Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Códigos de Grupo Gerado por Grupos de Reflexões Finitos

por

Cassio André Sousa da Silva

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Setembro/2003
João Pessoa - Pb

Códigos de Grupo Gerado por Grupos de Reflexões Finitos

por

Cassio André Sousa da Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. Orlando Stanley Juriaans - IME-USP

Prof. Dr. Hélio Pires de Almeida - UFPB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Setembro/2003

Agradecimentos

1. Agradeço a Deus, pois sem ele nada seria possível; a minha família em Belém: José Luiz, Benedita Sousa e Rita de Cássia que sempre me apoio em toda trajetória estudantil; à minha esposa Neurimá e à minha filha Carolina que compreenderam tantas vezes a minha ausência.

2. Ao meu orientador e amigo professor, Dr. *Antônio de Andrade e Silva*, pela eficaz *orientação* nesta dissertação, a sua colaboração e ao seu incentivo, e pela paciência que tivera ao longo deste mestrado.

3. Ao professor Dr. Marivaldo P. Matos, que nunca se negou, quando o procurei para expor as minhas dúvidas, e aos colegas do Curso de Mestrado.

4. Aos colegas do curso de mestrado, em especial aos amigos Waldir Barbaresco, Joelma Ananias, Aroldo José de Oliveira, Dércio Braga Santos, Flávio Alexandre Falcão e Marcus Antônio Alcântara

5. A Sônia, pela competência e presteza no atendimento de secretaria.

6. Ao Meu Cunhado Arnaldo pelo suporte financeiro para a realização do Curso de Mestrado.

7. Não poderia deixar de citar seu Ivan da limpeza, pelos constantes favores que fizera.

8. Ao amigo JB pelos inesquecíveis momentos de descontração.

Dedicatória

À famíla que amo:
minha esposa Neurimá
e
à minha filha Carolina.

Resumo

Códigos de Grupo do tipo Slepian gerado por grupos de reflexões finitas são considerados. Os resultados clássicos de códigos de grupos são uma generalização dos conhecidos códigos de modulação de Slepian. Estes resultados mostram que o problema do vetor inicial para estes códigos tem uma solução canônica que pode ser facilmente calculada. Isto permite uma enumeração de todos os códigos neste sentido restrito e resolve o problema do vetor inicial para todos os grupos de reflexão finita. São dados fórmulas para calcular a cardinalidade e a mínima distância destes códigos.

Abstract

Slepian-type group codes generated by finite Coxeter groups are considered. The resulting class of group codes is a generalization of the well-known permutation modulation codes these of Slepian. It shown that a restricted initial-point problem for these codes has a canonical solution that can easily be computed. This allows one to enumerate all optimal group codes in this restricted sense and essentially solves the initial-point problem for all finite reflection groups. Formulas for the cardinality and the minimum distance of such codes are give

Notação

$S|_W$ - aplicação S restrita ao conjunto W

$B_\epsilon(\mathbf{x}_0)$ - bola aberta de raio ϵ e centro $\mathbf{x}_0$

aH - classe lateral à esquerda

C - código

(M, n) - código de grupo em $\mathbb{R}^n$

F - corpo

$V - X$ - complementar

$S^\perp$ - complemento ortogonal

$\mathcal{L}(V, V)$ - conjunto de operadores lineares de V

$\mathbb{N}$ - conjunto dos números naturais

$\mathbb{Z}$ - conjunto dos números inteiros

$\mathbb{R}$ - conjunto dos números reais

$\mathbb{C}$ - conjunto dos números complexos

Π_P - conjunto de raízes passivas

$GL(V)$ - conjunto dos operadores lineares invertíveis $\mathcal{L}(V, V)$

$GL_n(F)$ - conjunto das matrizes invertíveis ordem n

$M_n(F)$ - conjunto das matrizes de ordem n

$O(V)$ - conjunto dos operadores ortogonais de $GL(V)$

$O(n, \mathbb{R})$ - conjunto das matrizes ortogonais com entradas em $\mathbb{R}$

V_G - conjunto dos elementos do $\mathbb{R}^n$ que são fixados por G

$V_G^\perp$ - conjunto dos elementos ortogonais a V_G

k - dimensão do código

d^2 - distância quadrática

$d_{\min}$ - distância mínima

$S_\epsilon(\mathbf{x}_0)$ - esfera de raio ϵ e centro $\mathbf{x}_0$

$F^{\mathbb{I}}$ - espaço de seqüências

G_x - estabilizador de x

X - fecho de X

∂X - fronteira de X

$M(H, G)$ - grupo das matrizes monomiais

$\frac{G}{H}$ - grupo quociente

S_n - grupo de simetria

H_2^m - grupo diedral de ordem $2m$

$[.]$ - índice

$\simeq$ - isomorfismo

X^0 - interior de X

$\mathbf{M}^{-1}$ - matriz invertível

$\mathbf{M}^t$ - matriz transposta

DP - matriz monomial

$\|.\|$ - norma

$\mathbf{P}_n$ - matríz de Permutação

ker - núcleo do homomorfismo

T - operador linear

$O(x)$ - órbita do elemento

$o(a)$ - ordem do elemento

$|.|$ - ordem do grupo

$\mathbb{R}^n$ - produto cartesiano de $\mathbb{R}$ (n cópias)

$\langle . \rangle$ - produto interno

$H \rtimes K$ - produto semi-direto de H por K

$\backsim$ - relação de equivalência

$\oplus$ - soma direta

$\leq$ - subgrupo

$\langle a \rangle$ - subgrupo gerado pelo elemento a

$\trianglelefteq$ - subgrupo normal

tr - traço da matriz

Δ - sistema de raízes

R - taxa de informação do código

$\dot{\cup}$ - união disjunta

Sumário

Introdução

O principal objetivo desta dissertação é a construção de códigos de grupos ótimos gerado por grupos de reflexões finitas ou grupos de Coxeter irredutíveis. Esta construção é baseada no problema do vetor inicial. Este problema é resolvido a partir da utilização de um sistema de vetores com características próprias, chamado de sistema de raízes, o qual é constituido de outros subconjuntos, entre eles, as raízes passivas que dará o passo fundamental para a escolha do vetor inicial. Desta forma a distância mínima $d_{\min}(C)$ do código pode ser calculada pela escolha deste vetor inicial.

O primeiro tratamento compreensível de grupo de reflexão finita foi dado por Coxeter em 1934, que classificou completamente todos grupos e deduziu várias de suas propriedades usando principalmente métodos geométricos, por esta razão podemos chamar grupo de reflexão finito de grupos de Coxeter. Outra abordagem de natureza mais algébrica foi apresentada no relatório feito por P. Cartier no seminário de Chevalley. O leitor interessado em mais detalhes pode consultar [2].

Código de grupos, que recentemente tem sido chamado de conjunto de sinais geometricamente uniforme, pode ser visto como uma combinação de codificação e modulação. Os resultados clássicos de código de grupos são generalizações dos já bem conhecidos códigos de modulação de permutação introduzidos por Slepian [14] há mais de 25 anos, onde verificamos que o problema do vetor inicial restrito a grupos de Coxeter tem uma solução que pode ser facilmente calculada.

Nesta dissertação apresentamos os conceitos básicos da extensiva teoria de grupos de reflexão finita, dando ênfase ao conhecido grupo diedral, e aos grupos de reflexão $\mathcal{A}_n$ e $\mathcal{B}_n$ que são ações do grupo de permutação nos vetores da base canônica do $\mathbb{R}^n$, o leitor interessado em mais grupos de reflexão pode consultar [7].

Esta dissertação tem como base o artigo de Mittelholzer e Lahtonen [12].

No capítulo 1, faremos uma abordagem sobre a teoria de grupos e alguns resultados

básicos de álgebra linear e grupos de reflexões finitas.

No capítulo 2, começamos com a definição de região fundamental e apresentamos sistema de raízes para grupos de reflexão finita.

No capítulo 3, apresentamos os conceitos básicos da teoria de códigos.de grupos, além disso, com o objetivo de determinar de forma geral os procedimentos para a escolha do vetor inicial ótimo, mostramos como determinar estabilizador $G_{\mathbf{y}}$ a partir de um vetor $\mathbf{y}$ qualquer do $\mathbb{R}^n$ utilizando para isto as reflexões dos grupos de Coxeter irredutíveis. O Teorema 3.3 determina a distância mínima para o código $C = O(\mathbf{x}_0)$ e em seguida, o seu corolário relaciona distância e vetor inicial ótimo; mostramos que as regiões de decodificação são unicamente determinadas pelo estabilizador $G_{\mathbf{x}_0}$. Esta propriedade assegura que existe uma única solução para o problema do vetor inicial, quando o estabilizador é fixado, o Teorema 3.4 mostra que a região de decisão F de um grupo de reflexão finita é única, a menos de isometria, contudo, esta propriedade não é válida para grupos de isometria arbitrária, o leitor interessado em um exemplo pode consultar [12]. Com o objetivo de melhor entendimento da teoria, finalizamos este capítulo dando alguns exemplos para a determinação do vetor inicial.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos algumas definições e resultados básicos da teoria de grupos e que serão necessários para os capítulos subsequentes. O leitor interessado em mais detalhes pode consultar [4, 6, 13].

1.1 Grupos

Um conjunto não vazio G munido com uma operação binária $(a, b) \longmapsto a * b$ é um *grupo* se as seguintes condições são satisfeitas:

1. A operação é associativa: $a * (b * c) = (a * b) * c$, $\forall a, b, c \in G$.

2. Existe um elemento neutro, isto é, $\exists\, e \in G$ tal que $e * a = a * e = a$, $\forall a \in G$.

3. Todo elemento possui um elemento inverso, isto é, $\forall\ a \in G$, $\exists\ b \in G$ tal que $a * b = b * a = e$.

O grupo é abeliano ou comutativo se também vale:

4. A operação é comutativa, isto é, $a * b = b * a$, $\forall\ a, b \in G$.

Para simplificar a notação usaremos ab em vez de $a * b$.

Seja G um grupo. Dizemos que G é *finito* se ele contém um número finito de elementos. Caso contrário, ele é *infinito*. A *ordem* ou *cardinalidade* de G, denotada por $|G|$, é o número de elementos de G.

Exemplo 1.1 *Seja $M_n(\mathbb{R})$ o conjunto de todas as matrizes $n \times n$ sobre $\mathbb{R}$. Então*

$$\mathrm{GL}(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$$

com a operação usual de multiplicação de matrizes é um grupo não abeliano, chamado grupo linear geral. *De fato, sejam $\mathbf{A}, \mathbf{B} \in \mathrm{GL}(n, \mathbb{R})$. Então, pelo Teorema de Binet,*

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B}) \neq 0.$$

Logo, $\mathbf{AB} \in \mathrm{GL}(n, \mathbb{R})$. Assim, o produto usual de matrizes é uma operação binária em $\mathrm{GL}(n, \mathbb{R})$. É claro que esta operação binária é associativa e

$$\mathbf{I} \in M_n(\mathbb{R})$$

é o elemento identidade de $\mathrm{GL}(n, \mathbb{R})$. Finalmente, se

$$\mathbf{A} \in M_n(\mathbb{R})$$

é tal que $D = \det(\mathbf{A}) \neq 0$, então

$$\mathbf{A}^{-1} = \frac{1}{D} \operatorname{adj}(\mathbf{A})$$

é a inversa de A e

$$\det(\mathbf{A}^{-1}) = \frac{1}{\det(\mathbf{A})} \neq 0.$$

Assim,

$$\mathbf{A}^{-1} \in \mathrm{GL}(n, \mathbb{R}) \ \ e \ \ \mathbf{A}^{-1}\mathbf{A} = \mathbf{A}\mathbf{A}^{-1} = \mathbf{I}.$$

Se G e H são dois grupos, então o *produto direto* (*externo*) de G com H, denotado por $G \times H$, é o conjunto de todos os pares ordenados (g, h), onde $g \in G$ e $h \in H$, com a operação binária

$$(g, h) * (g', h') = (gg', hh').$$

É fácil mostrar que $G \times H$ é um grupo com elemento identidade (e, e) e o elemento inverso de (g, h) é (g^{-1}, h^{-1}). Assim, $G^2 = G \times G$. Generalizando, temos

$$G^n = G \times G \times \cdots \times G.$$

Um subconjunto não vazio H de um grupo G é um *subgrupo* de G, denotado por $H \leq G$, quando com a operação herdada de G, H é um grupo.

