b) \cdot (a, b)\sigma = (a^2, b^2)\sigma$
  $a^2 = (a, b) \cdot (a, b) = (a^2, b^2)$
  $ba = (a, b)\sigma \cdot (a, b) = (a, b) \cdot (b, a)\sigma = (ab, ba)\sigma$
  $b^2 = (a, b)\sigma \cdot (a, b)\sigma = (a, b) \cdot (b, a)\sigma^2 = (a, b) \cdot (b, a) = (ab, ba)$
  $ba^{-1} = (a, b)\sigma \cdot (a^{-1}, b^{-1}) = (a, b)(b^{-1}, a^{-1})\sigma = (ab^{-1}, ba^{-1})\sigma$
  $(ba^{-1})^2 = (ab^{-1}, ba^{-1})\sigma \cdot (ab^{-1}, ba^{-1})\sigma = (ab^{-1}, ba^{-1}) \cdot (ba^{-1}, ab^{-1})\sigma^2 = (e, e)$

  Note que $ab^{-1} = (ba^{-1})^{-1} = ba^{-1}$, pois ba^{-1} tem ordem dois. Além disso, o grupo gerado por a e b é não comutativo, pois $ab \neq ba$ já que $a^2 \neq ab$.

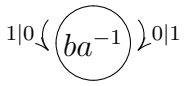

Figura 31 – Autômato $ba^{-1} = (ab^{-1}, ba^{-1})\sigma$

Além disso, percebemos que os estados $ba^{-1} = ab^{-1}$ ja que ambos tem ordem dois. O próximo candidato é o grupo *Lamplighter* cuja apresentação é $L_2 = \langle \sigma, \delta | \sigma^2 = 1, [\sigma, \sigma^{\delta^j}](j \in \mathbb{Z})\rangle$. Este grupo já fora previamente abordado em termos de um sistema dinâmico, onde σ representava a ação de acender uma lâmpada e δ um movimento a direita.

Como $a = (a, b)$ temos:

$(0)^a = 0$
$(1)^a = 1$
$(00)^a = 00^a = 00$
$(01)^a = 01^a = 01$
$(10)^a = 10^b = 11$

$(11)^a = 11^b = 10$

Como $ba^{-1} = (ab^{-1}, ba^{-1})\sigma$:

$(0)^{ba^{-1}} = 1$
$(1)^{ba^{-1}} = 0$
$(00)^{ba^{-1}} = 10^{ab^{-1}} = 11$
$(01)^{ba^{-1}} = 11^{ab^{-1}} = 10$
$(10)^{ba^{-1}} = 00^{ba^{-1}} = 01$
$(11)^{ba^{-1}} = 01^{ba^{-1}} = 00$

Resumidamente, o estado a provoca um movimento a direita na palavra sem alteração da letra, já o estado b provoca movimento a direita na palavra e uma alteração da letra. Ao aplicar ba^{-1} um movimento para a letra seguinte à esquerda, um movimento contrário (para a direita) retornando ao prefixo de comprimento 1 e depois uma alteração no prefixo de comprimento 1. Os estados a e b são ambos de ordem infinita e, de fato, b é a imagem de δ sob o isomorfismo θ do grupo gerado por σ e δ para o autômato grupo. Desse modo, imaginando que a palavra seja equivalente a rua no sistema dinâmico, podemos supor a seguinte correspondência entre os estados do autômato e os elementos δ e σ de L_2:

$\theta : \sigma \mapsto ba^{-1}$ ("acende"/"apaga")
$\theta : \delta \mapsto a$ (move para a direita)

Por fim, resta verificar que $[\sigma, \sigma^{\delta^j}] = 1$, ou seja, $[ba^{-1}, (ba^{-1})^{a^j}] = 1$. Expandindo o comutador na apresentação (lembre-se que ba^{-1}, tem ordem dois, ou seja $ba^{-1} = (ba^{-1})^{-1}$):

$[ba^{-1},(ba^{-1})^{a^j}] = (ba^{-1})^{-1}((ba^{-1})^{a^j})^{-1}(ba^{-1})(ba^{-1})^{a^j}$
$= ba^{-1}((a^{-j}ba^{-1}a^j)^{-1})(ba^{-1})a^{-j}(ba^{-1})a^j$
$= b(a^{-1}a^{-j})b(a^{-1}a^j)b(a^{-1}a^{-j})b(a^{-1}a^j)$
$= b(a^{-(j+1)})b(a^{(j-1)})b(a^{-(j+1)})b(a^{(j-1)}).$

Aplicando-se a sequência de tarefas acima vamos mostrar que o comutador em questão para qualquer valor de j é igual ao elemento identidade. Para atingir esse fim, aplicaremos as tarefas dadas da direita para esquerda:

- a^{j-1} (move $j-1$ para a direita)
- b (move para a posição j e acende a lâmpada)
- $a^{-(j+1)}$ (move para a posição -1)
- b (move para a posição 0 e acende a lâmpada)

- a^{j-1} (move para a posição $j-1$)
- b (move para a posição j e apaga a lâmpada)
- $a^{-(j+1)}$ (move para a posição -1)
- b (move para a posição 0 e apaga a lâmpada, encerrando-se no *lampstand* vazio)

