Universidade Federal de Sergipe
PRÓ-REITORIA DE PÓS GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Um código co-dígito verificador baseado em D_5: Uma aplicação dos grupos de simetria

Por

Elisabete Santana de Ávila e Silva

Mestrado Profissional em Matemática - São Cristovão - SE

Abril de 2013

Universidade Federal de Sergipe
PRÓ-REITORIA DE PÓS GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT

Elisabete Santana de Ávila e Silva

Um código co-dígito verificador baseado em D_5: Uma aplicação dos grupos de simetria

Trabalho apresentado ao Departamento de Matemática da Universidade Federal de Sergipe como requisito final para a obtenção do título de Mestre em Matemática pelo PROFMAT.

Orientador: Prof. Dr. Kalasas Vasconcelos de Araújo

São Cristóvão - Sergipe
Abril de 2013

Elisabete.png

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE**

Silva, Elisabete Santana de Ávila e
S586c Um código co-dígito verificador baseado em D5: uma aplicação dos grupos de simetria / Elisabete Santana de Ávila e Silva; orientador kalasas Vasconcelos de Araújo. – São Cristóvão, 2013.
27 f.: il.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional – Profmat) – Universidade Federal de Sergipe, 2013.

1. Álgebra abstrata. 2. Teoria dos grupos. 3. Simetria. I. Araújo, Kalasas Vasconcelos de, orient. II. Título

CDU 512.54

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe ,como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Um código co-dígito verificador baseado em D5: Uma aplicação dos grupos de simetria

por

Elisabete Santana de Ávila e Silva

Aprovada pela Banca Examinadora:

Prof. Dr. Kalasas Vasconcelos de Araujo - UFS
Orientador

Prof. Dr. Cláudio Tadeu Cristino - UFRPE
Primeiro Examinador

Prof. Dr. Zaqueu Alves Ramos - UFS
Segundo Examinador

São Cristóvão, 11 de abril de 2013

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Critóvão. Tel. (00 55 79) 2105-6986 – Fax (0 xx 55 79) 2105-6566
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat_ufs@yahoo.com.br

Sumário

Dedicatória

À minha família.

Agradecimentos

- A Deus, porque tudo que sou e tenho veio Dele e tudo que faço é pelo Seu poder e para a Sua honra e glória;
- Ao meu esposo, Abílio Netto, pelo amor e cumplicidade de cada dia;
- Ao pequeno fruto do meu ventre, João Felipe, que a cada chute dentro de mim, me fazia entender que era um especial torcedor por essa vitória;
- À minha mãe, Cristina, mestre da vida e fonte inspiradora, e ao meu pai, Leo, fiel presença;
- Ao professor Dr. Kalasas Vasconcelos, pelo desafio que me entregou, mas que com disponibilidade, paciência e palavras de confiança me ajudou a enfrentar;
- As minhas irmãs, grandes companheiras, pelas mãos sempres estendidas;
- Aos meus cunhados, irmãos de coração;
- Aos grandes amigos encontrados, Lúcia Pereira, Marcele Moreno, Welington Batista Luz, Luis Anselmo, Evani Machado, Edvaldo Reis, Elton Jones, Elson Nascimento, César Augusto, Ávido Sadote, Carlos Alberto, André Calderado, Sérgio Ricardo e reencontrados nesta jornada, Davi Dantas, José Hélio, Gilvan Andrade, Márcio Monte Alegre;
- Aos professores, Cláudio Tadeu Cristino e Zaqueu Alves Ramos, que compuseram a banca examinadora;
- Aos admiráveis professores, Almir Rogério, Éder Mateus, Danilo Felizardo, Evilson Vieira, Paulo Rabelo, José Anderson, Wagner Ferreira, Arlúcio Cruz, Naldisson dos Santos e Fábio dos Santos, que com empenho e dedicação, compartilharam seus conhecimentos e nos deram a oportunidade de crescermos como profissionais.

Resumo

Este trabalho tem como objetivo descrever o Código baseado em D_5 como aplicação de parte da Álgebra Abstrata, através dos Grupos de Simetria, bem como suas vantagens em relação a outros códigos, em se tratando da detecção de erros de digitação. Para tanto, fornecemos algumas definições e teoremas da teoria dos Grupos úteis à compreensão deste trabalho. Estudamos os Grupos de Permutação e os Grupos de Simetria, assuntos de grande relevância para o estudo dos Grupos Diedrais, por serem, estes, caso particular dos grupos citados e base para o desenvolvimento do código aqui descrito.

Palavras chaves: Grupos, Grupos de Simetria, Grupos Diedrais, Código baseado em D_5.

Abstract

This present work to describe the code based on D_5 as part of the application of Abstract Algebra, through Symmetry Groups, as well as its advantages over other codes in the case of detection of typos. To this end, we provide some definitions and theorems of the theory of groups useful for understanding this work. Study groups Permutation Groups and Symmetry, issues of great relevance to the study of dihedral groups, being these, particularly if those groups and the basis for the development of the code described herein.

Key words: Groups, Symmetry groups, Dihedral Groups, Code Based on D_5.