Proposição 1.1 *Sejam G um grupo e H um subconjunto não vazio de G. Então H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas*:

1. *Para todos $h_1, h_2 \in H$, tem-se $h_1 h_2 \in H$.*

2. *Para todo $h \in H$, tem-se $h^{-1} \in H$.* ■

Sejam X um subconjunto não vazio de G e

$$\mathcal{F} = \{H : H \leq G \text{ e } X \subseteq H\}.$$

Então

$$\langle X \rangle = \bigcap_{H \in \mathcal{F}} H$$

é o menor subgrupo de G contendo X e chamado o *subgrupo gerado* por X. Se X é um conjunto finito, digamos

$$X = \{x_1, \ldots, x_n\},$$

denotaremos $\langle X \rangle$ por

$$\langle X \rangle = \langle x_1, \ldots, x_n \rangle.$$

Proposição 1.2 *Sejam G um grupo e X um subconjunto não vazio de G. Então*

$$\langle X \rangle = \left\{ \prod_{i=1}^{n} x_i : n \in \mathbb{N} \text{ e } x_i \in X \cup X^{-1}, i = 1, \ldots, n \right\},$$

onde $X^{-1} = \{x^{-1} : x \in X\}$. ■

Seja G um grupo. Se existir $a \in G$ tal que

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\},$$

dizemos que G é um *grupo cíclico*.

Uma *partição* de um conjunto não vazio Ω é um conjunto

$$P(\Omega) = \{\Gamma : \Gamma \subset \Omega, \Gamma \neq \varnothing\}$$

tal que as seguintes condições são satisfeitas:

1. $\Gamma_1 \cap \Gamma_2 = \varnothing, \forall \Gamma_1, \Gamma_2 \in P(\Omega), \Gamma_1 \neq \Gamma_2$;

2. $\Omega = \bigcup_{\Gamma \in P(\Omega)} \Gamma$.

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, o conjunto

$$aH = \{ah : \forall h \in H\}$$

é chamado a *classe lateral à esquerda* de H em G determinada por a. De modo semelhante, podemos definir a classe lateral à direita Ha de H em G. O conjunto de todas as classes laterais à esquerda de H em G formam uma partição de G, que denotamos por $\frac{G}{H}$.

Dados $a, b \in G$, dizemos que a *é congruente a* b *módulo* H se $a^{-1}b \in H$, que denotamos por $a \equiv b \pmod{H}$. É fácil verificar que $\equiv$ é uma relação de equivalência em G e que a classe de equivalência determinada por a é igual a classe lateral à esquerda aH. O elemento a é chamado um *representante* da classe de equivalência. É também fácil verificar que existe uma correspondência biunívoca entre o conjunto das classes laterais à esquerda de H em G e o conjunto das classes laterais à direita de H em G. A cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de H em G é chamado o *índice* de H em G, que denotamos por $[G : H]$.

Teorema 1.1 (Lagrange) *Sejam G um grupo e H um subgrupo de G. Então $|G| = |H|[G : H]$. Em particular, se G é finito, então $|H| \mid |G|$ e $[G : H] \mid |G|$.* ■

Um subgrupo H de um grupo G é chamado *normal* de G, em símbolos $H \trianglelefteq G$, se

$$aha^{-1} \in H, \forall a \in G, h \in H.$$

Neste caso, $\frac{G}{H}$ com a operação binária $(aH)(bH) = abH$ é um grupo.

Sejam G e H dois grupos. Uma função φ de G em H é um *homomorfismo de grupos* se

$$\varphi(ab) = \varphi(a)\varphi(b),$$

para todos $a, b \in G$. Neste caso, a *imagem* de φ é o conjunto

$$\begin{aligned} \operatorname{Im}\varphi &= \{h : h = \varphi(g) \text{ para algum } g \in G\} \\ &= \{\varphi(g) : g \in G\}. \end{aligned}$$

O *núcleo* de φ é o conjunto

$$\ker\varphi = \{g \in G : \varphi(g) = e\}.$$

É fácil verificar que $\operatorname{Im}\varphi$ é um subgrupo de H e $\ker\varphi$ é um subgrupo normal de G.

Um homomorfismo de grupos $\varphi : G \longrightarrow H$ é um *isomorfismo* se φ é bijetora. Quando existir um isomorfismo entre G e H dizemos que G e H são *isomorfos* e denotamos por $G \simeq H$. Um *endomorfismo* de um grupo G é um homomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\mathrm{End}\,(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um homomorfismo}\}.$$

Um *automorfismo* de um grupo G é um isomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\mathrm{Aut}\,(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um isomorfismo}\}.$$

Teorema 1.2 *Sejam G, H dois grupos e $\varphi : G \longrightarrow H$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker \varphi} \simeq \mathrm{Im}\,\varphi.$$

■

Seja Ω um conjunto finito e não vazio. Então o conjunto de todas as bijeções de Ω sobre Ω, denotado por S_Ω, com a operação de composição, é chamado o *grupo de simetrias* de Ω. Qualquer subgrupo de S_Ω é chamado de *grupo de permutação*. Quando $\Omega = \{1, 2, \ldots, n\}$ denotamos S_Ω por S_n.

Uma permutação $\alpha \in S_n$ é chamada de *r-ciclo* se existirem elementos distintos

$$a_1, \ldots, a_r \in \{1, \ldots, n\}$$

tais que

$$\alpha(a_1) = a_2, \alpha\,(a_2) = a_3, \ldots, \alpha\,(a_{r-1}) = \alpha_r, \alpha(a_r) = a_1,$$

e

$$\alpha\,(b) = b, \forall b \in \{1, \ldots, n\} - \{a_1, \ldots, a_r\},$$

denotado por

$$\alpha = (a_1 \cdots a_r).$$

O número r é chamado o *comprimento* do ciclo. Os 2-ciclos são chamados de *transposições*. Seja $\beta \in S_n$ um s-ciclo, digamos

$$\beta = (b_1 \cdots b_s).$$

Dizemos que α e β são *disjuntas* se

$$\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \emptyset.$$

Proposição 1.3 *Toda permutação $\sigma \in S_n$, $\sigma \neq id$, pode ser escrita de modo único, a menos da ordem, como produto de ciclos disjuntos.*

Demosntração. Para demonstrar a proposição usaremos indução sobre n.

(Existência) Se $n = 1$ nada há para ser provado. Suponhamos que o resultado seja válida para todos os conjuntos com menos de n elementos e $n > 1$.

Como $\sigma \neq id$ temos que existe

$$a_1 \in \{1, \ldots, n\}$$

tal que $\sigma(a_1) \neq a_1$. Definimos $a_2, a_3, \ldots$ por

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{s-1}) = a_s, \ldots.$$

Sendo

$$\sigma(a_i) \in \{1, \ldots, n\}$$

temos que existe um menor inteiro $m \geq 2$ tal que

$$\sigma(a_m) = a_i$$

para algum i, com $1 \leq i < m$.

Afirmação: $i = 1$.

De fato, se $i \neq 1$, então

$$\sigma(a_m) = a_i = \sigma(a_{i-1}).$$

Como σ é injetora temos que

$$a_m = a_{i-1},$$

o que é impossível.

Seja

$$S = \{1, \ldots, n\} - \{a_1, \ldots, a_m\}.$$

Se $S = \emptyset$, então σ é um m-ciclo e acabou. Suponhamos que

$$S \neq \emptyset \text{ e } \sigma^* = \sigma|_S.$$

Então $\sigma^*(a) = \sigma(a) \in S$, para todo $a \in S$, σ^* é uma permutação em um conjunto com $n - m$ elementos e $n - m < n$. Logo, pela hipótese de indução,

$$\sigma^* = \tau_1 \cdots \tau_{r-1},$$

onde $\tau_1, \ldots, \tau_{r-1}$ são ciclos disjuntos. Como $\sigma = \sigma^* \tau_r$, onde

$$\tau_r = (a_1, \ldots, a_m)$$

temos que σ é um produto de ciclos disjuntos.

(Unicidade) Suponhamos que

$$\sigma = \tau_1 \cdots \tau_r = \gamma_1 \cdots \gamma_s,$$

com $s \geq 2$. Como

$$\gamma \cdots \gamma_s (a_1) = \sigma (a_1) \neq a_1$$

temos que existe um único γ_i tal que

$$\gamma_i (a_1) = \sigma(a_1),$$

pois os γ_j são disjuntos.

Afirmação: $\tau_r = \gamma_i$.

De fato, como $\sigma (a_1) = \gamma_i (a_1)$ e os γ_j disjuntos temos que

$$\gamma_i (\sigma (a_1)) \neq \sigma (a_1) \text{ e } \gamma_j (\sigma (a_1)) = \sigma (a_1), j \neq i.$$

Portanto,

$$\sigma (\sigma (a_1)) = \gamma_i (\sigma (a_1)),$$

isto é, $\gamma_i (a_2) = a_3$. De modo análogo, obtemos que

$$\gamma_i (a_{k-1}) = a_k, \forall k \geq 2,$$

isto é, $\tau_r = \gamma_i$.

Re-enumerando, se necessário, podemos assumir que $\tau_r = \gamma_s$. Logo,

$$\tau_1 \cdots \tau_{r-1} = \gamma_1 \cdots \gamma_{s-1}$$

Assim, pela hipótese indução, a seqüência $\tau_1, \ldots, \tau_{r-1}$ é no máximo uma re-ordenação da seqüência $\gamma_1, \ldots, \gamma_{s-1}$. Portanto, $r - 1 = s - 1$, isto é, $r = s$ e a decomposição σ é única a menos da ordem ■

Proposição 1.4 *Seja S_n um grupo de permutação. Então*:

1. *Todo elemento de S_n é um produto de transposições, isto é, $S_n = \langle T \rangle$, onde*

$$T = \{(ij) : 1 \leq i < j \leq n\}.$$

2. *$S_n = \langle X \rangle$, onde*

$$X = \{(1k) : 1 < k \leq n\} = \{(12), (13), \ldots, (1n)\}.$$

3. *$S_n = \langle Y \rangle$, onde*

$$Y = \{(k-1k) : 1 < k \leq n\} = \{(12), (23), \ldots, (n-1n)\}.$$

Demonstração. Para demostrar 1. basta notar que

$$id = (12)(12) \in \langle T \rangle \text{ e } (a_1, \ldots, a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2) \in \langle T \rangle,$$

e usar a Proposição 1.3. Para demostrar 2., basta notar que

$$(ij) = (1i)(1j)(1i), 1 \leq i < j \leq n,$$

e usar o item 1. Finalmente, para demostrar 3., basta notar que

$$(kk+1) = (1k)(1k+1)(1k)$$

e usar o item 2. ■

1.2 Ações de Grupo

Sejam G um grupo e Ω um conjunto não vazio. Dizemos que G *age* sobre Ω se existir uma aplicação

$$* : G \times \Omega \longrightarrow \Omega,$$

com $*(a, x) = ax$, tal que as seguintes condições são satisfeitas:

1. $a(bx) = (ab)x$, para todos $a, b \in G, x \in \Omega$;

2. $ex = x$, para todo $x \in \Omega$.

A aplicação $*$ é chamado a *ação* de G sobre Ω e Ω é chamado um *G-conjunto*. Se $|\Omega| = n$, então n é chamado o *grau* do G-conjunto Ω.