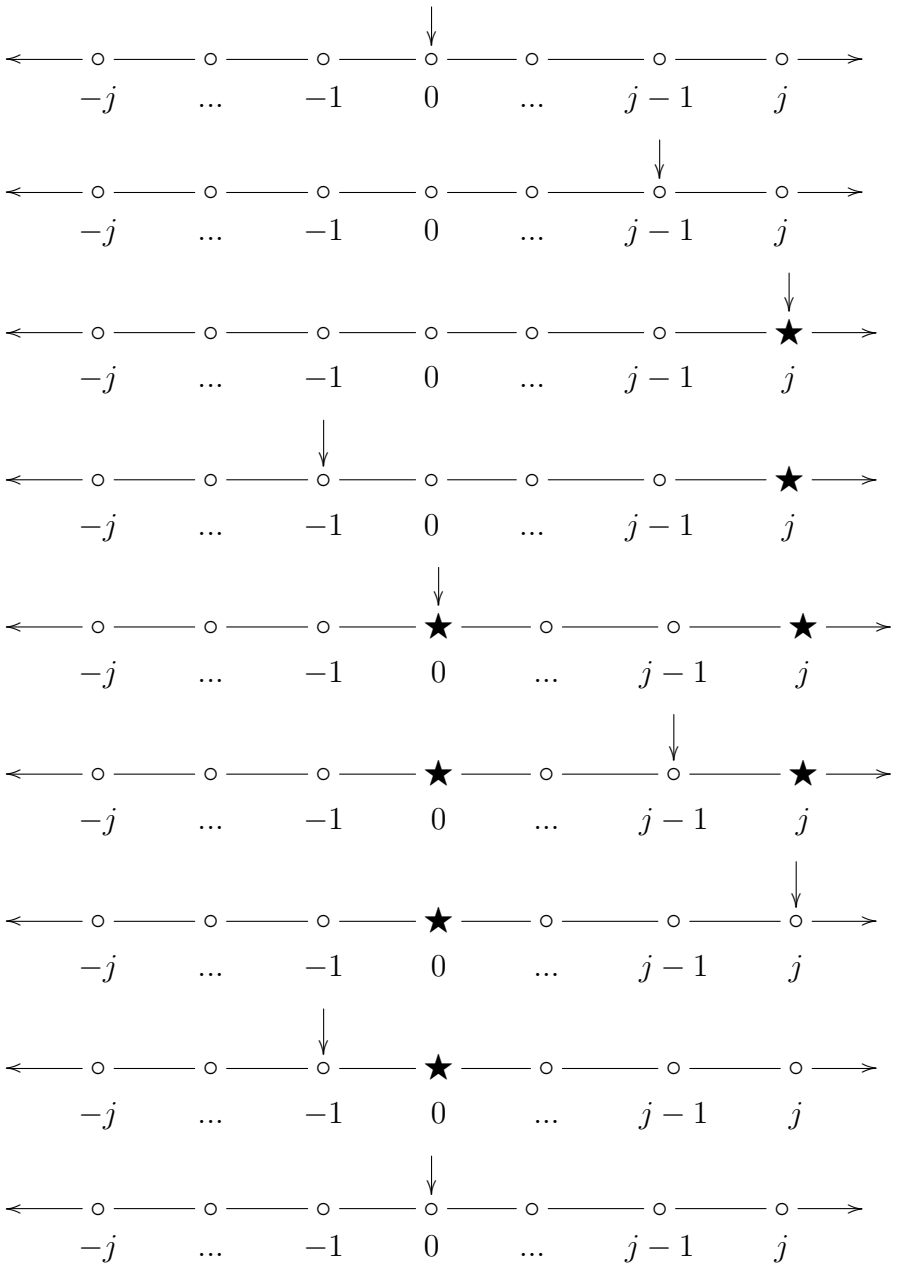

Figura 32 – Interpretação dinâmica do Comutador

A Figura 32 ilustra esse processo dinamicamente. Observe que ao realizar sucessivamente essas tarefas partindo do *Lampstand* vazio, sempre retornaremos a esse estado inicial. Essa representação alternativa ilustra o que o grupo *Lamplighter* tem de tão interessante, que é a possibilidade de ser descrito de várias

formas. Note ainda nessa representação que a tem ordem infinita, pois, é o movimento para direita na rua infinita. De maneira análoga concluímos que b tem ordem infinita, pois é o movimento a direita com a alteração de estado ("acende"/"apaga").

Satisfeita a igualdade $[\sigma, \sigma^{\delta^j}] = e$ para um j, inteiro arbitrário, fica claro que $G = \langle b, ba^{-1} \rangle \cong L_2$.

- $b = (b, a)\sigma$

  Temos que:

  $ab = (a, b) \cdot (b, a)\sigma = (ab, ba)\sigma$
  $a^2 = (a, b) \cdot (a, b) = (a^2, b^2)$
  $ba = (b, a)\sigma \cdot (a, b) = (b, a) \cdot (b, a)\sigma = (b^2, a^2)\sigma$
  $b^2 = (b, a)\sigma \cdot (b, a)\sigma = (b, a) \cdot (a, b)\sigma^2 = (b, a) \cdot (a, b) = (ba, ab)$
  $ba^{-1} = (b, a)\sigma \cdot (a^{-1}, b^{-1}) = (b, a) \cdot (b^{-1}, a^{-1})\sigma = (e, e)\sigma = \sigma$
  $(ba^{-1})^2 = \sigma^2 = e$
  $ab^{-1} = (ba^{-1})^{-1} = \sigma^{-1} = \sigma$
  $(ab^{-1})^2 = \sigma^2 = e$

  Este caso é bastante semelhante ao anterior. Possuímos os elementos ab^{-1} e ba^{-1} de ordem dois. De maneira análoga a realizada anteriormente, podemos mostrar que a correspondência $\theta : \sigma \mapsto ba^{-1}$ e $\theta : \delta \mapsto a$ é um isomorfismo e portanto, o grupo $G = \langle b, ba^{-1} \rangle$ gerado é o *Lamplighter*.

- $b = (a, a)\sigma$

  Temos que:

  $ab = (a, b) \cdot (a, a)\sigma = (a^2, ba)\sigma$
  $a^2 = (a, b) \cdot (a, b) = (a^2, b^2)$
  $ba = (a, a)\sigma \cdot (a, b) = (a, a) \cdot (b, a)\sigma = (ab, a^2)\sigma$
  $b^2 = (a, a)\sigma \cdot (a, a)\sigma = (a, a) \cdot (a, a)\sigma^2 = (a, a) \cdot (a, a) = (a^2, a^2)$
  $ba^{-1} = (a, a)\sigma \cdot (a^{-1}, b^{-1}) = (a, a)(b^{-1}, a^{-1})\sigma = (ab^{-1}, e)\sigma$
  $(ba^{-1})^2 = (ab^{-1}, e)\sigma \cdot (ab^{-1}, e)\sigma = (ab^{-1}, e) \cdot (e, ab^{-1})\sigma^2 = (ab^{-1}, ab^{-1})$
  $ab^{-1} = (a, b) \cdot (a^{-1}, a^{-1})\sigma = (a, b)(a^{-1}, a^{-1})\sigma = (e, ba^{-1})\sigma$
  $(ab^{-1})^2 = (e, ba^{-1})\sigma \cdot (e, ba^{-1})\sigma = (e, ba^{-1}) \cdot (ba^{-1}, e)\sigma^2 = (ba^{-1}, ba^{-1})$

  A análise conjunta dos termos ab, a^2, b^2, ba e do respectivo autômato representado na Figura 33 leva a importantes considerações. O grupo gerado por a e b não é comutativo. Além disso, ao observarmos a Figura 34, notamos que as relações $ba^{-1} = (ab^{-1}, e)\sigma$ e $(ba^{-1})^2 = (ab^{-1}, ab^{-1})$ implicam que a ordem de ba^{-1}