Introdução

A presença maciça do computador na nossa sociedade, com o uso de sistemas de comunicação digital nas mais diversas áreas, tem levado ao estudo e desenvolvimento de novas estruturas e métodos matemáticos que dêem suporte a essas novas tecnologias digitais. A teoria dos códigos é um campo de pesquisa atual, muito atraente, tanto do ponto de vista científico, quanto tecnológico, pois é capaz de misturar conceitos e técnicas importantes da Álgebra abstrata com aplicações imediatas da vida real. A utilização de códigos para identificar produtos e até mesmo pessoas, serve para armazenar suas informações e efetivar a transmissão dessas informações de forma mais segura. Esses códigos correspondem a uma sequência de dígitos numéricos ou alfanuméricos que guardam alguns dados a respeito do produto ou pessoa que está representando. Esses identificadores são encontrados no registro geral, no CPF e CNPJ, na carteira de habilitação, em cartões de crédito, contas bancárias, bilhetes de passagens aéreas, placas de automóveis, acervo de bibliotecas, produtos a venda em lojas e supermercados, dentre várias outras aplicações comerciais.

Entretanto, apesar de seguros, esses códigos estão suscetíveis a erros, principalmente humanos, durante a sua transmissão, tais como:

- Erros de formatação: supressão ou acréscimo de dígitos;
- Erros de dígito singular : substituição de um dígito correto por um dígito incorreto;
- Erros de transposição: troca na posição de dois dígitos;
- Erros gêmeo: digitação dupla de um mesmo dígito.

Em virtude disso, tem-se buscado criar e aprimorar métodos que verifiquem tais erros e que possibilitem a comunicação de dados de maneira mais efetiva. Dígitos verificadores (ou de checagem) são mecanismos que utilizam um ou mais dígitos, acrescentados a uma cadeia de dígitos original, que certifica e/ou corrige esta cadeia, dando maior segurança contra fraudes, erros de digitação ou leitura (através de um scanner, por exemplo). O uso desses dígitos como identificadores numéricos para detecção de erros é, atualmente, um modelo prático e de expressiva eficiência. Eles são formulados através de algoritmos, que podem ser públicos ou não, nos quais empregam-se conceitos algébricos, como a aritmética modular e a teoria de grupos.

Dentre os diversos esquemas de detecção de erros podemos citar:

- Esquema três pesos: baseado na aritmética módulo 10, consiste de 9 dígitos e utiliza três pesos (mais comumente, 7, 3 e 9) no chamado vetor peso. É utilizado por bancos

americanos e em passaportes e possui uma taxa de detecção de erros de 100% para erros singulares e de 88,9% para erros de transposição;

- Esquema módulo 9: Utilizado pelo serviço postal dos EUA e pelos cheques Visa. A taxa de detecção de erros é de 98% para erros singulares;

- Esquema módulo 7: Utilizado pelas Federal Express e United Parcel Service. Detecta 93,3% de erros singulares e de transposição;

- Esquema módulo 11: Utilizado pelo ISBN (Padrão Internacional de Numeração de Livros). Possui taxa de 100% na detecção de erros singulares e de transposição, mas possui a desvantagem de utilizar um carácter alfabético, "X", para representar o valor 10;

- Esquema de permutação: Baseado na aritmética módulo 10, o vetor peso depende da paridade do número de dígitos. É utilizado em cartões de crédito, bibliotecas, bancos de sangue, etc. Detecta 100% de todos os erros, com exceção dos de transposição, que possui taxa de 95,6%;

- Código 39: Baseado na aritmética módulo 39, permite a escrita das 26 letras do alfabeto, dos algarismos de 0 a 9 e ainda dos caracteres -, ., "espaço". É utilizado em companhias automotivas, indústrias de saúde e departamento de defesa. Não consegue detectar 100% dos erros singulares;

- Aritmética módulo 43: Segue o código 39, com o acréscimo de mais 4 caracteres, $, /, + e %. Consegue detectar 100% dos erros singulares e de transposição;

- Sistemas UPC e EAN: Representam o Código Universal de Produtos ou Código de Barras, por isso possuem ampla utilização nas transações comerciais. Consistem numa sequência de 12 (UPC) ou 13 (UPC-A e EAN) dígitos traduzidos em barras assimétricas e utilizam a aritmética módulo 10. O vetor peso do UPC é (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) e do EAN é (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1). O UPC detecta 100% dos erros singulares e 88,9% dos erros de transposição.

Os esquemas até então citados são encontrados com mais detalhes em [5].

O objeto de estudo desse trabalho é o Código baseado em D5 que, embora possua aplicação quase nula, é um dos esquemas de maiores sofisticação e eficiência na verificação de erros de dígitos. Mostraremos, para tanto, que o uso da teoria de grupos, que envolve conceitos matemáticos mais sofisticados que os utilizados nos sistemas baseados na Aritmética Modular, através das operações em um grupo diedral, bem como as definições estabelecidas, fazem deste esquema, até então, o mais completo.

Apresentaremos algumas definições e fatos desta teoria com o objetivo de levar uma melhor compreensão do código descrito, como aplicação da Álgebra abstrata através dos Grupos de Simetria.

Tentaremos esclarecer, da melhor forma possível, o que de fato significa esse código, como foram desenvolvidos os conceitos algébricos empregados e como são detectados os erros mais correntes.

Lista de Figuras

Lista de Tabelas

Capítulo 1

Preliminares

Neste capítulo, estudaremos definições básicas e fatos a respeito da teoria dos grupos que serão usados nos capítulos seguintes onde trataremos de forma mais específica o tema desse trabalho.

1.1 Definições básicas

1. **Grupo**

   Um grupo é um par ordenado $(G, *)$ formado por um conjunto não-vazio G e uma operação binária $*$ sobre G, tal que essa operação sastisfaz os seguintes axiomas:

   (i) *Associatividade*

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

   (ii) *Existência de elemento neutro*

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

   (iii) *Existência de simétricos*

   $\forall a \in G$, $\exists a^{-1} \in G$, tal que $a * a^{-1} = a^{-1} * a = e$

   Se em um grupo $(G, *)$ verifica-se o axioma da *comutatividade*:

   (iv) $a * b = b * a$, $\forall a, b \in G$

   dizemos que esse grupo é um *grupo abeliano*.