Exemplo 1.2 *Sejam $G = S_n$ e $\Omega = \{1, 2, \ldots, , n\}$. Então Ω é um G-conjunto sob a ação*

$$*(\sigma, i) = \sigma(i), \sigma \in S_n, i \in \Omega.$$

Observação 1.1 *Existe uma correspodência biunívoca entre o conjunto de ações de G em Ω e o conjunto de homomorfismo de G em S_Ω. De fato, seja Ω um G-conjunto. Então para cada $a \in G$ fixado, a aplicação $\varphi_a(x) = ax$ é uma permutação de Ω, pois*

$$\begin{aligned} x &= ex = (a^{-1}a)x = a^{-1}(ax) = \varphi_{a^{-1}}(ax) \\ &= \varphi_{a^{-1}}(\varphi_a(x)) = \varphi_{a^{-1}} \circ \varphi_a(x), \forall x \in \Omega. \end{aligned}$$

Logo, $\varphi_{a^{-1}} \circ \varphi_a = id$. De modo análogo, mostra-se que $\varphi_a \circ \varphi_{a^{-1}} = id$. Assim, a aplicação

$$\varphi : G \longrightarrow S_\Omega$$

dada por $\varphi(a) = \varphi_a$ é um homomorfismo, pois

$$\varphi_{ab}(x) = (ab)x = a(bx) = \varphi_a(bx) = \varphi_a(\varphi_b(x)) = \varphi_a \circ \varphi_b(x), \forall x \in \Omega.$$

Reciprocamente, suponhamos que $\varphi : G \longrightarrow S_\Omega$ é um homomorfismo. Então é fácil verificar que a aplicação

$$* : G \times \Omega \longrightarrow \Omega,$$

definida por $*(a, x) = \varphi(a)x$ é uma ação de G sobre Ω. Neste caso, dizemos que φ é uma representação por permutação *de G em S_Ω.*

Seja Ω um G-conjunto. Então

$$G_0 = \{a \in G : ax = x, \forall x \in \Omega\}$$

é um subgrupo normal de G. Dizemos que uma ação de G em Ω é *fiel* ou G *age efetivamente* sobre Ω se $\varphi : G \longrightarrow S_\Omega$ é um homomorfismo injetor ou, equivalentemente,

$$\ker \varphi = G_0 = \{e\} \Leftrightarrow ax = x, \forall x \in \Omega \Rightarrow a = e.$$

Note que

$$\frac{G}{G_0}$$

sempre age efetivamente sobre Ω.

Seja Ω um G-conjunto não vazio. Então para cada $x \in \Omega$ o conjunto

$$G_x = \{a \in G : ax = x\}$$

é um subgrupo de G chamado o *estabilizador* ou *subgrupo isotrópico* de x. Note que

$$G_0 = \bigcap_{x \in \Omega} G_x.$$

O conjunto

$$O(x) = \{ax : a \in G\}$$

é chamado a *órbita* de x. Dados $x, y \in \Omega$, definimos $x \sim y$ se, e somente se, existe $a \in G$ tal que $y = ax$. É fácil verificar que $\sim$ é uma relação de equivalência em Ω e que $O(x)$ são as classes de equivalências de Ω. Logo,

$$\Omega = \dot{\bigcup_{x \in \Omega}} O(x)$$

Dizemos que G *age transitivamente* sobre Ω ou Ω *é um G-conjunto transitivo*, se para quaisquer $x, y \in \Omega$, existir $a \in G$ com $ax = y$ ou, equivalentemente, $\Omega = O(x)$, $\forall x \in \Omega$. Dizemos que G *age fortemente transitivo* sobre Ω se dados $x, y \in \Omega$, então existir um único $a \in G$ tal que $y = ax$. Neste caso, $|G| = |\Omega|$.

Observação 1.2 *G age transitivamente sobre cada órbita, pois se $y, z \in O(x)$, então existem $a, b \in G$ tais que*

$$y = ax \ \ e \ \ z = bx.$$

Logo, existe $c = ba^{-1} \in G$ tal que $z = cy$.

Sejam Σ e Ω dois G-conjuntos. Um *homomorfismo de G-conjuntos* é uma função $\varphi : \Sigma \to \Omega$ tal que

$$\varphi(ax) = a\varphi(x),$$

para todo $a \in G$ e $x \in \Sigma$. Um homomorfismo de G-conjuntos $\varphi : \Sigma \longrightarrow \Omega$ é um *isomorfismo de G-conjuntos* se φ é bijetora. Quando existir um isomorfismo de G-conjuntos entre Σ e Ω, dizemos que Σ e Ω são *isomorfos* e denotamos por $\Sigma \simeq \Omega$.

Proposição 1.5 *Sejam Ω um G-conjunto transitivo. Então*

$$\Omega \simeq \frac{G}{G_x}, \forall x \in \Omega.$$

Demonstração. Para cada $x \in \Omega$ vamos definir

$$\varphi : \frac{G}{G_x} \to \Omega$$

por $\varphi(aG_x) = ax$, para todo $a \in G$. É fácil verificar que φ está bem definida e é injetora. Agora, dado $u \in G$ e $aG_x \in \frac{G}{G_x}$, obtemos que

$$\varphi(u(aG_x)) = \varphi((ua)G_x) = (ua)x = u(ax) = \varphi(aG_x),$$

isto é, φ é um homomorfismo de G-conjuntos. Finalmente, dado $y \in \Omega$ existe, por hipótese, $a \in G$ tal que $y = ax = \varphi(aG_x)$, isto é, φ é sobrejetora. Portanto,

$$\Omega \simeq \frac{G}{G_x}, \forall x \in \Omega.$$

■

Corolário 1.1 *Sejam Ω um G-conjunto e $x \in \Omega$. Então*

$$O(x) \simeq \frac{G}{G_x} \;\; e \;\; |O(x)| = [G : G_x].$$

Em particular, se G é finito, então $|O(x)| \mid |G|$.

Demonstração. Basta observar que $O(x)$ é um G-conjunto transitivo para cada $x \in \Omega$.■

Exemplo 1.3 *Sejam G um grupo, H e K subgrupos finito de G. Então*

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

De fato, seja $\Omega = \frac{G}{K}$, então a aplicação

$$* : H \times \Omega \longrightarrow \Omega,$$

definida por $*(a, gK) = agK$ é uma ação de H sobre Ω. Como

$$O(K) = \{aK : a \in H\} = HK$$

temos que

$$|HK| = |K|\, r,$$

onde r é o número de classes laterais aK em $O(K)$. Por outro lado, pela Corolário 1.1*,*

$$|O(K)| = [H : H_K].$$

e

$$\begin{aligned} H_K &= \{a \in H : aK = K\} \\ &= \{a \in H : a \in K\} = H \cap K. \end{aligned}$$

Logo,

$$r = [H : H \cap K] = \frac{|H|}{|H \cap K|} \ \ e \ \ |HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Teorema 1.3 *Sejam G um grupo, $H \leq G$ e $\Lambda = \frac{G}{H}$ um G-conjunto. Seja π_H a representação por permutação induzida por esta ação. Então*:

1. *G age transitivamente sobre Λ.*

2. *O estabilizador em G do ponto $H \in \Lambda$ é o subgrupo H.*

3. *O núcleo da ação é dado por*

$$\ker \pi_H = \bigcap_{b \in G} bHb^{-1}$$

e $\ker \pi_H$ é o maior subgrupo normal de G contido em H.

Demonstração.1. Para ver que G age transitivamente sobre Λ. Sejam aH, $bH \in \Lambda$ e $c = ba^{-1} \in G$. Então

$$caH = (ba^{-1})aH = bH.$$

2. O estabilizador do ponto H é

$$G_H = \{a \in G : aH = H\} = H.$$

3. Por definição de π_H temos que

$$\begin{aligned} \ker \pi_H &= \{a \in G : abH = bH, \forall b \in G\} \\ &= \{a \in G : b^{-1}ab \in H, \forall b \in G\} \\ &= \{a \in G : a \in bHb^{-1}, \forall b \in G\} \\ &= \bigcap_{b \in G} bHb^{-1}. \end{aligned}$$

A segunda afirmação, segue do fato de que

$$\ker \pi_H \lhd G \ \text{ e } \ \ker \pi_H \leq H.$$

Finalmente, se $N \lhd G$ e $N \subset H$ então

$$N = xNx^{-1} \leq xHx^{-1}, \forall x \in G.$$

Assim, $N \leq \ker \pi_H$. ■

Corolário 1.2 (Cayley) *Todo grupo é isomorfo a um grupo de permutação.* ■

Sejam G um grupo, H e K dois subgrupos. Dizemos que G é um *produto semidireto* de H por K, denotado por $G = H \rtimes K$, se as seguintes condições são satisfeitas:

1. $G = HK$;
2. $H \trianglelefteq G$;
3. $H \cap K = \{e\}$.

Neste caso, K é um *complemento* de H e $K \simeq \frac{G}{H}$, pois

$$K \simeq \frac{K}{H \cap K} \simeq \frac{HK}{H} = \frac{G}{H}.$$

Teorema 1.4 *Sejam G um grupo e H um subgrupo normal de G. Então as seguintes condições são equivalentes*:

1. *G é um produto semidireto de H por $\frac{G}{H}$;*
2. *Existe um homomorfismo de grupos $\varphi : \frac{G}{H} \longrightarrow G$, com*

$$\pi \circ \varphi = id_{\frac{G}{H}},$$

   onde $\pi : G \longrightarrow \frac{G}{H}$ é o homomorfismo canônico;

3. *Existe um homomorfismo de grupos $\phi : G \longrightarrow G$, com $\ker \phi = H$ e $\phi(x) = x$ para todo $x \in \operatorname{Im} \phi$.*

Demonstração. (1. $\Longrightarrow$ 2.) Seja K um complemento de H em G, isto é, $K \simeq \frac{G}{H}$. Então, cada $a \in G$ pode ser escrito de modo único na forma $a = hk$ com $h \in H$ e $k \in K$. Seja

$$\varphi : \frac{G}{H} \longrightarrow G$$

definida por $\varphi(Ha) = k$. Então é fácil verificar que φ é um homomorfismo bem definido com

$$\pi \circ \varphi = id_{\frac{G}{H}}.$$

(2. $\Longrightarrow$ 3.) Vamos definir $\phi : G \longrightarrow G$ por $\phi = \varphi \circ \pi$. Se $x \in \operatorname{Im}\phi$, então existe $a \in G$ tal que $x = \phi(a)$. Logo,

$$\phi(x) = \phi(\phi(a)) = \varphi \circ (\pi \circ \varphi)(\pi(a)) = \varphi \circ \pi(a) = \phi(a) = x,$$

isto é, $\phi(x) = x$ para todo $x \in \operatorname{Im}\phi$. Se $a \in \ker\phi$, então $\phi(a) = \varphi \circ \pi(a) = e$. Logo, $k = e$ e $a \in H$, isto é, $\ker\phi \subseteq H$. Reciprocamente, se $a \in H$, então

$$\phi(a) = \varphi \circ \pi(a) = \varphi(Ha) = \varphi(H) = e,$$

e, assim, $a \in \ker\phi$.

(3. $\Longrightarrow$ 1.) Fazendo $K = \operatorname{Im}\phi$. Obtemos que $G = HK$, pois

$$a = ae = a\phi(a)^{-1}\phi(a) = [a\phi(a^{-1})]\phi(a) \in HK,$$

para todo $a \in G$. Finalmente, se $x \in H \cap K$, então $\phi(x) = e$ e $x = \phi(x)$. Logo, $x = e$, isto é,

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

Como

$$K = \operatorname{Im}\phi \simeq \frac{G}{H}$$

temos que G é o produto semidireto de H por $\frac{G}{H}$. ■

Seja G o produto semidireto de H por K. Então, cada $a \in G$ pode ser escrito de modo único na forma:

$$a = hk, h \in H \text{ e } k \in K.$$

Assim, dados $a_1, a_2 \in G$, digamos $a_1 = h_1k_1$ e $a_2 = h_2k_2$, com $h_1, h_2 \in H$ e $k_1, k_2 \in K$, obtemos que

$$a_1a_2 = (h_1k_1)(h_2k_2) = (h_1k_1h_2k_1^{-1})(k_1k_2) = (h_1h_2^{k_1})(k_1k_2),$$

onde $h_2^{k_1} = k_1h_2k_1^{-1}$. Agora, seja K agindo em G por conjugação, isto é,

$$k \cdot a = kak^{-1}.$$

Então, para cada $k \in K$:

1. $\sigma_k : H \longrightarrow H$, $\sigma_k(h) = k \cdot h$ é um automorfismo.