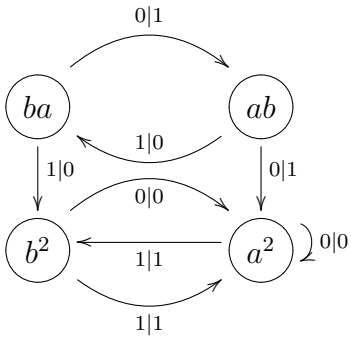

Figura 33 – Autômato $ba = (ab, a^2)$

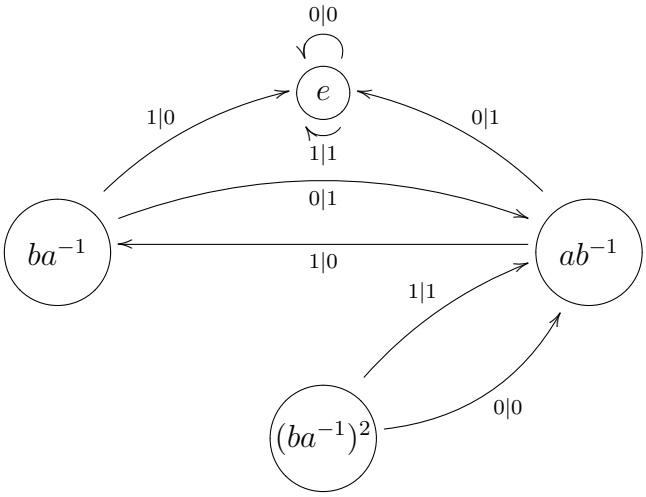

Figura 34 – Autômato $(ba^{-1})^2 = (ab^{-1}, ab^{-1})$

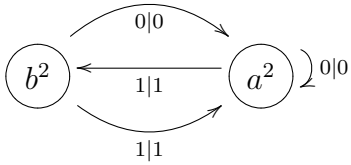

Figura 35 – Autômato $a^2 = (a^2, b^2)$

é infinita. Tem-se que pelas relações $a^2 = (a^2, b^2)$ e $b^2 = (a^2, a^2)\sigma^2 = (a^2, a^2)$, a e b possuem a mesma ordem.

Além disso, $a^2 = b^2 = e$, ou seja, a e b possuem ordem dois. Podemos aplicar esses autômatos em um conjunto de palavras para visualizar mais facilmente essa relação.

$(0)^{a^2} = 0$

$(1)^{a^2} = 1$

$(00)^{a^2} = 00^{a^2} = 00$

$(01)^{a^2} = 01^{a^2} = 01$

$(10)^{a^2} = 10^{b^2} = 10$

$(11)^{a^2} = 11^{b^2} = 11$
$(0)^{b^2} = 0$
$(1)^{b^2} = 1$
$(00)^{b^2} = 00^{a^2} = 00$
$(01)^{b^2} = 01^{a^2} = 01$
$(10)^{b^2} = 10^{a^2} = 10$
$(11)^{b^2} = 11^{a^2} = 11$

Repare também que se $x = ba^{-1}$ e $y = a$, a relação $xy = yx^{-1}$ é válida, pois $ba^{-1}a = b$ e $aab^{-1} = a^2b^{-1} = b^{-1}$, como b tem ordem dois, $b = b^{-1}$ e $ba^{-1}a = aab^{-1}$. Sendo assim, podemos dizer que este grupo é isomorfo a D_∞.

iv. $a = (b, a)$

Temos também quatro possibilidades para b: $b = (b, b)\sigma$, $b = (b, a)\sigma$, $b = (a, b)\sigma$, ou $b = (a, a)\sigma$. Esses casos se assemelham aos realizados para $a = (a, b)$, ocorrendo apenas a troca 0 por 1. Os grupos gerados são os mesmos, já que as propriedades básicas se mantém.

- $b = (b, b)\sigma$

  Temos que:

  $ab = (b, a) \cdot (b, b)\sigma = (b^2, ab)\sigma$
  $aa = a^2 = (b, a) \cdot (b, a) = (b^2, a^2)$
  $ba = (b, b)\sigma \cdot (b, a) = (b, b) \cdot (a, b)\sigma = (ba, b^2)\sigma$
  $bb = b^2 = (b, b)\sigma \cdot (b, b)\sigma = (b, b) \cdot (b, b)\sigma^2 = (b, b) \cdot (b, b) = (b^2, b^2) = (e, e)$
  $ba^{-1} = (b, b)\sigma \cdot (b^{-1}, a^{-1}) = (b, b)(a^{-1}, b^{-1})\sigma = (ba^{-1}, e)\sigma$

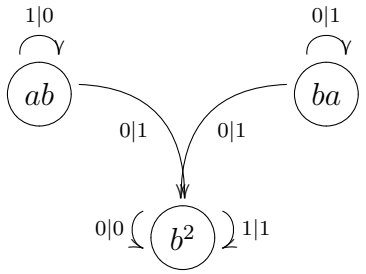

Figura 36 – Autômato $ab = (b^2, ab)\sigma$

Note a semelhança da Figura 36 ($ab = (ab, b^2)\sigma$) com a Figura 29 ($ab = (b^2, ab)\sigma$). De fato, há apenas a inversão de 0 por 1 nos autômatos. O mesmo padrão se repete nas Figuras 30 e 37. Como naquele caso demonstrado, é possível fazer $x = ba^{-1}$ e $y = b$ e mostrar que as propriedades do grupo Diedral são

satisfeitas. Os autômatos bab^{-1} e $ba^{-1}b$ também são iguais e portanto, $G = \langle b, ba^{-1} \rangle \cong D_\infty$.