2. **Ordem de um Grupo**

   Um grupo $(G, *)$ é dito finito se G possui um número finito de elementos. O número de elementos de G é denominado *Ordem de* $(G, *)$ e é denotado por $|G|$. Esse grupo também é chamado *grupo de finita ordem*.

3. **Grupo Cíclico**

Um grupo multiplicativo $(G, *)$ *(grupo cuja operação* $*$ *é a multiplicação)* será denominado *Grupo Cíclico* se, para algum elemento $a \in G$, a igualdade $G = [a] = \{a^m \mid m \in \mathbb{Z}\}$ é verificada. Para grupos aditivos, teremos $G = [a] = \{ma \mid m \in \mathbb{Z}\}$.

4. **Subgrupo**

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 $(G, *)$, ou seja $(H, *)$.

Proposio 1.1.1. *Um subconjunto não-vazio* H *de um grupo* $(G, *)$ *é um subgrupo de* $(G, *)$ *se, e somente se:*

(i)$a, b \in H$*, então* $a * b \in H$*;*

(ii) $a \in H$*, então* $a^{-1} \in H$*.*

Todo grupo possui dois *subgrupos* ditos *triviais*: o próprio grupo e o grupo formado por seu elemento neutro e. Assim, $(G, *)$ e $(\{e\}, *)$, e elemento neutro de $(G, *)$, são os subgrupos triviais de $(G, *)$.

5. **Índice de um grupo**

Se $(H, *)$ é um subgrupo de $(G, *)$, então o número de diferentes classes laterais à direita de H em G, é denominado *índice de* H *em* G e é denotado por $|G : H|$. Se G é um grupo finito, então ele possui índice finito. Se G for um grupo infinito o seu índice pode ser finito ou infinito.

6. **Geradores**

Um subconjunto S de elementos de um grupo $(G, *)$ com a propriedade de que todo elemento de G pode ser escrito como um produto finito de elementos de S e seus inversos é denominado conjunto de *Geradores de* $(G, *)$, e denotamos por $G = \langle S \rangle$.

Se S é finito, então $(G, *)$ é chamado *Grupo Finitamente Gerado.*

7. **Subgrupo Normal**

Um subgrupo $(N, *)$ de um grupo $(G, *)$ é dito *Normal* se $Na = aN$, para todo $a \in G$, onde $Na = \{n \cdot a | n \in \mathbb{N}\}$. Mais precisamente, as classes laterais (à direita, aN, e à esquerda, Na) coincidem como conjuntos para qualquer $a \in G$. Escrevemos $N \lhd G$ para indicar que N é subgrupo normal em G.

8. **Grupo Quociente**

   Seja $(N, *)$ um subgrupo normal de $(G, *)$. O conjunto de todas as classes laterais à direita de N em G é denotado G/N. Nesse conjunto são válidas as seguintes propriedades para a multiplicação de subconjuntos de G:

   (i) $(aN)(bN) = (ab)N$

   (ii) $[(aN)(bN)](cN) = (aN)[(bN)(cN)]$

   (iii) $(aN)(eN) = (ae)N = aN = (ea)N = (eN)(aN)$

   (iv) $(aN)(a^{-1}N) = (aa^{-1})N = eN = (a^{-1}a)N = (a^{-1}N)(aN)$

   O grupo formado pelo conjunto G/N e pela multiplicação de subconjuntos de G é denominado *Grupo Quociente* de G por N.

9. **Homomorfismos e Isomorfismos de Grupos**

   Sejam os grupos $(G, *)$ e $(G', \cdot)$ e $f : G \to G'$ uma função de G em G'. Dizemos que f é um *homomorfismo* se:

$$f(x * y) = f(x) \cdot f(y), \forall x, y \in G$$

   Se o homomorfismo $f : G \to G'$ for bijetivo dizemos que f é um *isomorfismo* e, nesse caso, dizemos que G é isomorfo a G' e denotamos por $G \simeq G'$.

1.2 Fatos

1. ***Teorema de Lagrange***

   Se $(G, *)$ é um grupo finito e $(H, *)$ é um subgrupo de $(G, *)$, então a ordem de $(H, *)$, $|H|$, é um divisor da ordem de $(G, *)$, $|G|$; em particular, $|G| = |H|.|G : H|$.

2. O conjunto S_n, formado pelas bijeções em um conjunto com n elementos, é um grupo em relação à operação composição de funções.

3. ***Teorema de Cayley***

   Se $(G, *)$ é um grupo de ordem $|G| = n$ então $(G, *)$ é isomorfo a um subgrupo do grupo S_n.

Capítulo 2

Grupos de Simetria

Neste capítulo, focaremos nosso estudo nas definições e propriedades dos Grupos de Simetria para que possamos compreender o Grupo Diedral, grupo base para desenvolvimento do Código em D_5.

2.1 Definições

1. **Permutação**

   Uma *permutação* σ do conjunto S é uma função de S em S bijetiva, ou seja:

   $\sigma : S \to S : \sigma$ bijetiva

2. **Grupo de Permutação e Grupo de Simetria**

   Um grupo $(G, *)$ em que $G = \{\sigma : S \to S : \sigma \text{ bijetiva } \}$ e $*$ é a operação composição de funções "$\circ$", é denominado *Grupo de Permutações* do conjunto S. Se $S = \{1, 2, 3, ..., n\}$, $n \in \mathbb{Z}_{\geq 1}$, denotaremos esse grupo por S_n e ele será denominado *Grupo de Simetria*. A ordem de S_n é igual a $n!$, ou seja $|S_n| = n!$.