2. $\varphi : K \longrightarrow \mathrm{Aut}(H) \leq S_G$ definida por $\varphi(k) = \sigma_k$ é um homomorfismo.

De fato 1.

$$\begin{aligned} \sigma_k \circ \sigma_{k^{-1}}(h) &= \sigma_k(\sigma_{k^{-1}}(h)) \\ &= \sigma_k(khk^{-1}) \\ &= k(k^{-1}hk)k^{-1} = h. \end{aligned}$$

De modo análogo,

$$\sigma_{k^{-1}} \circ \sigma_k(h) = h, \forall h \in H.$$

Logo, $\sigma_{k^{-1}}$ é a inversa de σ_k e σ_k é bijetora. Dados $h_1, h_2 \in H$,

$$\begin{aligned} \sigma_k(h_1h_2) &= k(h_1h_2)k^{-1} \\ &= (kh_1k^{-1})(kh_2k^{-1}) \\ &= \sigma_k(h_1)\sigma_k(h_2). \end{aligned}$$

Logo, $\sigma_k \in \mathrm{Aut}(H)$, $\forall k \in K$.

2. Basta demonstrar que $\sigma_{k_1k_2} = \sigma_{k_1} \circ \sigma_{k_2}$, $\forall k_1, k_2 \in K$. De fato, dado $h \in H$,

$$\begin{aligned} \sigma_{k_1k_2}(h) &= (k_1k_2)h(k_1k_2)^{-1} = k_1(k_2hk_2^{-1})k_1^{-1} \\ &= \sigma_{k_1}(k_2hk_2^{-1}) = \sigma_{k_1}(\sigma_{k_2}(h)) \\ &= \sigma_{k_1} \circ \sigma_{k_2}(h). \end{aligned}$$

Assim, a multiplicação em G torna-se

$$a_1a_2 = (h_1k_1)(h_2k_2) = (h_1\varphi(k_2)h_2)(k_1k_2).$$

Neste caso, G é o produto semidireto de H por K via φ, isto é, $G = H \rtimes_\varphi K$. Note que, se $\varphi \neq id$, então G é não abeliano, pois existem $h \in H$ e $k \in K$ tais que

$$khk^{-1} = \varphi(k)h \neq h.$$

Exemplo 1.4 *Sejam H um grupo abeliano qualquer e $K = \langle k \rangle \simeq \mathbb{Z}_{2m}$. Definimos o homomorfismo $\varphi : K \longrightarrow \mathrm{Aut}(H)$ por $\varphi(k)(h) = h^{-1}$. Então $G = H \rtimes_\varphi K$ é um grupo não abeliano. Note que*

$$\varphi(k^2)(h) = \varphi(k)(\varphi(k)(h)) = \varphi(k)(h^{-1}) = h,$$

isto é, $k^2hk^{-2} = h$*, para todo* $h \in H$*. Logo,* $k^2 \in Z(G)$*, onde*

$$Z(G) = \{g \in G : gh = hg, \forall h \in G\}$$

é um subrgrupo normal de G *chamado o* centro *de* G*. Agora, consideremos o seguinte caso particulare: se*

$$H = \langle h \rangle \simeq \mathbb{Z}_n \text{ e } K = \langle k \rangle \simeq \mathbb{Z}_2,$$

então $G = H \rtimes_\varphi K$ *é um grupo não abeliano de ordem* $2n$ *isomorfo ao* grupo diedral*, que denotamos por* D_{2n} *:*

$$D_{2n} = \langle h, k \rangle, \text{ e } h^n = k^2 = e, \ hk = kh^{-1},$$

onde h *é identificado com* (h, e) *e* k *é identificado com* (e, k)*.*

Sejam F um corpo e $\mathbf{I} = [\mathbf{e}_1 \cdots \mathbf{e}_n]$ a matriz $n \times n$ identidade sobre F, com vetores colunas $\mathbf{e}_i$, $i = 1, \ldots, n$. Uma *matriz de permutação* sobre F é uma matriz $\mathbf{P}$ obtida permutando as colunas de $\mathbf{I}$, isto é, existe $\sigma \in S_n$ tal que

$$\mathbf{P} = [\mathbf{e}_{\sigma(1)} \cdots \mathbf{e}_{\sigma(n)}]$$

ou, equivalentemente, $\mathbf{P}$ é uma matriz na qual qualquer linha e coluna tem um único elemento não nulo e todos os elementos não nulos são iguais a 1.

Afirmação: O conjunto P_n de todas as matrizes de permutação é um grupo.
De fato, dados $\mathbf{M}, \mathbf{N} \in P_n$, digamos

$$\mathbf{M} = (m_{ij}) \text{ e } \mathbf{N} = (n_{ij}),$$

Seja

$$\mathbf{MN} = \mathbf{P} = (p_{ij}),$$

onde

$$p_{ij} = \sum_{k=1}^{n} m_{ik} n_{kj}.$$

Então para qualquer i existe um único k tal que

$$m_{ik} = 1$$

e existe um único j tal que

$$n_{kj} = 1.$$

Logo, fixado i, $p_{ij} = 1$ para um e somente um j. De modo análogo, fixado j, $p_{ij} = 1$ para um e somente um i. Assim, $p_{ij} = 1$ se existir um único k tal que

$$m_{ik} = n_{kj} = 1$$

e $p_{ij} = 0$, caso contrário. Portanto, $\mathbf{P}$ é uma matriz de permutação, isto é,

$$\mathbf{MN} \in P_n.$$

Assim, temos a associatividade em P_n e $\mathbf{I}$ é elemento identidade de P_n. É fácil verificar que

$$\mathbf{PP}^t = \mathbf{P}^t\mathbf{P} = \mathbf{I}.$$

Portanto, $\mathbf{P}^{-1} = \mathbf{P}^t \in P_n$.

Note que a aplicação $f : S_n \to P_n$ dada por

$$f(\sigma) = \mathbf{P} = [\mathbf{e}_{\sigma(1)} \cdots \mathbf{e}_{\sigma(n)}]$$

é um isomorfismo de grupos.

Seja G um grupo multiplicativo qualquer. Uma *matriz monomial* $\mathbf{A}$ sobre G é uma matriz de permutação $\mathbf{P}$ cujas entradas não nulas são substituídas por elementos de G, isto é, $\mathbf{A} = \mathbf{DP}$, onde

$$\mathbf{D} = \text{diag}(a_1, \ldots, a_n), \forall a_i \in G,$$

é uma matriz diagonal de ordem n. Dizemos que $\mathbf{P}$ é o *suporte* de $\mathbf{A}$. Logo, o conjunto

$$M(G, P_n) = \{\text{todas as matrizes monomiais } A \text{ sobre } G \text{ com suporte em } P_n\}$$

é claramente um grupo. Além disso,

$$P_n \simeq M(\{e\}, P_n) \leq M(G, P_n) \text{ e } M(G, \{\mathbf{I}\}) \simeq G^n.$$

Teorema 1.5 *Seja G um grupo multiplicativo qualquer e P_n o grupo de matrizes de permutação. Então*

$$M(G, P_n) = M(G, \{\mathbf{I}\}) \rtimes M(\{e\}, P_n).$$

Demonstração. Por definição temos que

$$M(G, P_n) = M(G, \{\mathbf{I}\})M(\{e\}, P_n).$$

Assim, basta mostrar que

$$M(G,\{\mathbf{I}\}) \trianglelefteq M(G,P_n) \text{ e } M(G,\{\mathbf{I}\}) \cap M(\{e\},P_n) = \{e\mathbf{I}\}.$$

Dados $\mathbf{A} = \mathbf{DP} \in M(G,P_n)$ e $\mathbf{D}' \in M(G,\{\mathbf{I}\})$, temos que

$$\begin{aligned} \mathbf{AD}'\mathbf{A}^{-1} &= \mathbf{D}(\mathbf{PD}'\mathbf{P}^{-1})\mathbf{D}^{-1} \\ &= \mathbf{DD}''\mathbf{D}^{-1} \in M(G,\{\mathbf{I}\}). \end{aligned}$$

Finalmente, dado

$$\mathbf{A} \in M(G,\{\mathbf{I}\}) \cap M(\{e\},P_n),$$

temos que $\mathbf{A} = \mathbf{DI}$ e $\mathbf{A} = \text{diag}(e,\ldots,e)\mathbf{P}$, isto é,

$$\mathbf{D} = \text{diag}(a_1,\ldots,a_n) = \text{diag}(e,\ldots,e).$$

Portanto, $\mathbf{A} = e\mathbf{I}$. ■

Exemplo 1.5 *Sejam $G = \{1,-1\}$ um grupo multiplicativo e*

$$P_2 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

o grupo das matrizes de permutação. Então

$$M(G,P_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$$

é isomorfo ao grupo diedral D_4.

1.3 Operadores Lineares

Nesta seção apresentaremos algumas definições e resultados básicos sobre Álgebra Linear, que serão necessários para o entendimento dos capítulos subsequentes, o leitor interessado em mais detalhes pode consultar [5].

Seja F um corpo. Um conjunto não vazio V equipado com duas operações $(\mathbf{u},\mathbf{v}) \mapsto \mathbf{u}+\mathbf{v}$ e $(\alpha,\mathbf{u}) \mapsto \alpha\mathbf{u}$, é um *espaço vetorial* sobre F se as seguintes condições são satisfeitas:

1. $(V, +)$ é um grupo comutativo;

2. $\alpha(\beta\mathbf{u}) = (\alpha\beta)\mathbf{u}$, para todos $\alpha, \beta \in F$ e $\mathbf{u} \in V$;

2. $(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$, para todos $\alpha, \beta \in F$ e $\mathbf{u} \in V$

3. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$, para todos $\mathbf{u}, \mathbf{v} \in V$ e $\alpha \in F$;

4. $1\mathbf{u} = \mathbf{u}$, para todo $\mathbf{u} \in V$.

Um espaço vetorial V, salvo menção explicíta em contrário, significa um espaço vetorial sobre $\mathbb{R}$ com dimensão $\dim(V) = n$. Um *operador linear* de V é uma aplicação $T : V \to V$ tal que

$$T(\alpha\mathbf{u} + \mathbf{v}) = \alpha T(\mathbf{u}) + T(\mathbf{v}), \forall \mathbf{u}, \mathbf{v} \in V \text{ e } \alpha \in \mathbb{R}.$$

Denotamos por $\mathcal{L}(V, V)$ o conjunto de todos os operadores lineares de V. Neste caso, $\mathcal{L}(V, V)$ é um espaço vetorial com $\dim(\mathcal{L}(V, V)) = n^2$. Denotamos por $\mathrm{GL}(V)$ o conjunto de todos elementos de invertíveis de $\mathcal{L}(V, V)$.

Afirmação: $\mathrm{GL}(V)$ é um grupo isomorfo ao grupo $\mathrm{GL}(n, \mathbb{R})$.
De fato, sejam $T \in \mathrm{GL}(V)$ e

$$\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$$

uma base fixada de V. Como $T(\mathbf{u}_j) \in V$, $j = 1, \ldots, n$, temos que existem únicos $a_{ij} \in \mathbb{R}$ tais que

$$T(\mathbf{u}_j) = \sum_{i=1}^{n} a_{ij}\mathbf{u}_i, j = 1, \ldots, n.$$

Fazendo $\mathbf{A} = (a_{ij})$, obtemos para cada $T \in \mathrm{GL}(V)$ uma única matriz $\mathbf{A}$. Assim, a aplicação

$$\varphi : \mathrm{GL}(V) \to \mathrm{GL}(n, \mathbb{R})$$

definida por $\varphi(T) = \mathbf{A}$ é um isomorfismo.