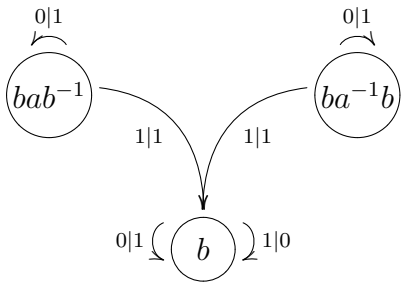

Figura 37 – Autômato $bab^{-1} = (ba^{-1}b, b)$

- $b = (a, b)\sigma$

  Temos que:

  $ab = (b, a) \cdot (a, b)\sigma = (ba, ab)\sigma$
  $a^2 = (b, a) \cdot (b, a) = (b^2, a^2)$
  $ba = (a, b)\sigma \cdot (b, a) = (a, b) \cdot (a, b)\sigma = (a^2, b^2)\sigma$
  $b^2 = (a, b)\sigma \cdot (a, b)\sigma = (a, b) \cdot (b, a)\sigma^2 = (a, b) \cdot (b, a) = (ab, ba)$
  $ba^{-1} = (a, b)\sigma \cdot (b^{-1}, a^{-1}) = (a, b)(a^{-1}, b^{-1})\sigma = (e, e)\sigma$
  $(ba^{-1})^2 = (e, e)\sigma \cdot (e, e)\sigma = (e, e) \cdot (e, e)\sigma^2 = (e, e)$

  Ao analisar essas equações percebemos que b possui ordem infinita, além disso a ordem de ba^{-1} é dois. Situação idêntica a observada anteriormente para $a = (a, b)$ e $b = (a, b)\sigma$. Fazendo a correspondência $\theta : \sigma \to ba^{-1}$ e $\theta : \delta \to b$, é possível mostrar que é satisfeita a igualdade $[\sigma, \sigma^{\delta^j}] = e$ para um j, inteiro arbitrário. Logo $G = \langle b, ba^{-1} \rangle \cong L_2$. Ou seja o grupo gerado é o *Lamplighter*.

- $b = (b, a)\sigma$

  Temos que:

  $ab = (b, a) \cdot (b, a)\sigma = (ab, ba)\sigma$
  $a^2 = (b, a) \cdot (b, a) = (b^2, a^2)$
  $ba = (b, a)\sigma \cdot (b, a) = (b, a) \cdot (a, b)\sigma = (ba, ab)\sigma$
  $b^2 = (b, a)\sigma \cdot (b, a)\sigma = (b, a) \cdot (a, b)\sigma^2 = (b, a) \cdot (a, b) = (ba, ab)$
  $ba^{-1} = (b, a)\sigma \cdot (b^{-1}, a^{-1}) = (b, a) \cdot (a^{-1}, b^{-1})\sigma = (ba^{-1}, ab^{-1})\sigma$
  $(ba^{-1})^2 = \sigma^2 = e$
  $ab^{-1} = (ba^{-1})^{-1} = \sigma^{-1} = \sigma$
  $(ab^{-1})^2 = \sigma^2 = e$

Possuímos elementos ab^{-1} e ba^{-1} de ordem dois. Já os elementos a e b possuem ordem infinita. Além disso, a correspondência $\theta : \sigma \mapsto ba^{-1}$ e $\theta : \delta \mapsto a$ é um isomorfismo. Portanto, o grupo $G = \langle b, ba^{-1} \rangle$ gerado é o *Lamplighter*.

- $b = (a, a)\sigma$

  Temos que:

  $ab = (b, a) \cdot (a, a)\sigma = (ba, a^2)\sigma$
  $a^2 = (b, a) \cdot (b, a) = (b^2, a^2)$
  $ba = (a, a)\sigma \cdot (b, a) = (a, a) \cdot (a, b)\sigma = (a^2, ab)\sigma$
  $b^2 = (a, a)\sigma \cdot (a, a)\sigma = (a, a) \cdot (a, a)\sigma^2 = (a, a) \cdot (a, a) = (a^2, a^2)$
  $ba^{-1} = (a, a)\sigma \cdot (b^{-1}, a^{-1}) = (a, a)(a^{-1}, b^{-1})\sigma = (e, ab^{-1})\sigma$
  $(ba^{-1})^2 = (ab^{-1}, e)\sigma \cdot (e, ab^{-1})\sigma = (e, ab^{-1}) \cdot (ab^{-1}, e)\sigma^2 = (ab^{-1}, ab^{-1})$
  $ab^{-1} = (b, a) \cdot (a^{-1}, a^{-1})\sigma = (b, a)(a^{-1}, a^{-1})\sigma = (ba^{-1}, e)\sigma$
  $(ab^{-1})^2 = (ba^{-1}, e)\sigma \cdot (ba^{-1}, e)\sigma = (ba^{-1}, e) \cdot (e, ba^{-1})\sigma^2 = (ba^{-1}, ba^{-1})$

  Caso idêntico ao mostrado para $a = (a, b)$ e $b = (a, a)\sigma$. Os estados $ba^{-1} = ab^{-1}$ possuem ordem infinita. Já a e b possuem ordem igual a dois. Se $x = ba^{-1}$ e $y = a$, a relação $xy = yx^{-1}$ é válida, pois $ba^{-1}a = b$ e $aab^{-1} = a^2b^{-1} = b^{-1}$, como b tem ordem dois, $b = b^{-1}$ e $ba^{-1}a = aab^{-1}$. Sendo assim, o grupo gerado é o D_∞.

□

Neste capítulo foram apresentados os grupos gerados por autômatos de até dois estados no alfabeto de duas letras. É interessante notar que várias possibilidades de combinações de dois estados são possíveis, entretanto essas combinações de estados conduzem a um número limitado de grupos gerados.

5 Aplicações para o Ensino

A tecnologia computacional vem evoluindo em passos rápidos. Um celular moderno tem mais poder de processamento do que um avançado computador da década de 60. Tarefas que antigamente eram exclusivamente manuais são automatizadas com o uso de máquinas. Há uma demanda crescente por profissionais com habilidades computacionais no mercado de trabalho.

Nessa sociedade cada vez mais tecnológica, o ensino de algoritmos, autômatos e linguagem máquinas se torna cada vez mais essencial. Seja para aprender uma profissão ou para resolver problemas do cotidiano. Já não é mais raro escolas modelo ensinarem em tenras idades princípios básicos de programação. Entretanto, o ensino desses, para ser bem sucedido, deve ser associado a fundamentos da matemática.

Este capítulo propõe uma abordagem para o ensino de autômatos e máquinas de leitura. Esse enfoque é baseado em conceitos discutidos anteriormente. O objetivo é fornecer ao aluno, do ensino fundamental, um contato com a linguagem de máquina.

O conteúdo abordado destina-se a alunos a partir do 4º ano do Ensino Fundamental, após terem consolidado conceitos como: múltiplos, divisores de um número, divisão euclidiana e resto. Além disso, os conceitos abordados neste capítulo podem ser utilizados para apresentar a linguagem de máquina a alunos que nunca tiveram contato.