3. **Ciclo e Notação cíclica**

   Sejam a_1, a_2, a_3,..., a_k, com $k \geq 1$, elementos distintos do conjunto $S = \{1, 2, 3, ..., n\}$, $n \in \mathbb{Z}_{\geq 1}$. Então $\delta = (a_1, a_2, a_3, ..., a_k)$ representa a permutação em S_n que troca a_1 por a_2, a_2 por a_3,..., a_{k-1} por a_k e a_k por a_1. Essa permutação é denominada *ciclo* e, como δ possui k elementos, dizemos que δ é um *ciclo de comprimento k* ou ainda um *k-ciclo*. Um 2-ciclo é chamado *Transposição*.

4. **Ciclos Disjuntos**

   Sejam $\sigma = (i_1, i_2, ..., i_r)$ e $\tau = (j_1, j_2, ..., j_s)$, com $r, s \in \mathbb{Z}_{\geq 1}$, dois ciclos de S_n. Dizemos que σ e τ são dois *ciclos disjuntos* se $\{i_1, i_2, ..., i_r\} \cap \{ j_1, j_2, ..., j_s \} = \emptyset$.

2.2 Exemplos

Exemplo 2.2.1. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ *denota a permutação* $\alpha : \{1,2,3,4\} \to \{1,2,3,4\}$ *definida por* $\alpha(1) = 3$, $\alpha(2) = 4$, $\alpha(3) = 2$, $\alpha(4) = 1$. *Em notação de ciclos,* α *pode ser escrita na forma* $\alpha = (1,3,2,4)$.

Exemplo 2.2.2. $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 3 & 6 \end{pmatrix}$ *denota a permutação* $\beta : \{1,2,3,4,5,6\} \to \{1,2,3,4,5,6\}$ *definida por* $\beta(1) = 4$, $\beta(2) = 1$, $\beta(3) = 5$, $\beta(4) = 2$, $\beta(5) = 3$, $\beta(6) = 6$. *Em notação de ciclos,* β *pode ser escrita na forma* $\beta = (1,4,2)(3,5)(6)$ *ou* $\beta = (1,4,2)(3,5)$.

2.3 Fatos

1. Ciclos disjuntos comutam.

   Demonstração em [4], pág. 201.

2. Toda permutação em S_n pode ser escrita como um produto de ciclos disjuntos.

   Demonstração em [1], pág. 221.

3. Toda permutação em S_n é um produto de transposições.

   Demonstração em [1], pág. 221.

4. A permutação identidade em S_n não é produto de uma quantidade ímpar de transposições.

   Demonstração em [1], pág. 222.

5. Nenhuma permutação em S_n é simultaneamente par e ímpar.

   Demonstração em [1], pág. 223.

6. Define-se a paridade de uma permutação σ de acordo com a paridade do número de transposições na qual σ pode ser escrita. O conjunto das permutações pares formam um grupo. Tal grupo é denominado *Grupo Alternado* e é denotado por A_n.

7. A_n é um subgrupo normal de ordem $\frac{n!}{2}$ e índice 2. Deste modo, A_n é um grupo simples, ou seja, admite somente os subgrupos triviais.

   Demonstração em [1], pág 224.

Capítulo 3

Código baseado em D_5

Neste capítulo, exibiremos o Grupo Diedral na primeira seção. Em seguida, estudaremos o caso particular $n = 5$, estabelecendo notações e descrevendo a tábua de operação de D_5 objetivando a preparação para a construção do código.

3.1 Grupo Diedral D_n

Uma importante família de exemplos de grupos é a classe de grupos cujos elementos são simetrias de figuras geométricas. A subclasse mais simples é aquela em que essas figuras são polígonos regulares.

Para descrever essas simetrias, denotamos os vértices do polígono regular escolhido por 1, 2, 3,..., n, consecutivamente, ($n \geq 3$ e $n \in \mathbb{Z}_0$), e o conjunto das simetrias por D_n. As simetrias serão movimentos rígidos do polígono, dados por rotações e reflexões. Em D_n serão:

- n rotações de $\frac{2\pi i}{n}$ radianos, $0 \leq i \leq n-1$, em torno do centro;
- n reflexões sobre os n eixos de simetria, onde:

  (i) se *n é ímpar*, cada eixo de simetria intercepta um vértice e o ponto médio do lado oposto a esse vértice;

  (ii) se *n é par*, existem $\frac{n}{2}$ eixos de simetria que interceptam dois vértices opostos e $\frac{n}{2}$ que bissectam perpendicularmente dois lados opostos.

O grupo D_n é denominado *grupo diedral de grau n* e sua ordem é dada pela cardinalidade do conjunto de simetrias em um polígono regular de n vértices, logo $|D_n| = 2n$.

Denotando as rotações por r e as reflexões por w, teremos em D_n:

(i) $w^2 = w \circ w = e$ e $r^n = e$

(ii) $[w] = \{w^m : m \in \mathbb{Z}\} = \{e, w\}$ e $[r] = \{r^m : m \in \mathbb{Z}\} = \{e, r, r^2, r^3, ..., r^{n-1}\}$ Onde: $r^m = r \circ r (m = 2) e r^m = r^{m-1} \circ r (m > 2)$.