Um escalar $\lambda \in \mathbb{R}$ é um *autovalor* de $T \in \mathcal{L}(V, V)$, se existir $\mathbf{u} \in V$, $\mathbf{u} \neq \mathbf{0}$ tal que

$$T(\mathbf{u}) = \lambda\mathbf{u}.$$

O vetor $\mathbf{u}$ é chamado o *autovetor* de T associado ao autovalor λ.

Lema 1.1 *Autovetores associados a autovalores distintos são sempre linearmente independentes.* ■

Sejam W um subespaço de V e $T \in \mathcal{L}(V,V)$. Dizemos que W é *invariante* em relação a T se $T(W) \subseteq W$, isto é,

$$T(\mathbf{w}) \in W, \forall \mathbf{w} \in W.$$

Seja V um espaço vetorial de dimensão n sobre $\mathbb{R}$ equipado com o produto interno usual. A *norma quadrática* ou *peso Euclidiano* $N(\mathbf{x}) = ||\mathbf{x}||^2$ de um vetor $\mathbf{x} \in V$ é a soma dos quadrados de suas componentes, isto é,

$$N(\mathbf{x}) = \langle \mathbf{x}, \mathbf{x} \rangle = \mathbf{x} \cdot \mathbf{x}^t$$

A *distância Euclidiana quadrática* entre dois vetores $\mathbf{x}, \mathbf{y} \in V$ é a norma quadrática de sua diferença, isto é,

$$d^2(\mathbf{x}, \mathbf{y}) = N(\mathbf{x} - \mathbf{y}).$$

Seja

$$\mathcal{B} = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$$

uma base para $\mathbb{R}^n$. Dizemos que a base

$$\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$$

para $\mathbb{R}^n$ é uma *base dual* de $\mathcal{B}$ se

$$\langle \mathbf{x}_i, \mathbf{y}_j \rangle = \delta_{ij},$$

pois existe um único funcional $f_{\mathbf{x}}(\mathbf{y}) = \langle \mathbf{x}, \mathbf{y} \rangle$ associado com $\mathbf{x} \in \mathbb{R}^n$ e, assim, podemos identificar o espaço dual $(\mathbb{R}^n)^*$ com $\mathbb{R}^n$.

Uma *isometria* ou um *movimento rígido* em $\mathbb{R}^n$ é uma aplicação $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ que preserva distância, isto é,

$$\|T(\mathbf{x}) - T(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|, \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$

Denotamos por $\text{Isom}(\mathbb{R}^n)$ o conjunto de todas as isometrias de $\mathbb{R}^n$.

Afirmação: $\text{Isom}(\mathbb{R}^n)$ é um grupo.

De fato, sejam $S, T \in \text{Isom}(\mathbb{R}^n)$. Então

$$\begin{aligned} \|S \circ T(\mathbf{x}) - S \circ T(\mathbf{y})\| &= \|S(T(\mathbf{x})) - S(T(\mathbf{y}))\| \\ &= \|T(\mathbf{x}) - T(\mathbf{y})\| \\ &= \|\mathbf{x} - \mathbf{y}\|, \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n. \end{aligned}$$

Logo, $S \circ T \in \text{Isom}(\mathbb{R}^n)$. Assim, a composição usual de aplicações é uma operação binária em $\text{Isom}(\mathbb{R}^n)$. É claro que esta operação binária é associativa e

$$\mathbf{I} \in \mathcal{F}(\mathbb{R}^n, \mathbb{R}^n)$$

é o elemento identidade de $\text{Isom}(\mathbb{R}^n)$. Sejam $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ e $T \in \text{Isom}(\mathbb{R}^n)$. Se $T(\mathbf{x}) = T(\mathbf{y})$, então

$$0 = \|T(\mathbf{x}) - T(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\| \Rightarrow \mathbf{x} = \mathbf{y}.$$

Logo, T é injetor. Para provar que todo elemento $T \in \text{Isom}(\mathbb{R}^n)$ é sobrejetor vamos primeiro apresentar algumas definições:

Sejam $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. O *segmento de reta* de extremos $\mathbf{x}$ e $\mathbf{y}$ é o conjunto

$$[\mathbf{x}, \mathbf{y}] = \{(1-t)\,\mathbf{x} + t\mathbf{y} : 0 \leq t \leq 1\}.$$

Um subconjunto não vazio S de $\mathbb{R}^n$ é chamado *convexo* se

$$[\mathbf{x}, \mathbf{y}] \subseteq S, \forall \mathbf{x}, \mathbf{y} \in S.$$

Dados $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$ tais que

$$\|\mathbf{x} - \mathbf{z}\| = \|\mathbf{x} - \mathbf{y}\| + \|\mathbf{y} - \mathbf{z}\|.$$

Então

$$\|T(\mathbf{x}) - T(\mathbf{z})\| = \|T(\mathbf{x}) - T(\mathbf{y})\| + \|T(\mathbf{y}) - T(\mathbf{z})\|,$$

isto é, $T(S)$ é convexo, para todo subconjunto convexo S de $\mathbb{R}^n$. Seja

$$\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$$

uma base qualquer de $\mathbb{R}^n$. Então

$$S_0 \subset S_1 \subset \cdots \subset S_n,$$

onde

$$S_0 = \{\mathbf{0}\}, S_i = \langle \mathbf{x}_1, \ldots, \mathbf{x}_i \rangle, i = 1, \ldots, n-1 \text{ e } S_n = \mathbb{R}^n.$$

Logo,

$$T(S_0) \subset T(S_1) \subset \cdots \subset T(S_n) \text{ e } \dim T(S_{i+1}) > \dim T(S_i), i = 0, \ldots, n-1,$$

pois os S_i são convexos. Assim, $\dim T(S_n) \geq n$. Portanto, $T(S_n) = \mathbb{R}^n$, isto é, T é sobrejetora.

Exemplo 1.6 *Se* $\mathbf{t} \in \mathbb{R}^n$*, então a aplicação* $T_{\mathbf{t}} : \mathbb{R}^n \longrightarrow \mathbb{R}^n$*, definida por*

$$T_{\mathbf{t}}(\mathbf{x}) = \mathbf{x} + \mathbf{t},\ \forall \mathbf{x} \in \mathbb{R}^n,$$

é um movimento rígido, chamado a translação à direita *por* $\mathbf{t}$*. É claro que* $T_{\mathbf{t}}(\mathbf{0}) = \mathbf{t}$*, de modo que* $T_{\mathbf{t}}$ *não é um operador linear se* $\mathbf{t} \neq \mathbf{0}$*. Se denotamos por* $T(\mathbb{R}^n)$ *o conjunto de todas as translações à direita, então* $T(\mathbb{R}^n)$ *é um subgrupo de* $\mathrm{Isom}(\mathbb{R}^n)$ *isomorfo ao grupo aditivo* $(\mathbb{R}^n, +)$*,* $T_{\mathbf{t}} \leftrightarrow \mathbf{t}$*.*

Uma operador linear $S : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é *ortogonal* se

$$\|S\mathbf{x}\| = \|\mathbf{x}\|, \forall \mathbf{x} \in \mathbb{R}^n.$$

Note que todo operador ortogonal é um movimento rígido. Se denotamos por $O(\mathbb{R}^n)$ o conjunto de todos os operadores ortogonais, então $O(\mathbb{R}^n)$ é um subgrupo de $\mathrm{Isom}(\mathbb{R}^n)$.

Lema 1.2 *Sejam* $S : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ *um operador linear e*

$$\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$$

a base canônica de $\mathbb{R}^n$*. Então* $S \in O(\mathbb{R}^n)$ *se, e somente se,*

$$\{S\mathbf{e}_1, \ldots, S\mathbf{e}_n\}$$

é uma base ortonormal de $\mathbb{R}^n$*.*

Demonstração: Suponhamos que S seja ortogonal. Se

$$\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{e}_i \text{ e } \mathbf{y} = \sum_{i=1}^{n} y_i \mathbf{e}_i,$$

então

$$\|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 = 2\langle \mathbf{x}, \mathbf{y} \rangle = 2\sum_{i=1}^{n} x_i y_i.$$

Em particular,

$$\|S(\mathbf{x}) + S(\mathbf{y})\|^2 - \|S(\mathbf{x})\|^2 - \|S(\mathbf{y})\|^2 = 2\langle S(\mathbf{x}), S(\mathbf{y}) \rangle.$$

Como

$$\|\mathbf{x} + \mathbf{y}\|^2 = \|S(\mathbf{x} + \mathbf{y})\|^2 = \|S(\mathbf{x}) + S(\mathbf{y})\|^2$$

temos que

$$\langle S(\mathbf{x}),S(\mathbf{y})\rangle = \langle \mathbf{x}, \mathbf{y}\rangle , \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$

Em particular,

$$\delta_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j\rangle = \langle S(\mathbf{e}_i), S(\mathbf{e}_j)\rangle .$$

Assim,

$$\{S\mathbf{e}_1, \ldots, S\mathbf{e}_n\}$$

é uma base ortonormal. Reciprocamente, se

$$\mathbf{x} = \sum_{i=1}^{n} x_i\mathbf{e}_i \text{ e } \mathbf{y} = \sum_{i=1}^{n} y_i\mathbf{e}_i,$$

então

$$\begin{aligned} \|S(\mathbf{x}) - S(\mathbf{y})\|^2 &= \|S(\mathbf{x} - \mathbf{y})\|^2 \\ &= \left\| \sum_{i=1}^{n} (x_i - y_i)S(\mathbf{e}_i) \right\|^2 \\ &= \sum_{i=1}^{n} (x_i - y_i)^2 \\ &= \|\mathbf{x} - \mathbf{y}\|^2 . \end{aligned}$$

Portanto, S é ortogonal. ■

Lema 1.3 *Todo movimento rígido que fixa a origem é um operador linear.*

Demonstração. Seja T um movimento rígido tal que $T(\mathbf{0}) = \mathbf{0}$. Suponhamos que

$$T(\mathbf{e}_i) = \mathbf{e}_i, i = 1, \ldots, n.$$

Então

$$\|T(\mathbf{x})\| = \|T(\mathbf{x}) - T(\mathbf{0})\| = \|\mathbf{x} - \mathbf{0}\| = \|\mathbf{x}\| , \forall \mathbf{x} \in \mathbb{R}^n.$$

Denotando $T(\mathbf{x})$ por $(y_1, \ldots, y_n)$, obtemos que

$$y_1^2 + \cdots + y_n^2 = x_1^2 + \cdots + x_n^2. \tag{1.1}$$

Por outro lado,

$$\|T(\mathbf{x}) - \mathbf{e}_1\| = \|T(\mathbf{x}) - T(\mathbf{e}_1)\| = \|\mathbf{x} - \mathbf{e}_1\| .$$

Logo,

$$(y_1 - 1)^2 + y_2^2 + \cdots + y_n^2 = (x_1 - 1)^2 + x_2^2 + \cdots + x_n^2. \tag{1.2}$$

Assim, subtraindo a equação (1.1) de (1.2) e desenvolvendo, obtemos que

$$2y_1 - 1 = 2x_1 - 1 \text{ e } y_1 = x_1.$$

De modo análogo, obtemos que $y_i = x_i$, para todo $i = 2, \ldots, n$. Portanto, $T(\mathbf{x}) = \mathbf{x}$, isto é, T é a aplicação identidade.

Suponhamos, agora, que $T(\mathbf{e}_i) = \mathbf{u}_i$, $i = 1, \ldots, n$ e que $S : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ seja um operador linear tal que

$$S(\mathbf{e}_i) = \mathbf{u}_i, i = 1, \ldots, n,$$

onde

$$\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$$

é uma base ortonormal de $\mathbb{R}^n$. É claro que S é invertível e $S^{-1} \circ T \in \text{Isom}(\mathbb{R}^n)$. Como

$$S^{-1} \circ T(\mathbf{0}) = \mathbf{0} \text{ e } S^{-1} \circ T(\mathbf{e}_i) = \mathbf{e}_i, i = 1, \ldots, n$$

temos que $T = S$. ■

Proposição 1.6 *Todo elemento $f \in \text{Isom}(\mathbb{R}^n)$ pode se escrito de modo único como*

$$f = T \circ S,$$

onde $T \in T(\mathbb{R}^n)$ e $S \in O(\mathbb{R}^n)$.