5.1 Linguagem de Máquina

A linguagem de máquina (código de máquina) é uma linguagem estritamente numérica projetada para ser executada o mais rápido possível. Pode ser considerada como a representação de nível mais baixo de um programa de computador compilado. É uma linguagem de programação primitiva dependente de hardware.

5.2 Base decimal e base binária

O sistema numeral decimal é o sistema padrão para denotar números inteiros e não inteiros. É formado pelos algarismos 0,1,2,3,4,5,6,7,8 e 9. Além disso, é um sistema posicional, ou seja, a posição do algarismo no número muda o seu valor.

O sistema de numeração binário também é posicional. Emprega o número dois como base e portanto, exige apenas dois símbolos diferentes para seus dígitos: 0 e 1. Nesse sentido, difere do sistema decimal que usa 10 símbolos diferentes.

A importância do sistema binário para a tecnologia da computação deriva principalmente de seu aspecto compacto e confiável. Os dígitos 0 e 1 podem ser representados em dispositivos eletromecânicos com dois estados: "acesso/apagado", "aberto/fechado" ou "vá/não vá".

Detalharemos agora os algoritmos de conversão de decimal para binário, assim como binário para decimal. Os exemplos, assim como parte do texto, foram extraídos do livro de cálculo numérico: aspectos teóricos e computacionais [10].

5.2.1 Decomposição de um número em um sistema de bases

Os números empregados no cálculo computacional podem ser de dois tipos: base decimal e sistemas de "ponto flutuante" (por exemplo, o número 3,56 no sistema de ponto flutuante fica: 0.356×10^{-1}). Os computadores atuais representam os números internamente no formato binário, como uma sequência de zeros e uns. Apesar dessa representação ser conveniente para as máquinas é antinatural para os seres humanos. Atualmente, é preferido o uso do sistema de numeração decimal. Ressalta-se que no passado o nosso sistema de numeração já foi na base 12 e também na base 60.

Em geral qualquer número pode ser decomposto numa soma dos dígitos que o constitui vezes potências da sua base.

Definição 5.2.1 (Teorema Fundamental da Numeração)**.** *O valor decimal de um determinado número em outro sistema de numeração pode ser expresso por meio da seguinte fórmula:*

$$N = \sum_{i=-d}^{n} (\phi_i \times \sigma^i)$$

onde:

- ϕ *é a base do sistema de numeração.*
- i *é a posição do dígito em relação a vírgula.*
- d *é o número de dígitos a direita da vírgula.*
- n *é o número de dígitos a esquerda da vírgula -1.*
- σ *é cada um dos dígitos que compõe o número.*

Para o caso binário temos:

$$N = a_0 \times 2^0 + a_1 \times 2^1 + a_2 \times 2^2 ... a_n \times 2^n.$$

Veremos inicialmente a conversão de números inteiros. Considere os números $(347)_{10}$ e $(10111)_2$. Estes números podem ser assim escritos:

$(347)_{10} = 3 \times 10^2 + 4 \times 10^1 + 7 \times 10^0$

$(10111)_2 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$.

Considere agora um número fracionário qualquer, tal como $(10,1)_2$. Este pode ser escrito da seguinte forma:

$(10,1)_2 = 1 \times 2^1 + 0 \times 2^0 + 1 \times 2^{-1}$.

5.3 Conversão de Binário para Decimal

Podemos realizar a conversão de binário para decimal facilmente. Por exemplo, vamos encontrar o correspondente do número binário $(10111)_2$ na base decimal $(x)_{10}$.

$(10111)_2 = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$

Colocando agora o número dois em evidência temos:

$(10111)_2 = 2 \times (1 + 2 \times (1 + 2 \times (0 + 2 \times 1))) + 1 = (23)_{10}$

Agora considere o número $(110,11)_2$. Vamos encontrar o correspondente desse número na base decimal $(x)_{10}$.

$(110,11)_2 = 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 + 1 \times 2^{-1} + 1 \times 2^{-2} = 6,75 = (6,75)_{10}$

Um número inteiro em decimal pode sempre ser representado exatamente por um inteiro binário. Entretanto, essa afirmação não é válida para todos os números fracionários em decimal. Números fracionários decimais, tais como 0,1, não possuem representação finita em binário.

5.4 Conversão de Decimal para Binário

Por outro lado, para convertermos um número escrito na base decimal para binário devemos aplicar um método (divisões sucessivas) para a parte inteira e um método (multiplicações sucessivas) para a parte fracionária, se houver.

5.4.1 Método das divisões sucessivas

Converteremos o número inteiro 23 na base decimal para a base binária usando o método das divisões sucessivas. Ou seja, queremos encontrar um número x escrito em binário tal que: $(23)_{10} \overset{divisões\ sucessivas}{\longrightarrow} (x)_2$.

Como a Figura 38 ilustra, $(x)_2 = (10111)_2$ é o resultado da conversão. Aplicamos ao número decimal que desejamos converter, sucessivas divisões por dois. Devemos seguir

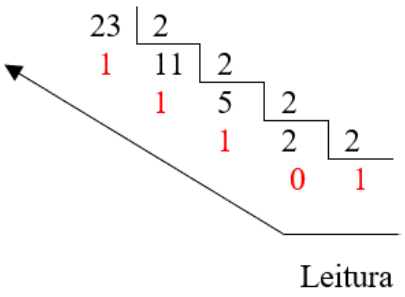

Figura 38 – Conversão 23 decimal em binário: $(23)_{10} = (10111)_2$

as divisões até que o quociente seja menor que a base. O número binário convertido é constituído pelos sucessivos restos dessas divisões. Além disso, a leitura é feita no sentido indicado pela seta.

Faremos agora um exemplo um pouco mais complexo:

Usando novamente o método de divisões sucessivas, converteremos o número 347 escrito na base decimal para a base binária. Em outras palavras, queremos encontrar x (escrito apenas com zeros e uns) tal que: $(347)_{10} \overset{divisões\ sucessivas}{\longrightarrow} (x)_2$.