Desta forma, temos os seguintes fatos:

1. $1, r, r^2, ..., r^{n-1}$ são todos distintos, $r^n = 1$ e, assim, $|r| = n$;

2. $|w| = 2$;

3. $w \neq r^i$, para todo i, $1 \leq i \leq n-1$;

4. $rw = wr^{-1}$, ou seja, r e w não comutam e, portanto, D_n é um grupo não-abeliano;

5. $wr^i \neq wr^j$, para todos i e j, $0 \leq i, j \leq n-1$, com $i \neq j$, assim

$$D_n = \{1, r, r^2, ..., r^{n-1}, w, wr, wr^2, ..., wr^{n-1}\}$$

   isto é, cada elemento de D_n pode ser escrito unicamente na forma $w^k r^i$ para $k \in \{0, 1\}$ e $0 \leq i \leq n-1$;

6. $r^i w = wr^{-i}$, para todo i, $0 \leq i \leq n$.

Exemplo 3.1.1. *Para $n = 3$, temos o grupo D_3, que consiste das 6 simetrias do triângulo equilátero: 3 rotações no sentido anti-horário de $0, \frac{2\pi}{3}$ e $\frac{4\pi}{3}$ radianos em torno do centro, denotadas por r_0, r_1, r_2, respectivamente, e 3 reflexões sobre seus eixos de simetria (linhas tracejadas), que correspondem as retas que passam pelo baricentro e por cada vértice do triângulo, denotadas por s, t, u.*

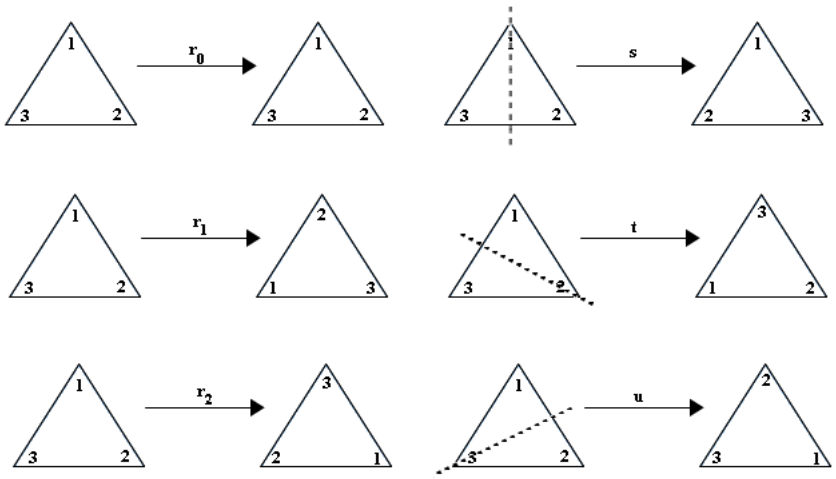

Figura 3.1: *Simetrias em D_3*

A tábua de composição desse grupo é dada por:

$\circ$	r_0	r_1	r_2	s	t	u
r_0	r_0	r_1	r_2	s	t	u
r_1	r_1	r_2	r_0	u	s	t
r_2	r_2	r_0	r_1	t	u	s
s	s	u	t	r_0	r_1	r_2
t	t	s	u	r_1	r_0	r_2
u	u	t	s	r_2	r_1	r_0

Tabela 3.1: Tábua de composição de D_3

De acordo com a tabela 3.1 temos:

- r_0 *é o elemento neutro (ou identidade);*
- $r_1^2 = r_1 \circ r_1 = r_2$

  $s \circ r_1 = u$

  $s \circ r_1^2 = t$

  Assim, $D_3 = \{r_1^0, r_1^1, r_1^2, s, s \circ r_1, s \circ r_1^2\}$

  Ou seja, D_3 *é gerado por* r_1 *e* s ($D_3 = \langle r_1, s \rangle$);
- D_3 *não é abeliano.*

Exemplo 3.1.2. *Para* $n = 4$*, temos o grupo* D_4*, que consiste das 8 simetrias do quadrado: 4 rotações no sentido anti-horário de* $0, \frac{\pi}{2}$*,* π *e* $\frac{3\pi}{2}$ *radianos em torno do centro, denotadas por* r_0, r_1, r_2, r_3*, respectivamente, e 4 reflexões sobre seus eixos de simetria (linhas tracejadas), 2 que correspondem as retas que bissectam perpendicularmente dois lados opostos e 2 que interceptam vértices opostos, denotadas por* s, t, u, v*.*

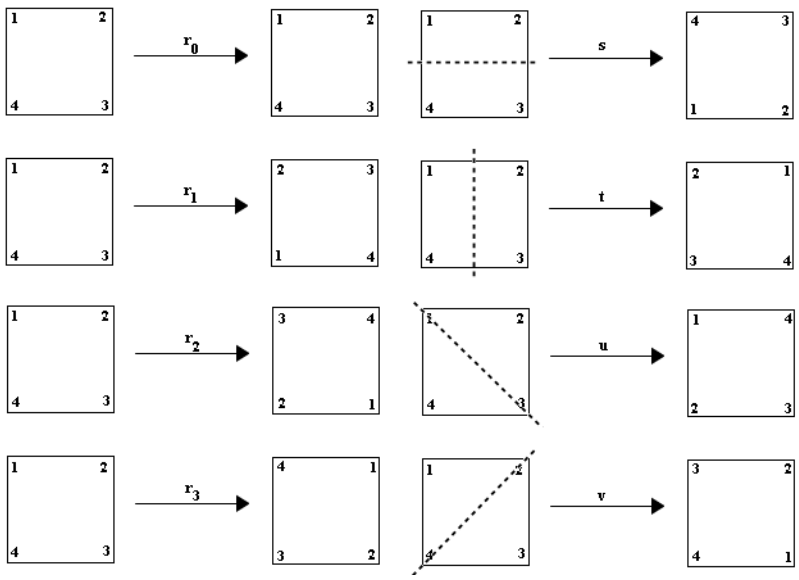

Figura 3.2: *Simetrias em* D_4

A tábua de composição desse grupo é dada por:

$\circ$	r_0	r_1	r_2	r_3	s	t	u	v
r_0	r_0	r_1	r_2	r_3	s	t	u	v
r_1	r_1	r_2	r_3	r_0	v	u	s	t
r_2	r_2	r_3	r_0	r_1	t	s	v	u
r_3	r_3	r_0	r_1	r_2	u	v	t	s
s	s	u	t	v	r_0	r_2	r_1	r_2
t	t	v	s	u	r_2	r_0	r_3	r_1
u	u	t	v	s	r_3	r_1	r_0	r_2
v	v	s	u	t	r_1	r_3	r_2	r_0

Tabela 3.2: Tábua de composição de D_4

De acordo com a tabela 3.2 temos:

- r_0 *é o elemento neutro (ou identidade);*
- $r_1^2 = r_1 \circ r_1 = r_2$

  $r_1^3 = r_1^2 \circ r_1 = r_2 \circ r_1 = r_3$

  $s \circ r_1 = u$

  $s \circ r_1^2 = t$

  $s \circ r_1^3 = v$

  Assim, $D_4 = \{r_1^0, r_1^1, r_1^2, r_1^3, s, s \circ r_1, s \circ r_1^2, s \circ r_1^3\}$

  Ou seja, D_4 *é gerado por* r_1 *e* s $(D_4 = \langle r_1, s \rangle)$*;*

- *D_4 não é abeliano.*

3.2 Grupo D_5

O grupo D_5 consiste das 10 permutações do pentágono regular: 5 rotações no sentido anti-horário de $0, \frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}$ e $\frac{8\pi}{5}$ radianos em torno do centro, denotadas por r_0, r_1, r_2, r_3, r_4, respectivamente, e 5 reflexões sobre seus eixos de simetria S_1, S_2, S_3, S_4, S_5 (3.3), denotadas por r_5, r_6, r_7, r_8, r_9, respectivamente.

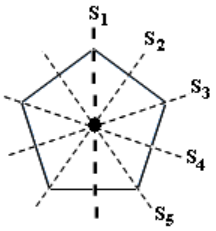

Figura 3.3: *Eixos de simetria de um pentágono regular*

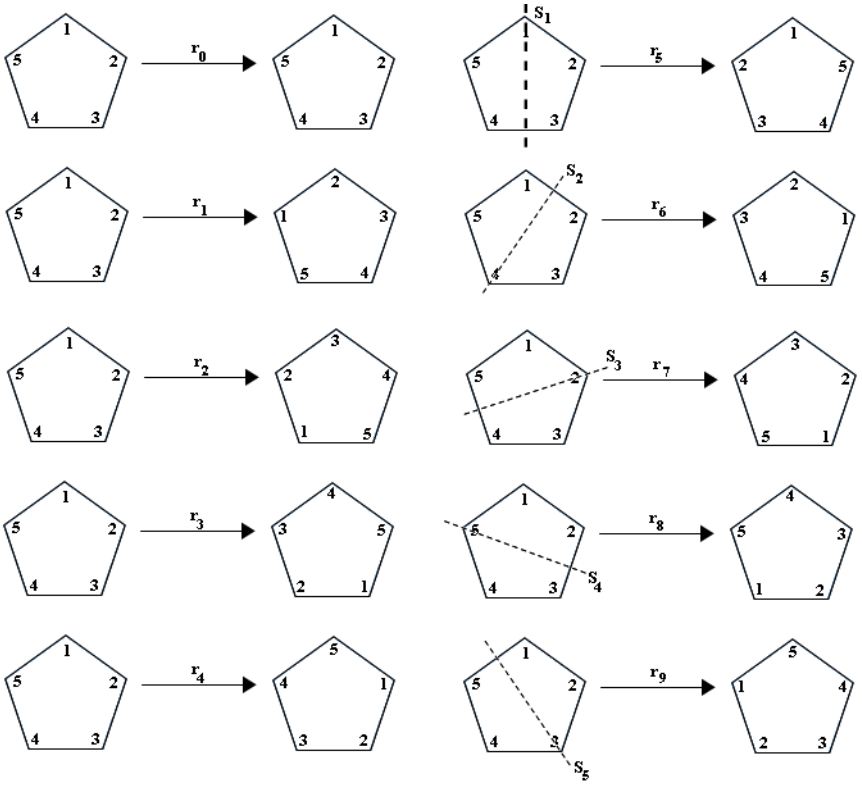

Figura 3.4: *Simetrias em D_5*

A tábua de composição de simetrias desse grupo é dada por:

$\circ$	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9
r_0	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9
r_1	r_1	r_2	r_3	r_4	r_0	r_6	r_7	r_8	r_9	r_5
r_2	r_2	r_3	r_4	r_0	r_1	r_7	r_8	r_9	r_5	r_6
r_3	r_3	r_4	r_0	r_1	r_2	r_8	r_9	r_5	r_6	r_7
r_4	r_4	r_0	r_1	r_2	r_3	r_9	r_5	r_6	r_7	r_8
r_5	r_5	r_9	r_8	r_7	r_6	r_0	r_4	r_3	r_2	r_1
r_6	r_6	r_5	r_9	r_8	r_7	r_1	r_0	r_4	r_3	r_2
r_7	r_7	r_6	r_5	r_9	r_8	r_2	r_1	r_0	r_4	r_3
r_8	r_8	r_7	r_6	r_5	r_9	r_3	r_2	r_1	r_0	r_4
r_9	r_9	r_8	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0