Demonstração: Dado $f \in \text{Isom}(\mathbb{R}^n)$, sejam $\mathbf{t} = f(\mathbf{0})$ e $S = f - \mathbf{t}$. Então é fácil verificar que $S \in \text{Isom}(\mathbb{R}^n)$ e $S(\mathbf{0}) = \mathbf{0}$. Logo, pelo Lema 1.3, $S \in O(\mathbb{R}^n)$. Portanto,

$$f = T \circ S,$$

onde $T(\mathbf{x}) = \mathbf{x} + \mathbf{t}$, para todo $\mathbf{x} \in \mathbb{R}^n$. Agora, seja

$$f = T_1 \circ S_1$$

outra decomposição. Então

$$T \circ S = T_1 \circ S_1.$$

Logo,

$$\begin{aligned} S \circ S_1^{-1} &= T^{-1} \circ (T \circ S) \circ S_1^{-1} \\ &= T^{-1} \circ (T_1 \circ S_1) \circ S_1^{-1} \\ &= T^{-1} \circ T_1. \end{aligned}$$

Assim, $T^{-1} \circ T_1(\mathbf{0}) = \mathbf{0}$ e $\mathbf{t}_1 - \mathbf{t} = \mathbf{0}$, isto é, $T = T_1$. Portanto, $S = S_1$. ■

Corolário 1.3 *Seja $T \in \mathrm{Isom}(\mathbb{R}^n)$. Então $T(\mathbf{0}) = \mathbf{0}$ se, e somente se,*

$$\langle T(\mathbf{x}),T(\mathbf{y})\rangle = \langle \mathbf{x}, \mathbf{y}\rangle, \forall \mathbf{x}, \mathbf{y} \in \mathbb{R}^n.$$

Corolário 1.4 $\mathrm{Isom}(\mathbb{R}^n) = T(\mathbb{R}^n) \rtimes O(\mathbb{R}^n)$.

Demonstração: Pela Proposição 1.6, basta demonstrar que

$$T(\mathbb{R}^n) \trianglelefteq \mathrm{Isom}(\mathbb{R}^n) \text{ e } T(\mathbb{R}^n) \cap O(\mathbb{R}^n) = \{I\}.$$

Dados $S \in O(\mathbb{R}^n)$ e $T_{\mathbf{t}} \in T(\mathbb{R}^n)$, obtemos que

$$\begin{aligned} S \circ T_{\mathbf{t}} \circ S^{-1}(\mathbf{x}) &= S(T_{\mathbf{t}}(S^{-1}(\mathbf{x}))) \\ &= S(S^{-1}(\mathbf{x}) + \mathbf{t}) \\ &= \mathbf{x} + S(\mathbf{t}) \\ &= T_{S(t)}(\mathbf{x}), \forall \mathbf{x} \in \mathbb{R}^n. \end{aligned}$$

Logo,

$$S \circ T_{\mathbf{t}} \circ S^{-1} = T_{S(t)} \in T(\mathbb{R}^n) \text{ e } T(\mathbb{R}^n) \trianglelefteq \mathrm{Isom}(\mathbb{R}^n).$$

É fácil verificar que

$$T(\mathbb{R}^n) \cap O(\mathbb{R}^n) = \{I\}.$$

Sejam V um espaço vetorial com produto interno e S um subconjunto não vazio de V. O conjunto

$$S^{\perp} = \{\mathbf{u} \in V : \langle \mathbf{u}, \mathbf{v}\rangle = 0, \forall \mathbf{v} \in S\},$$

é um subespaço de V, chamado o *complemento ortogonal* de $\langle S\rangle$. Além disso, se W é um subespaço de V invariante com relação a T, então $W^{\perp}$ é invariante com relação a T^t.

Seja $T \in \mathrm{Isom}(\mathbb{R}^n)$ tal que $T(\mathbf{0}) = \mathbf{0}$. Dizemos que T é uma *rotação* (ou *preserva orientação*) se $\det T = 1$ e *inverte orientação* se $\det T = -1$.

Sejam V um espaço vetorial e U, W subespaços de V tais que

$$V = U \oplus W.$$

Uma *reflexão em U ao longo de W* é um operador linear $R : V \longrightarrow V$ definida por

$$R(\mathbf{u} + \mathbf{w}) = \mathbf{u} - \mathbf{w}$$

para todo $\mathbf{u} \in U$ e $\mathbf{w} \in W$.

Proposição 1.7 *Sejam V um espaço vetorial de dimenção finita sobre $\mathbb{R}$ e $T \in \mathcal{L}(V,V)$. Então as a seguintes condições são equivalentes*:

1. *T é uma reflexão*;

2. *$V = \ker(T-I) \oplus \ker(T+I)$*;

3. *Existe uma base de V tal que T é representada pela matriz diagonal da forma*

$$\begin{bmatrix} \mathbf{I} & 0 \\ 0 & -\mathbf{I} \end{bmatrix};$$

4. *$T^2 = I$.*

Demonstração: (1. $\Rightarrow$ 2.) Suponhamos que T seja uma reflexão. Então existem U, W subespaços de V tais que

$$V = U \oplus W.$$

Assim, é fácil verificar

$$U = \ker(T-I) \text{ e } W = \ker(T+I).$$

(2. $\Rightarrow$ 3.) Seja n a dimensão de V. Como $\ker(T-I)$ é um subespaço de V temos que $\ker(T-I)$ contém uma base

$$\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$$

que é parte de uma base

$$\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v}_{k+1}, \ldots, \mathbf{v}_n\}$$

de V. É fácil verificar que

$$\{\mathbf{v}_{k+1}, \ldots, \mathbf{v}_n\}$$

é uma base de $\ker(T+1)$. Portanto, a representação matricial de T com relação à base $\mathcal{B}$ tem forma desejada. (3. $\Rightarrow$ 4.) é claro da representação matricial de T.

Finalmente, (4. $\Rightarrow$ 1.) Suponhamos que $T^2 = I$, isto é,

$$(T-I)(T+I) = 0$$

Então é fácil verificar que

$$\text{Im}(T+I) \subseteq \ker(T-I) \text{ e } \text{Im}(T-I) \subseteq \ker(T+I)$$

Dado $\mathbf{v} \in V$, obtemos que

$$\begin{aligned}
\mathbf{v} &= 1 \cdot \mathbf{v} \\
&= (\frac{1}{2} + \frac{1}{2})\mathbf{v} \\
&= \frac{1}{2}\mathbf{v} + \frac{1}{2}\mathbf{v} \\
&= \frac{1}{2}\mathbf{v} + \frac{1}{2}T(\mathbf{v}) + \frac{1}{2}\mathbf{v} - \frac{1}{2}T(\mathbf{v}) \\
&= \frac{1}{2}\left(\mathbf{v} + T(\mathbf{v})\right) + \frac{1}{2}\left(\mathbf{v} - T(\mathbf{v})\right).
\end{aligned}$$

Logo,

$$V = \ker\left(T - I\right) + \ker\left(T + I\right).$$

Por outro lado, se

$$\mathbf{v} \in \ker\left(T - I\right) \cap \ker\left(T + I\right),$$

então $T(\mathbf{v}) = \mathbf{v}$ e $T(\mathbf{v}) = -\mathbf{v}$, assim, $\mathbf{v} = -\mathbf{v}$, ou seja, $\mathbf{v} = \mathbf{0}$. Assim,

$$\ker\left(T + 1\right) \cap \ker\left(T - 1\right) = \{\mathbf{0}\}.$$

Portanto, tomando

$$U = \ker\left(T - I\right) \text{ e } V = \ker\left(T + I\right),$$

obtemos que T é uma reflexão de U ao longo de W. ■

Sejam V um espaço vetorial com produto interno e W subespaço de V. Dados $\mathbf{u}, \mathbf{v} \in V$, definimos $\mathbf{u} \sim \mathbf{v}$ se, e somente se, $\mathbf{v} - \mathbf{u} \in W$. É fácil verificar que $\sim$ é uma relação de equivalência em V e que

$$W + \mathbf{u} = \{\mathbf{v} \in V : \mathbf{u} \sim \mathbf{v}\}$$

são as classes de equivalências de V. Sejam V um espaço vetorial de dimensão n e W subespaço de V de dimensão $n - 1$. Dizemos que H é um *hiperplano* em V se

$$H = W + \mathbf{u}, \forall \mathbf{u} \in V,$$

isto é, H são as classes de W. Em particular, se $\mathbf{u} = \mathbf{0}$, então $H = W$ é um subespeço de dimensão $n - 1$. Logo,

$$\dim H^{\perp} = 1.$$

Portanto, existe $\mathbf{v} \in V$, $\mathbf{v} \neq \mathbf{0}$ tal que

$$H^{\perp} = \langle \mathbf{v} \rangle \text{ e } \langle \mathbf{v}, \mathbf{h} \rangle = 0, \forall \mathbf{h} \in H.$$

Assim, multiplicando por um escalar, se necessário, podemos sempre assumir que $\mathbf{v}$ é um vetor unitário.

Sejam H um hiperplano em $\mathbb{R}^n$ tal que $\mathbf{0} \in H$ e $R : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ uma reflexão de H ao longo de $H^{\perp} = \langle \mathbf{u} \rangle$. Então, pela Proposição 1.7, $R \in O(\mathbb{R}^n)$ e

$$R(\mathbf{x}) = \mathbf{h} - a\mathbf{u},$$

onde $\mathbf{x} = \mathbf{h} + a\mathbf{u}$, $\mathbf{h} \in H$ e $a \in \mathbb{R}$. Note que

$$R(H) = H \text{ e } R(\mathbf{u}) = -\mathbf{u}.$$

Assim, R comporta-se como um espelho em relação a H. Como

$$R(\mathbf{x}) = \mathbf{x} - 2a\mathbf{u}, \forall \mathbf{x} \in \mathbb{R}^n = H \oplus \langle \mathbf{u} \rangle,$$

e

$$\langle \mathbf{x}, \mathbf{u} \rangle = \langle \mathbf{h} + a\mathbf{u}, \mathbf{u} \rangle = a \langle \mathbf{u}, \mathbf{u} \rangle \Rightarrow a = \frac{\langle \mathbf{x}, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle}$$

temos que

$$R(\mathbf{x}) = \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle}\mathbf{u}, \forall \mathbf{x} \in \mathbb{R}^n. \tag{1.3}$$

Portanto, toda reflexão R de $O(\mathbb{R}^n)$ deixa algum hiperplano invariante, pois dado $\mathbf{r} \in \mathbb{R}^n$, $\mathbf{r} \neq \mathbf{0}$, o conjunto $H = \langle \mathbf{r} \rangle^{\perp}$ é um hiperplano de $\mathbb{R}^n$.

Lema 1.4 *Sejam* $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$ *com* $\langle \mathbf{u}, \mathbf{u} \rangle = \langle \mathbf{v}, \mathbf{v} \rangle \neq 0$. *Então existe uma reflexão* $S \in O(\mathbb{R}^n)$ *tal que* $S(\mathbf{u}) = \mathbf{v}$ *ou* $S(\mathbf{u}) = -\mathbf{v}$.