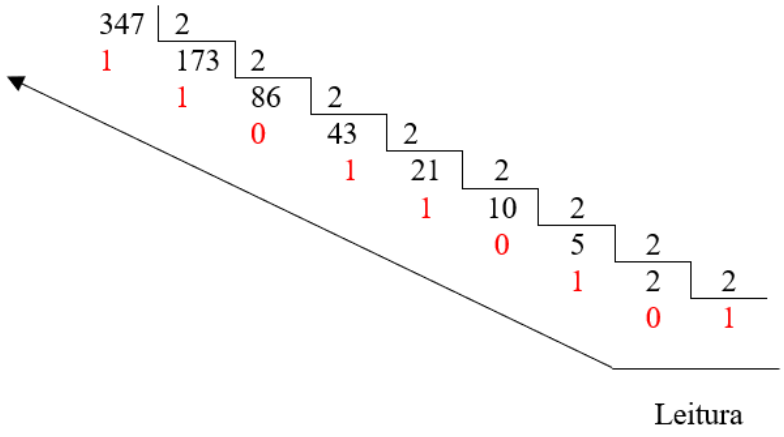

Figura 39 – Conversão 347 decimal em binário: $(347)_{10} = (101011011)_2$

Após realizar os passos desse procedimento, percebemos que $(x)_2 = (101011011)_2$ é o resultado da conversão (Figura 39) .

5.4.2 Método das multiplicações sucessivas

Tomemos números fracionários escritos na base decimal e façamos a conversão para a base binária. Para isso, devemos utilizar o método das multiplicações sucessivas. Esse método será demonstrado a seguir:

Inicialmente, converteremos $0,125$ para binário, $(0,125)_{10} \overset{multiplicações\ sucessivas}{\longrightarrow} (x)_2$.

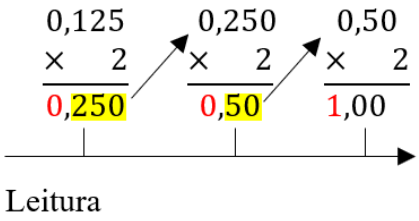

Figura 40 – Conversão de $(0,125)_{10}$ para a base binária: $(0,125)_{10} = (0,001)_2$

A partir da Figura 40, notamos que para realizar essa conversão devemos multiplicar sucessivamente o número fracionário até obtermos 1. O número binário será formado a partir das partes inteiras das multiplicações sucessivas. O sentido da leitura também é indicado na Figura 40, que é da esquerda para a direita. Logo $(x)_2 = (0,001)_2$.

Desejamos converter o número 0,1875, escrito em base decimal, para a base binária. Ou seja, queremos encontrar x (escrito apenas com zeros e uns) tal que: $(0,1875)_{10} \overset{multiplicações\ sucessivas}{\longrightarrow} (x)_2$. O procedimento é idêntico (representado na Figura 41).

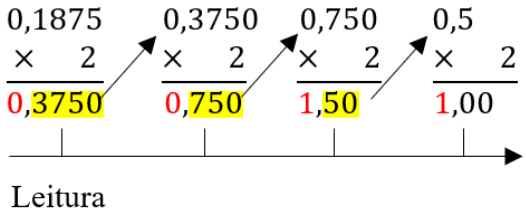

Figura 41 – Conversão $(0,1875)_{10}$ para a base binária: $(0,1875)_{10} = (0,0011)_2$.

Ressalta-se novamente que alguns números como o 0,1 não tem representação finita na base binária, em outras palavras, o método das multiplicações sucessivas, tal procedimento como apresentado, não para.

5.5 Operação de Adição em Binário

Uma pergunta pertinente é sobre como realizar operações básicas em binário. Nesta seção, analisaremos a operação mais básica, a adição.

A adição entre dois números binários possui as seguintes propriedades:

$0 + 0 = 0$

$0 + 1 = 1$

$1 + 0 = 1$

$1 + 1 = 0$ e vai 1 (soma-se 1 ao dígito imediatamente à esquerda).

Exemplo 5.5.1. Considere os números $(1100)_2$ (12 em decimal) e $(111)_2$ (7 em decimal). Podemos somá-los como exemplificado na Figura 42:

Figura 42 – Adição de 1100 a 111

E de fato $12 + 7 = 19 = (10011)_2$.

Exemplo 5.5.2. Considere agora os números $(1100)_2$ (12 em decimal) e $(1111)_2$ (15 em decimal). Podemos somá-los como exemplificado na Figura 43:

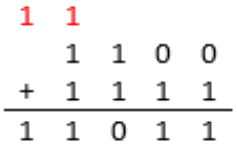

Figura 43 – Adição de 1100 a 1111

E de fato $12 + 15 = 27 = (11011)_2$.

Na soma de 0 com 1 o total é 1. Quando se soma 1 com 1, o resultado é 2, mas como 2 em binário é 10, o resultado é 0 (zero) e passa-se o outro 1 para a "frente", ou seja, para ser somado com o próximo elemento.

A adição entre dois números binários também pode ser compreendida em termos de autômatos. Esses estão ligados aos mecanismos das calculadoras básicas, que ao longo da história evoluíram e deram origem aos primeiros computadores.

Exemplo 5.5.3. A máquina de adição abordada no Capítulo 2 é o autômato que adiciona um pela esquerda a um número binário. Podemos utilizá-lo, para realizar adições em palavras de um mesmo comprimento.

Suponha que queremos somar um (pela direita) aos números: $(00)_2$ (0 em decimal), $(01)_2$ (1 em decimal), $(10)_2$ (2 em decimal) e $(11)_2$ (3 em decimal). Para usarmos a máquina para realizar essa adição, basta lermos essas palavras binárias na ordem inversa, conforme indica a Figura 44:

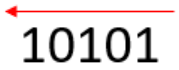

Figura 44 – Sentido de leitura da palavra binária neste processo de adicão

E então podemos computar os números em binário no autômato da Figura 45:

$$\begin{aligned} \tau(00) &= 1e(0) = 10 \qquad 0+1=1 \\ \tau(10) &= 0\tau(0) = 01 \qquad 1+1=2 \\ \tau(01) &= 1e(1) = 11 \qquad 2+1=3 \\ \tau(11) &= 0\tau(1) = 00 \qquad 3+1=0. \end{aligned}$$

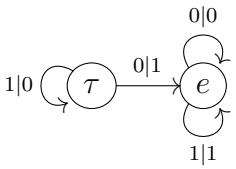

Figura 45 – Autômato $\tau = (e,\tau)\sigma$

Em outras palavras, se queremos somar 1 a um número qualquer tal como $(10)_2$, devemos ler na máquina $(01)_2$ que resulta em $(11)_2 = (3)_{10}$. E de fato, $2+1=3$.

Podemos repetir esse processo n vezes, para obter a adição por dois, três e assim por diante, desde que a adição preserve o comprimento da palavra, ou o número de dígitos do número binário.