Tabela 3.3: Tábua de composição de D_5

Por meio da tabela 3.3 verifica-se que em D_5 temos:

- r_0 é o elemento neutro (ou identidade);
- $r_0^{-1} = r_0$

  $r_1^{-1} = r_4$

  $r_2^{-1} = r_3$

  $r_3^{-1} = r_2$

  $r_4^{-1} = r_1$

  $r_5^{-1} = r_5$

  $r_6^{-1} = r_6$

  $r_7^{-1} = r_7$

  $r_8^{-1} = r_8$

  $r_9^{-1} = r_9$
- $r_1^2 = r_1 \circ r_1 = r_2$

  $r_1^3 = r_1^2 \circ r_1 = r_2 \circ r_1 = r_3$

  $r_1^4 = r_1^3 \circ r_1 = r_3 \circ r_1 = r_4$

  $r_5 \circ r_1 = r_9$

$r_5 \circ r_1^2 = r_5 \circ r_2 = r_8$

$r_5 \circ r_1^3 = r_5 \circ r_3 = r_7$

$r_5 \circ r_1^4 = r_5 \circ r_4 = r_6$ Assim, $D_5 = \{r_1^0, r_1^1, r_1^2, r_1^3, r_1^4, r_5, r_5 \circ r_1, r_5 \circ r_1^2, r_5 \circ r_1^3, r_5 \circ r_1^4\}$

Ou seja, D_5 é gerado por r_1 e r_5 ($D_5 = \langle r_1, r_5 \rangle$);

- D_5 não é abeliano.

3.3 Código Baseado em D_5

Em 1969, o matemático holandês J. Verhoeff desenvolveu, em sua tese de doutorado, um método simples, mas sofisticado, capaz de detectar erros singulares e ainda todos os erros de transposição adjacente, sem a necessidade de inserção de caracteres alfabéticos no código. Era, então, uma evolução da teoria dos códigos, utilizando a Álgebra abstrata através do grupo diedral D_5.

Para esta aplicação, escreveremos a composição entre as simetrias como produto de dígitos:

$$r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9 \longrightarrow 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

$$\circ \longrightarrow \bullet$$

Procedendo desta forma, a tabela de composição de simetrias em D_5 (tabela 3.3) será descrita como a seguinte tabela multiplicativa:

σ_i	$\bullet$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
σ_0	**0**	0	1	2	3	4	5	6	7	8	9
σ_1	**1**	1	2	3	4	0	6	7	8	9	5
σ_2	**2**	2	3	4	0	1	7	8	9	5	6
σ_3	**3**	3	4	0	1	2	8	9	5	6	7
σ_4	**4**	4	0	1	2	3	9	5	6	7	8
σ_5	**5**	5	9	8	7	6	0	4	3	2	1
σ_6	**6**	6	5	9	8	7	1	0	4	3	2
σ_7	**7**	7	6	5	9	8	2	1	0	4	3
σ_8	**8**	8	7	6	5	9	3	2	1	0	4
σ_9	**9**	9	8	7	6	5	4	3	2	1	0

Tabela 3.4: Tábua de multiplicação de dígitos para o código em D_5

Esse método consiste em aplicar potências de uma determinada permutação σ_i, $i = 0, 1, 2, 3, ..., 9$, em D_5, conforme a posição ocupada pelo dígito (a sequência de dígitos deve está de forma ordenada em sentido decrescente, ou seja, para uma sequência de n

dígitos, $n \in \mathbb{N}$, teremos $a_{n-1}a_{n-2}...a_1a_0$, onde a_0 é o dígito de verificação), e efetuar a operação "multiplicação"em D_5, indicada na tabela 3.4.

Assim, para uma dada sequência de dígitos $a_na_{n-1}a_{n-2}...a_1a_0$ e tomando uma determinada permutação $\sigma_i \in D_5$, o dígito de verificação será anexado de forma tal que:

$$\sigma_i^n(a_n) \bullet \sigma_i^{n-1}(a_{n-1}) \bullet ... \bullet \sigma_i^1(a_1) \bullet \sigma_i^0(a_0) = 0$$

Como sabemos que D_5 não é abeliano, temos diretamente que:

$$a \bullet \sigma_i(b) \neq b \bullet \sigma_i(a), \forall a, b \in D_5 \tag{3.1}$$

Esse fato demonstra que este método detecta todos os erros de dígito singular, bem como todos os erros de transposição adjacente:

- Como σ_i^k, $k \in \mathbb{N}$, é também uma permutação em D_5, todo erro único de digitação é detectado;

- Um erro de transposição adjacente, $...a_na_{n+1}... \longrightarrow ...a_{n+1}a_n...$, será detectado se, e somente se, $\sigma_i^n(a_n) \bullet \sigma_i^{n+1}(a_{n+1}) \neq \sigma_i^{n+1}(a_{n+1}) \bullet \sigma_i^n(a_n)$. Pela expressão 3.1, temos:

  $$a \bullet \sigma_i(b) \neq b \bullet \sigma_i(a)$$

  Aplicando σ_i^n em ambos os membros desta inequação, obtemos:

  $$\sigma_i^n(a \bullet \sigma_i(b)) \neq \sigma_i^n(b \bullet \sigma_i(a))$$

  $$\sigma_i^n(a) \bullet \sigma_i^{n+1}(b) \neq \sigma_i^n(b) \bullet \sigma_i^{n+1}(a)$$

  O que confirma a detecção dos erros de trasnposição adjacente.