Demonstração. Seja $\mathbf{r} = \mathbf{u} + \mathbf{v}$. Então temos duas possibilidades: Se $\mathbf{r} \neq \mathbf{0}$, então existe uma reflexão $S_{\mathbf{r}}$ em $\langle \mathbf{r} \rangle^{\perp}$ ao longo de $\langle \mathbf{r} \rangle$. Logo, $S_{\mathbf{r}}(\mathbf{r}) = -\mathbf{r}$. Como

$$\langle \mathbf{u} - \mathbf{v}, \mathbf{r} \rangle = 0$$

temos que $\mathbf{u} - \mathbf{v} \in \langle \mathbf{r} \rangle^{\perp}$ e $S_{\mathbf{r}}(\mathbf{u} - \mathbf{v}) = \mathbf{u} - \mathbf{v}$. Assim,

$$S_{\mathbf{r}}(\mathbf{u}) = S_{\mathbf{r}}(\mathbf{r} - \mathbf{v}) = -\mathbf{v}.$$

Se $\mathbf{r} = \mathbf{0}$, então $\mathbf{s} = \mathbf{u} - \mathbf{v} \neq \mathbf{0}$. Logo, existe uma reflexão $S_{\mathbf{s}}$ em $\langle \mathbf{s} \rangle^{\perp}$ ao longo de $\langle \mathbf{s} \rangle$. Logo, $S_{\mathbf{s}}(\mathbf{s}) = -\mathbf{s}$. Como

$$\langle \mathbf{u} + \mathbf{v}, \mathbf{s} \rangle = 0$$

temos que $\mathbf{u} + \mathbf{v} \in \langle \mathbf{s} \rangle^{\perp}$ e $S_{\mathbf{s}}(\mathbf{u} + \mathbf{v}) = \mathbf{u} + \mathbf{v}$. Assim,

$$S_{\mathbf{s}}(\mathbf{u}) = S_{\mathbf{s}}(\mathbf{s} + \mathbf{v}) = \mathbf{v}.$$

■

Teorema 1.6 *Toda aplicação ortogonal $S \in O(\mathbb{R}^n)$, $S \neq I$, pode ser escrita como um produto de reflexões.*

Demosntração. Para demonstrar o teorema usaremos indução sobre n.

Se $n = 1$, então $S(x) = ax$, com $a \in \mathbb{R}^*$, pois S é linear. Como

$$|ax| = |S(x)| = |x|$$

temos que $a = -1$. Logo, $S^2 = I$. Suponhamos que o resultado seja válido para todos os subespaços com dimensão menor do que n e $n > 1$. Seja $\mathbf{r} \in \mathbb{R}^n$, $\mathbf{r} \neq \mathbf{0}$. Então

$$\langle S(\mathbf{r}), S(\mathbf{r}) \rangle = \langle \mathbf{r}, \mathbf{r} \rangle \neq 0.$$

Assim, pelo Lema 1.4, existe uma reflexão $T \in O(\mathbb{R}^n)$ tal que $T(S(\mathbf{r})) = \pm\mathbf{r}$. Como $\langle \mathbf{r} \rangle^{\perp}$ é invariante sobre TS, pois

$$\langle TS(\mathbf{x}), \mathbf{r} \rangle = \langle TS(\mathbf{x}), \pm TS(\mathbf{r}) \rangle = \pm \langle \mathbf{x}, \mathbf{r} \rangle = 0, \mathbf{x} \in \langle \mathbf{r} \rangle^{\perp},$$

temos que $TS \in O(\langle \mathbf{r} \rangle^{\perp})$. Logo, pela hipótese de indução,

$$TS|_{\langle \mathbf{r} \rangle^{\perp}} = S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k},$$

onde $\mathbf{r}_i \in \langle \mathbf{r} \rangle^{\perp}$ e $S_{\mathbf{r}_i} \in O(\langle \mathbf{r} \rangle^{\perp})$. Sendo $S_{\mathbf{r}_i}(\mathbf{r}) = \mathbf{r}$, obtemos que as reflexões $S_{\mathbf{r}_i}$ são elementos de $O(\mathbb{R}^n)$. Assim,

$$S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}(\mathbf{r}) = \mathbf{r} = \pm TS(\mathbf{r})$$

e temos duas possibilidades. Se

$$S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}(\mathbf{r}) = \mathbf{r} = TS(\mathbf{r}),$$

então

$$S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k} = TS,$$

pois

$$S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}(\mathbf{x}) = TS(\mathbf{x}), \forall \mathbf{x} \in \langle \mathbf{r} \rangle^{\perp}.$$

Portanto,

$$S = TS_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}.$$

Se

$$S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}(\mathbf{r}) = \mathbf{r} = -TS(\mathbf{r}),$$

então

$$S_{\mathbf{r}} S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}(\mathbf{r}) = S_{\mathbf{r}}(\mathbf{r}) = -\mathbf{r} = TS(\mathbf{r}).$$

Logo,

$$S_{\mathbf{r}} S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k} = TS,$$

pois

$$S_{\mathbf{r}} S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}(\mathbf{x}) = S_{\mathbf{r}}(TS|_{\langle \mathbf{r} \rangle^{\perp}}(\mathbf{x})) = TS(\mathbf{x}), \forall \mathbf{x} \in \langle \mathbf{r} \rangle^{\perp}.$$

Portanto,

$$S = TS_{\mathbf{r}} S_{\mathbf{r}_2} \cdots S_{\mathbf{r}_k}.$$

■

1.4 Grupos de reflexão finito

Nesta seção apresentaremos alguns grupos de reflexões finitos, o leitor interessado em mais detalhes pode consultar [7, 9]

Um *grupo de reflexão finito* G é um grupo finito gerado por refexões de $O(\mathbb{R}^n)$. Seja $R_{\mathbf{r}} \in O(\mathbb{R}^2)$ uma reflexão em $H_{\mathbf{r}} = \langle \mathbf{r} \rangle^{\perp}$ ao longo de $\langle \mathbf{r} \rangle$, onde

$$H_{\mathbf{r}} = \{a\mathbf{u} : a \in \mathbb{R} \text{ e } \langle \mathbf{r}, \mathbf{u} \rangle = 0\}$$

é o hiperplano que faz um ângulo de $\frac{\theta}{2}$ com o eixo dos x. Então, pela Proposição 1.7, os vetores

$$\mathbf{r} = (\cos\frac{\theta}{2}, \operatorname{sen}\frac{\theta}{2}) \text{ e } \mathbf{u} = (-\operatorname{sen}\frac{\theta}{2}, \cos\frac{\theta}{2})$$

são os autovetores de $R_{\mathbf{r}}$ associados aos autovalores 1 e -1, respectivamente. Por definição

$$\mathcal{B} = \{\mathbf{r}, \mathbf{u}\}$$

é uma base ortonormal de $\mathbb{R}^2$. Portanto, $R_{\mathbf{r}}$ é representado em relação à base $\mathcal{B}$ pela matriz

$$\mathbf{B} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Proposição 1.8 *Sejam $R, T \in O(\mathbb{R}^2)$ tais que $R^2 = T^2 = I$. Então $H_2 = \langle R, T\rangle = \langle RT\rangle \rtimes \langle R\rangle$. Em particular, se H_2 é finito, $H_2 \simeq D_{2n}$, para algum $n \in \mathbb{N}$ e donotamos por H_2^n.*

Demonstração: Sejam $H = \langle RT\rangle$ e $K = \langle T\rangle$. Então devemos demostrar que $H \trianglelefteq H_2$, $H \cap K = \{I\}$, $H_2 = HK$ e $R(RT) = (RT)^{-1}R$. Note que

$$R(RT)R^{-1} = R(RT)R = TR = T^{-1}R^{-1} = (RT)^{-1}.$$

Logo, a última relação está satisfeita. De modo analogo, demonstra-se que $T(RT)T^{-1} = (RT)^{-1}$. Assim, $H \trianglelefteq H_2$. Como $H_2 = \langle R, T\rangle$ temos que todo elemento de H_2 é da forma

$$R^{m_1}T^{n_1}\cdots R^{m_k}T^{n_k}, \text{ para algum } k \in \mathbb{N} \text{ e } m_i, n_i \in \mathbb{Z}.$$

Agora, $R = R^{-1}$ e $T = T^{-1}$ implica que cada elemento de H_2 pode ser escrito na forma

$$R^{m_1}T^{n_1}\cdots R^{m_k}T^{n_k}, \text{ para algum } k \in \mathbb{N} \text{ e } 0 \leq m_i, n_i \leq 1.$$

Logo, cada elemento de H_2 pode ser escrito em uma das formas

$$(RT)^m, (RT)^m R, (TR)^m, \text{ ou } (TR)^m T \text{ para algum } m \in \mathbb{Z}_+,$$

as quais, ainda, podem ser re-escritas sob as formas

$$(RT)^m, (RT)^m R, (RT)^{-m}, \text{ ou } (RT)^{-(m+1)}R \text{ para algum } m \in \mathbb{Z}_+,$$

Assim, $H_2 = HK$. Agora, se $R \in H \cap K$, então existe $m \in \mathbb{Z}$ tal que $R = (RT)^m$. Logo,

$$\begin{aligned} R &= (RT)^m = R(TR)^{m-1}T \Rightarrow T = (TR)^{m-1} \\ T &= (TR)^{m-1} = T(RT)^{m-2}R \Rightarrow R = (RT)^{m-2}, \end{aligned}$$

continuando assim, obtemos que $R = I$. Finalmente, se H_2 é finito, então pelo Teorema 1.1 o elemento RT tem ordem finita, digamos $n \in \mathbb{N}$. Portanto,

$$H_2^n \simeq D_{2n}.$$

■

Sejam $T \in O(\mathbb{R}^2)$ uma rotação em torno da origem $\mathbf{0} \in \mathbb{R}^2$ e $\{\mathbf{e}_1, \mathbf{e}_2\}$ a base canônica de $\mathbb{R}^2$. Então, pelo Lema 1.2,

$$\{T(\mathbf{e}_1), T(\mathbf{e}_2)\}$$

é uma base ortonormal de $\mathbb{R}^2$. Logo, escolhendo $T(\mathbf{e}_1) = (x, y)$, obtemos que $T(\mathbf{e}_2) = \pm(-y, x)$. Assim,

$$x^2 + y^2 = 1 \Rightarrow |x| \leq 1 \text{ e } |y| \leq 1.$$

Como a função $\cos : \mathbb{R} \to [-1, 1]$ é sobrejetora temos que existe $\theta = \theta(T) \in \mathbb{R}$, $0 \leq \theta < 2\pi$, tal que

$$\cos\theta = x \text{ e } \operatorname{sen}\theta = y.$$

Portanto, T é representado em relação à base canônica de $\mathbb{R}^2$ pela matriz

$$\mathbf{A}_\theta = \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{bmatrix},$$

pois $\det(T) = 1$. Portanto, cada rotação em torno da origem é uma rotação anti-horária através de um ângulo $\theta = \theta(T)$. Vamos denotar por $\check{R}$ o conjunto de todas as rotações de $O(\mathbb{R}^2)$.

Proposição 1.9 *Sejam G um subgrupo finito de $O(\mathbb{R}^2)$. Então $K = \check{R} \cap G$ é cíclico e será denotado por C_2.*

Demostração. Se $K \neq \{I\}$, então existe $T \in K$, $T \neq I$, tal que $\theta = \theta(T)$, com $0 \leq \theta < 2\pi$, seja mínimo.

Afirmação: $K = \langle T \rangle$.

De fato, é claro que $\langle T \rangle \subseteq K$. Por outro lado, seja $S \in K$. Então existe $m \in \mathbb{Z}$ tal que

$$m\theta(T) \leq \theta(S) < (m+1)\theta(T).$$

Logo,

$$0 \leq \theta(S) - m\theta(T) < \theta(T).$$

Assim, pela minimalidade de $\theta(T)$, obtemos que $\theta(S) = m\theta(T)$. Como

$$\begin{bmatrix} \cos\theta(S) & -\operatorname{sen}\theta(S) \\ \operatorname{sen}\theta(S) & \cos\theta(S) \end{bmatrix} = \begin{bmatrix} \cos m\theta(T) & -\operatorname{sen} m\theta(T) \\ \operatorname{sen} m\theta(T) & \cos m\theta(T) \end{bmatrix}$$
$$= \begin{bmatrix} \cos\theta(T) & -\operatorname{sen}\theta(T) \\ \operatorname{sen}\theta(T) & \cos\theta(T) \end{bmatrix}^m$$

temos que $S = T^m$, para algum $m \in \mathbb{Z}$. Portanto, $K \subseteq \langle T \rangle$. ■

Observação 1.3 *1. Se a ordem de C_2 é igual a m, para algum $m \in \mathbb{N}$, dentotamos C_2 por C_2^m. Neste caso,*

$$\theta = \theta(T) = \frac{2\pi}{m}.$$

2. Suponhamos que $G \neq C_2^m$. Então existe $R \in G$ tal que $R^2 = I$. Então $G = H_2^m \simeq D_{2m}$, pois se $S \in G$ e $S^2 = I$, então

$$\det(RS) = (\det R)(\det S) = (-1)(-1) = 1.$$

Logo, $RS \in C_2^m$ e $\langle RS \rangle \subseteq C_2^m$. Como

$$|\langle RS \rangle| = |C_2^m| = m$$

temos que $\langle RS \rangle = C_2^m$.