5.6 Máquina de Leitura

Um autômato finito determinístico pode ser interpretado como uma máquina de leitura que possui os requisitos que serão apresentados a seguir. Este autômato, como vimos anteriormente, é capaz de ler uma palavra binária finita, um caractere de cada vez, lendo da esquerda para a direita. Lembre-se que o domínio de um autômato consiste de palavras binárias finitas e não os números binários representados por essas palavras. Começaremos listando de forma geral os requisitos de um autômato determinístico de finitos estados (de leitura):

- Possui um número finito de estados.
- Um de seus estados é designado como seu estado inicial.
- Ele pode ler apenas um conjunto finito de caracteres definido, chamado alfabeto, um de cada vez.
- Suas palavras de entrada devem ter comprimento finito.
- Dado um estado e um caractere possível, um conjunto de instruções determina a resposta (esta é a parte determinística de seu nome).
- Ele pode ler que a palavra chegou ao fim, momento em que para.
- Alguns estados são chamados *estados finais.*

Após essa breve introdução, estamos prontos para introduzir formalmente a definição de um autômato finito determinístico, ou simplesmente, autômato de leitura. O ponto principal desse tipo de autômato é saber se, após a palavra a ser lida, a *parada* acontece em um estado final. Nesse caso, dizemos que o autômato *reconhece* a palavra. O conjunto de todas as palavras reconhecidas por um autômato é chamado de *linguagem* desta máquina.

Definição 5.6.1. *Um autômato autômato finito determinístico é dado por* $A_q = (Q, Y, f, q_0, F)$ *onde:*

- Q *é um conjunto de estados;*
- Y *é o alfabeto de entrada;*
- $f\colon Q \times Y \to Q$ *é a aplicação parcial de transição de estados;*
- q_0 *é o estado denominado inicial.*
- F *é o conjunto de estados finais.*

É importante destacar que esse autômato é diferente do autômato de Mealy apresentado anteriormente. O autômato de Mealy lê uma palavra e devolve outra palavra de saída, enquanto a máquina de leitura, lê uma palavra e determina apenas se ela é aceita ou não.

Os estados inicial e final podem ser representados como na Figura 46:

Exemplo 5.6.1. O autômato apresentado na Figura 47, reconhece os números que deixam resto 1 na divisão por 2, ou seja, os números ímpares. Note que os estados inicial e final desse autômato são diferentes.

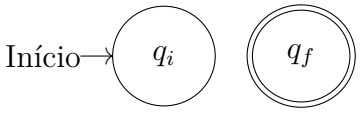

Figura 46 – Autômato estados inicial/final

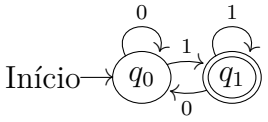

Figura 47 – Autômato que reconhece números ímpares

Exemplo 5.6.2. O autômato apresentado na Figura 48, é um caso em que os estados inicial e final de um autômato coincidem. Este autômato reconhece os números pares.

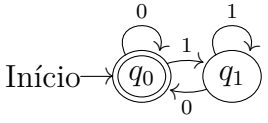

Figura 48 – Autômato que reconhece números pares

Um exemplo de máquina de leitura é o autômato que reconhece um número decimal e indica seu resto pela divisão por um número natural. No Capítulo 2 exploramos inicialmente essa ideia, que será agora aprofundada com vistas a aplicar ao ensino.

Considere a Figura 49, a máquina de leitura reconhece números múltiplos de 3. Note que quando a máquina para em q_0 então o número lido deixa resto 0 na divisão por 3.

Tome um número natural qualquer como o 27. Por exemplo, vamos agora determinar o resto de sua divisão por três. Note que: $(27)_{10} = (11011)_2$. A leitura será feita da esquerda para a direita. O algarismo 1 ao ser lido conduz a q_1. Em seguida, ao ler o algarismo 1 somos conduzidos ao estado q_0. A máquina ao ler o algarismo 0 leva ao estado q_0 novamente. Ao ler o próximo algarismo 1 somos levados ao estado q_1. E por fim com o algarismo 0 retornamos a q_0. Em resumo temos: $q_0 \xrightarrow{1} q_1 \xrightarrow{1} q_0 \xrightarrow{0} q_0 \xrightarrow{1} q_1 \xrightarrow{1} q_0$. Após essas etapas a leitura é encerrada. Concluímos que o número 27 é reconhecido pelo autômato da Figura 49 e portanto, o resto da divisão de 27 por 3 é 0. E de fato: $27/3 = 9$.

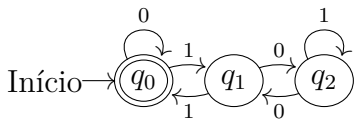

Figura 49 – Autômato que determina se um número binário é múltiplo de 3

De forma semelhante, quando a leitura é finalizada em q_1, embora o número não seja reconhecido pelo autômato podemos obter a informação de que o número lido deixa resto 1, quando a máquina para em q_2 ao fim da leitura o resto é 2. Tome o número natural 347. Vamos agora determinar o resto de sua divisão por três. Como mostrado anteriormente, $(347)_{10} = (101011011)_2$. Iniciaremos a leitura a partir da esquerda para a direita. O algarismo 1 ao ser lido conduz a q_1. Em seguida, ao ler o algarismo 0 (em q_1) somos conduzidos ao estado q_2. A máquina ao ler o algarismo 1 leva ao estado q_2. Ao ler o próximo algarismo 0 somos levados ao estado q_1. E assim por diante. Em resumo temos: $q_0 \xrightarrow{1} q_1 \xrightarrow{0} q_2 \xrightarrow{1} q_2 \xrightarrow{0} q_1 \xrightarrow{1} q_0 \xrightarrow{1} q_1 \xrightarrow{0} q_2 \xrightarrow{1} q_2 \xrightarrow{1} q_2$. Após essas etapas a leitura é encerrada. Concluímos que o resto da divisão de 347 por 3 é 2. E de fato: 347/3 = 115×3+2.

Considere agora a máquina de leitura que reconhece os múltiplos de 5. Esta é mais complexa que a máquina de divisão por três, porque possui uma maior quantidade de restos possíveis. Os diferentes estados q_1, q_2, q_3 e q_4, indicam os possíveis restos de um número natural lido pela máquina, estes são: 1,2,3,4 sucessivamente. Considere o número $(23)_{10} = (10111)_2$. O primeiro algarismo da esquerda para a direita é 1. Desse modo, partindo do estado inicial atingimos o estado q_1. Ao aplicarmos em sequência os algarismos 0,1,1 e 1 somos conduzidos ao estado q_3. Logo o resto da divisão de 23 por cinco é três.