O grupo D_5 desempenha um importante papel na elaboração de códigos detectores de erros, visto que ele é o único grupo de ordem 10 capaz de detectar os erros singulares e de trasnposição adjacente, os quais estão entre os erros de digitação mais frequentes, como mostra a seguinte tabela:

Exemplo 3.3.1. *Para exemplificar a aplicação desse método, tomaremos a sequência de dígitos* 7891962026756 *que corresponde ao código de barras de determinado produto, cujo dígito de verificação é* 6*. Determinaremos esse dígito se o produto fosse identificado com o código baseado em* D_5*. Para tanto, utilizaremos a permutação* $\sigma_2 = (0, 2, 4, 1, 3)(5, 7, 9, 6, 8)$.

Como n = 12, teremos:

$\sigma_2^{12}(a_{12}) \bullet \sigma_2^{11}(a_{11}) \bullet \sigma_2^{10}(a_{10}) \bullet \sigma_2^9(a_9) \bullet \sigma_2^8(a_8) \bullet \sigma_2^7(a_7) \bullet \sigma_2^6(a_6) \bullet \sigma_2^5(a_5) \bullet \sigma_2^4(a_4) \bullet \sigma_2^3(a_3) \bullet$
$\bullet\sigma_2^2(a_2) \bullet \sigma_2^1(a_1) \bullet \sigma_2^0(a_0) = 0$ *(3.2)*

Tipo de erro	Forma	Frequência
Singular	$a \to b$	79,1%
Transposição adjacente	$ab \to ba$	10,2%
Trasnposição de salto	$abc \to cba$	0,8%
Gêmeo	$aa \to bb$	0,5%
Salto gêmeo	$aca \to bcb$	0,3%
Outros	-	9,1%

Tabela 3.5: Tipos de erros de digitação e suas frequências segundo Verhoeff

σ_2 é uma rotação em D_5, então, utilizando a tabela 3.4:

$\sigma_2^2 = \sigma_2 \bullet \sigma_2 = 2 \bullet 2 = 4$
$\sigma_2^3 = \sigma_2^2 \bullet \sigma_2 = 4 \bullet 2 = 1$
$\sigma_2^4 = \sigma_2^2 \bullet \sigma_2^2 = 4 \bullet 4 = 3$
$\sigma_2^5 = \sigma_2^4 \bullet \sigma_2 = 3 \bullet 2 = 0$
$\sigma_2^{12} = \sigma_2^5 \bullet \sigma_2^5 \bullet \sigma_2^2 = 0 \bullet 0 \bullet \sigma_2^2 = \sigma_2^2$

Assim, podemos simplificar a expressão 3.2 e obter:

$\sigma_2^2(a_{12}) \bullet \sigma_2^1(a_{11}) \bullet \sigma_2^0(a_{10}) \bullet \sigma_2^4(a_9) \bullet \sigma_2^3(a_8) \bullet \sigma_2^2(a_7) \bullet \sigma_2^1(a_6) \bullet \sigma_2^0(a_5) \bullet \sigma_2^4(a_4) \bullet \sigma_2^3(a_3) \bullet$
$\bullet\sigma_2^2(a_2) \bullet \sigma_2^1(a_1) \bullet \sigma_2^0(a_0) = 0$

$\sigma_2^2(7)\bullet\sigma_2^1(8)\bullet\sigma_2^0(9)\bullet\sigma_2^4(1)\bullet\sigma_2^3(9)\bullet\sigma_2^2(6)\bullet\sigma_2^1(2)\bullet\sigma_2^0(0)\bullet\sigma_2^4(2)\bullet\sigma_2^3(6)\bullet\sigma_2^2(7)\bullet\sigma_2^1(5)\bullet\sigma_2^0(a_0) = 0$

$(4\bullet7)\bullet(2\bullet8)\bullet(0\bullet9)\bullet(3\bullet1)\bullet(1\bullet9)\bullet(4\bullet6)\bullet(2\bullet2)\bullet(0\bullet0)\bullet(3\bullet2)\bullet(1\bullet6)\bullet(4\bullet7)\bullet(2\bullet5)\bullet(0\bullet a_0) = 0$

$$6 \bullet 5 \bullet 9 \bullet 4 \bullet 5 \bullet 5 \bullet 4 \bullet 0 \bullet 0 \bullet 7 \bullet 6 \bullet 7 \bullet a_0 = 0$$

$$4 \bullet a_0 = 0$$

$$a_0 = 4^{-1}$$

$$a_0 = 1$$

Assim, o dígito de verificação utilizando o código em D_5 seria o 1 e, o código do produto, 7891962026751.

Referências Bibliográficas

[1] HUNGERFORD, Thomas W. *Abstract Algebra An Indroduction*. 575 pp. Estados Unidos da América: Saunders College Publishing, 1990.

[2] DUMMIT, DavidS,; FOOTE, Richard M. *Abstract Algebra*.Ed. 3. 945 pp. Estados Unidos da América: John Wiley and Sons, 2004.

[3] GONÇALVES, Adilson. *Introdução á Álgebra*. Ed. 3. 194 pp. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1995.

[4] DOMINGUES, Hygino H.; IEZZI, Gelson. *Álgebra Moderna*. Ed. 4. 368 pp. São Paulo: Atual, 2003.

[5] SOARES, Danielle de Carvalho. *Introdução aos códigos verificadores de erros*. Sergipe: Universidade Federal de Sergipe, 2011.