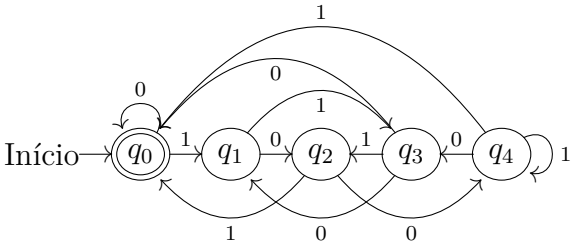

Figura 50 – Autômato que determina se um número na base decimal é múltiplo de 5

Tome novamente o número $(347)_{10} = (101011011)_2$. Ao ler esse número usando o autômato da Figura 50 obtemos: $q_0 \xrightarrow{1} q_1 \xrightarrow{0} q_2 \xrightarrow{1} q_0 \xrightarrow{0} q_0 \xrightarrow{1} q_1 \xrightarrow{1} q_3 \xrightarrow{0} q_1 \xrightarrow{1} q_3 \xrightarrow{1} q_2$. Logo o resto da divisão de 347 por 5 é dois.

Por último, utilizemos o número $(360)_{10} = (101101000)_2$. Ao ler esse número usando este autômato obtemos: $q_0 \xrightarrow{1} q_1 \xrightarrow{0} q_2 \xrightarrow{1} q_0 \xrightarrow{1} q_1 \xrightarrow{0} q_2 \xrightarrow{1} q_0 \xrightarrow{0} q_0 \xrightarrow{0} q_0 \xrightarrow{0} q_0$. Logo o resto da divisão de 360 por 5 é zero.

5.7 Comentários finais

Nesse capítulo foram apresentados conteúdos que ajudam a exercitar e consolidar os conceitos de múltiplos, divisores de um número, divisão euclidiana e resto no ensino

fundamental. Entre esses conceitos, abordamos a linguagem de máquinas, conversões binário para decimal, decimal para binário, a operação binária de adição e máquinas de leitura simples.

Os conceitos discutidos permitem o aluno se familiarizar com a linguagem de máquina. Essa abordagem pode ser utilizada como um primeiro contato do aluno com a linguagem computacional, esta é parte do alicerce conceitual utilizado para o desenvolvimento de várias tecnologias. Apesar disso, é importante destacar que existem outras metodologias e abordagens que podem ser utilizadas para esse primeiro contato.

Os recentes avanços científicos declaram a obsolescência de certas atividades e profissões. Em um mundo cada vez mais tecnológico e globalizado, a demanda por habilidades relacionadas a automatização e a programação são crescentes. O uso de algoritmos e máquinas de estado, em particular autômatos, permite que o desenvolvimento de competências essenciais a solução de diversos problemas. Ou seja, o aprendizado de linguagem de máquinas se inclui no rol de conhecimentos úteis a socialização do indivíduo. Nesse sentido, a escola, desde a educação básica a superior, necessita se adaptar a essas novas tendências.

Referências

[1] Gonçalves, A. *Introdução à Álgebra*. IMPA, Rio de Janeiro, 2017. Citado na página 21.

[2] Zuk, A. *Automata groups*. Bourbaki Seminar, Volume 2006/2007, Exposed 967-981, Asterisqué no. 971, 34 p., 2008. Disponível em inglês: <http://cms.dm.uba.ar/Members/gcorti/workgroup.GNC/notes.pdf>. Citado 3 vezes nas páginas 20, 21 e 56.

[3] Bonanome, M. C.; Dean, H. M. e Dean, J. P. *A Sampling of Remarkable Groups*. Springer Nature, Switzerland, 2018. Citado 3 vezes nas páginas 21, 43 e 56.

[4] Dantas, A. C. *Representações fechadas por estado de grupos metabelianos tipo entrelaçado*, tese de doutorado em matemática. Universidade de Brasília, 2016. Citado na página 56.

[5] Johnson, D. *Presentation of Groups*. Cambridge: Cambridge University Press, London, 1997. Citado na página 34.

[6] Bartone, E. *Peppe the Lamplighter: A Caldecott Honor Award Winner, Illustration by Ted Lewin*. HarperTrophy, 1997. Citado 2 vezes nas páginas 15 e 55.

[7] Domingues, H. H. e Iezzi, G. *Álgebra Moderna*. Saraiva Uni, São Paulo, 2018. Citado na página 21.

[8] Garcia, A. e Lequain, Y. A. E. *Elementos de Álgebra*. IMPA, Rio de Janeiro, 2018. Citado na página 21.

[9] Gupta, N. e Sidki, S. *On the burnside problem for periodic groups*. Math. Z. 182: 385–388, 1983. Citado 2 vezes nas páginas 19 e 43.

[10] Ruggiero, M. A. G. e Lopes, V. L. de R. *Cálculo Numérico: Aspectos Teóricos e Computacionais*. Pearson, São Paulo, 2000. Citado na página 78.

[11] Bondarenko, I.; Grigorchuk, R.; Kravchenko, R.; Muntyan, Y.; Nekrashevych, V.; Savchuk, D. e Sunic, Z. *Classification of groups generated by 3-state automata over a 2-letter alphabet*. 2018. Citado 2 vezes nas páginas 20 e 61.

[12] Lima, J. *Jorge de Lima: Obra Completa*. José Aguilar, Rio de Janeiro, 1958. Citado na página 55.

[13] Rotman, J. J. *An Introduction to the Theory of Groups*. Springer New York, NY, New York, 1995. Citado 2 vezes nas páginas 19 e 21.

[14] Sidki, S. N. *Regular trees and their automorphims*. Monografias de Matemática, Vol. 56, IMPA, 1998. Citado na página 43.

[15] Tinkham, M. *Group Theory and Quantum Mechanics*. Dover Publications, 2003. Citado na página 19.

[16] Zapata, F. F. R. *Os problemas da conjugação e da ordem para grupos gerados por autômatos de crescimento limitado*, tese de doutorado em matemática. Universidade de Brasília, 2011. Citado 2 vezes nas páginas 19 e 43.

[17] Robinson, D. J. S. *A Course in the Theory of Groups*. Springer New York, NY, New York, 1996. Citado na página 21.

[18] Wolfram, S. *A new kind of science*. Wolfram Media Inc., Champaign, IL, 2002. Citado 2 vezes nas páginas 19 e 21.