3. Portanto, pelas Proposições 1.8 *e* 1.9*, todo grupo de reflexão finito de $O(\mathbb{R}^2)$ é cíclico C_2^m ou diedral H_2^m, para algum $m \in \mathbb{N}$.*

Já vimos que podemos identificar o grupo de permutação S_{n+1} com um subgrupo de $O(\mathbb{R}^{n+1})$, pois toda matriz de permutação é um elemento de $O(\mathbb{R}^{n+1})$. Pelo item 3 da Proposição 1.4, todo elemento de S_{n+1} é um produto de transposições da forma

$$\tau = (kk+1), k = 1, \ldots, n.$$

Note que

$$\tau \leftrightarrow \mathbf{P}_{kk+1} = \mathbf{I}_{n+1} - \mathbf{E}_{kk} - \mathbf{E}_{k+1k+1} + \mathbf{E}_{kk+1} + \mathbf{E}_{k+1k}.$$

Seja $R_k \in O(\mathbb{R}^{n+1})$ a aplicação associada a $\tau \in S_{n+1}$. Então

$$R_k(\mathbf{e}_k) = \mathbf{e}_{k+1}, R_k(\mathbf{e}_{k+1}) = \mathbf{e}_k \text{ e } R_k(\mathbf{e}_j) = \mathbf{e}_j, \forall j \notin \{k, k+1\}.$$

Logo, $R_k^2 = I$, $k = 1, \ldots, n$. Portanto, S_{n+1} é isomorfo a um subgrupo de reflexões $\mathcal{H}$ de $O(\mathbb{R}^{n+1})$.

É fácil vreificar que

$$R_k(\mathbf{e}_{k+1} - \mathbf{e}_k) = -(\mathbf{e}_{k+1} - \mathbf{e}_k) \text{ e } R_k(\mathbf{e}_{k+1} + \mathbf{e}_k) = (\mathbf{e}_{k+1} + \mathbf{e}_k), k = 1, \ldots, n.$$

Seja

$$X = \{\mathbf{e}_i - \mathbf{e}_j : i \neq j \text{ e } 1 \leq i, j \leq n+1\}.$$

Então $W = \langle X \rangle$ é um subespaço de dimensão n em $\mathbb{R}^{n+1}$. Portanto,

$$\mathcal{A}_n = \{T_k : T_k = R_k \mid_W \text{ e } R_k \in \mathcal{H}\}$$

é um subgrupo de $O(\mathbb{R}^{n+1})$, pois

$$(R_k \mid_W) \circ (R_m \mid_W) = (R_k \circ R_m) \mid_W .$$

Proposição 1.10 *O grupo $\mathcal{A}_n$ é isomorfo a S_{n+1} e $|\mathcal{A}_n| = (n+1)!$.* ■

Seja $G = \{1, -1\}$ um grupo. Então, pelo Teorema 1.5,

$$\mathcal{B}_n = M(G, P_n)$$

é um subgrupo de $O(\mathbb{R}^n)$. Logo, identificando G com o subgrupo $\langle R \rangle$, onde $R \in O(\mathbb{R}^n)$ e $R^2 = I$, temos que

$$P_n = \langle R_2, R_3, \ldots, R_n \rangle,$$

onde, para $k = 1, \ldots, n-1$,

$$R_{k+1}(\mathbf{e}_k) = \mathbf{e}_{k+1}, R_{k+1}(\mathbf{e}_{k+1}) = \mathbf{e}_k \text{ e } R_{k+1}(\mathbf{e}_j) = \mathbf{e}_j, \forall j \notin \{k, k+1\}.$$

Proposição 1.11 *O grupo $\mathcal{B}_n$ é isomorfo a um subgrupo de reflexões de $O(\mathbb{R}^n)$ e $|\mathcal{B}_n| = 2^n n!$.* ■

Capítulo 2

Sistema de Raízes

Neste Capítulo apresentaremos algumas definições e resultados básicas sobre Sistemas de Raízes e Grupo Coxeter, o leitor interessado em mais detalhes pode consultar [7, 9]

2.1 Região Fundamental

O objetivo desta seção é descrever uma construção que produz uma região fundamental para qualquer subgrupo finito do grupo das transfomações invertíveis de um espaço vetorial de dimensão finita. Daremos algumas definições topológicas necessárias para os capítulos posteriores. O leitor interessado em mais detalhes pode consultar [10]

Seja $\mathbb{R}^n$ um espaço vetorial de dimensão n sobre $\mathbb{R}$ equipado com o produto interno usual. Fixado $\mathbf{x}_0 \in \mathbb{R}^n$ e um número real $\varepsilon > 0$, o conjunto

$$S_\epsilon(\mathbf{x}_0) = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, \mathbf{x}_0) = \varepsilon\}$$

é chamado a *esfera* de raio ε e centro $\mathbf{x}_0$ e o conjunto

$$B_\epsilon(\mathbf{x}_0) = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, \mathbf{x}_0) < \varepsilon\}$$

é chamado a *bola aberta* de raio ε e centro $\mathbf{x}_0$.

Um subconjunto U de $\mathbb{R}^n$ é *aberto* se, e somente se, para cada $\mathbf{x} \in U$ existir $\varepsilon > 0$ tal que

$$B_\epsilon(\mathbf{x}) \subseteq U.$$

Note que, a interseção finita e a união de conjuntos abertos é aberto. Um subconjunto X de $\mathbb{R}^n$ é *fechado* se, e somente se, o seu complementar $U = \mathbb{R}^n - X$ é aberto. Assim, a intersecção e a união finita de conjuntos fechados é fechado.

Sejam W um subconjunto de $\mathbb{R}^n$ fixado e

$$\mathcal{F} = \{Y \subseteq \mathbb{R}^n : W \subseteq Y \text{ e } Y \text{ é aberto em } \mathbb{R}^n\}.$$

Então o conjunto

$$W^0 = \bigcup_{Y \in \mathcal{F}} Y$$

é chamado o *interior* de W. Sejam X um subconjunto de $\mathbb{R}^n$ fixado e

$$\mathcal{F}' = \{Y \subseteq \mathbb{R}^n : X \subseteq Y \text{ e } Y \text{ é fechado em } \mathbb{R}^n\}.$$

Então o conjunto

$$\overline{X} = \bigcap_{Y \in \mathcal{F}'} Y$$

é chamado o *fecho* de X. A *fronteira* de X em $\mathbb{R}^n$ é dada por

$$\partial X = \overline{X} - X^0.$$

Sejam X um subconjunto de $\mathbb{R}^n$ fixado e $Y \subseteq X$. Então Y é chamado *aberto relativamente* a X se, e somente se, existir um aberto U de $\mathbb{R}^n$ tal que

$$Y = X \cap U.$$

Uma *cisão* de um subconjunto X de $\mathbb{R}^n$ é uma decomposição

$$X = A \cup B,$$

onde $A \cap B = \emptyset$ e os conjuntos A e B são ambos abertos em X. Note que todo subconjunto X de $\mathbb{R}^n$ admite pelo menos a *cisão trivial* $X = X \cup \emptyset$.

Um subconjunto X de $\mathbb{R}^n$ é *conexo* quando não admite outra cisão além da trivial.

Seja $\mathbf{x} \in \mathbb{R}^n$ a *componente conexa* de $\mathbf{x}$ é a união $K_{\mathbf{x}}$ de todos os subconjuntos conexos de $\mathbb{R}^n$ que contém $\mathbf{x}$. Note que existe pelo menos um subconjunto conexo de $\mathbb{R}^n$ contendo $\mathbf{x}$, a saber: $\{\mathbf{x}\}$. Logo $K_{\mathbf{x}}$ não é vazia. Além disso, $K_{\mathbf{x}}$ é o maior subconjunto conexo de $\mathbb{R}^n$ que contém $\mathbf{x}$ e

$$\mathbb{R}^n = \dot{\bigcup_{\mathbf{x} \in \mathbb{R}^n}} K_{\mathbf{x}}.$$

Lema 2.1 *Se $n \geq 2$, então $\mathbb{R}^n$ contém infinitos subespaços de dimensão $n-1$.*

Demonstração. Se $n \geq 2$, então podemos escolher dois vetores linearmente independentes $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{R}^n$. Assim, para cada $a \in \mathbb{R}$ definimos o subespaço de $\mathbb{R}^n$

$$V_a = \langle \mathbf{v}_1 + a\mathbf{v}_2 \rangle^{\perp}$$

de dimensão $n-1$. Logo, se $a \neq b$, então V_a e V_b são subespaço distintos de dimensão $n-1$. ■

Proposição 2.1 *$\mathbb{R}^n$ não pode ser escrito como uma união de um número finito de subespaços próprios.*

Demonstração. Se $n = 1$, então $\{0\}$ é o único subespaço próprio de $\mathbb{R}^n$. Suponhamos, como hipótese de indução, que o resultado seja válida para todo os espaços de dimensão $n-1$. Suponhamos, por absurdo, que

$$\mathbb{R}^n = V_1 \cup \cdots \cup V_m,$$

onde cada V_i é um subespaço próprio de $\mathbb{R}^n$ e W um subespaço qualquer de $\mathbb{R}^n$ de dimensão $n-1$. Então

$$\begin{aligned} W &= W \cap \mathbb{R}^n \\ &= W \cap (\bigcup_{i=1}^{m} V_i) \\ &= (W \cap V_1) \cup \cdots \cup (W \cap V_m). \end{aligned}$$

Por hipótese de indução, $W = W \cap V_i$ para algum i. Como $\dim W = n-1$ temos que $\dim V_i \leq n-1$ e $W \subseteq V_i$ implica que $W = V_i$. Portanto, todo subespaço W de dimensão $n-1$ ocorre como um dos subespaços $V_1, \ldots, V_m$, o que é uma contradição, pois $\mathbb{R}^n$ tem, pelo Lema 2.1, infinitos subespaços de dimensão $n-1$. ■

Corolário 2.1 *Se X é qualquer subconjunto finito de $\mathbb{R}^n$ e $\mathbf{0} \notin X$, então existe $\mathbf{t} \in \mathbb{R}^n$ tal que*

$$\langle \mathbf{t}, \mathbf{x} \rangle \neq 0, \forall \mathbf{x} \in X.$$

Demonstração. Sejam

$$X = \{\mathbf{x}_1, \ldots, \mathbf{x}_k\}$$

e $V_i = \langle \mathbf{x}_i \rangle^{\perp}$, $i = 1, \ldots, k$. Então V_i é um subespaço próprio de $\mathbb{R}^n$ com dimensão $n-1$. Logo, pela Proposição 2.1, existe

$$\mathbf{t} \in \mathbb{R}^n - \bigcup_{i=1}^{k} V_i$$

tal que

$$\langle \mathbf{t}, \mathbf{x} \rangle \neq 0, \forall \mathbf{x} \in X.$$

■

Seja G um grupo finito de $O(\mathbb{R}^n)$. Um subconjunto F de $\mathbb{R}^n$ é chamado uma *região fundamental* ou um *domínio fundamental* para G em $\mathbb{R}^n$ se as seguintes condições são satisfeitas:

1. F é aberto,
2. Se $I \neq T \in G$, então $F \cap T(F) = \emptyset$;
3. $\mathbb{R}^n = \bigcup\{T(\overline{F}) : T \in G\}$.

Mais geralmente, se W é um subespaço de $\mathbb{R}^n$ invariante sob G, então um subconjunto F de W é uma região fundamental para G em W se as seguintes condições são satisfeitas:

1. F é aberto relativamente a W;
2. Se $I \neq T \in G$, então $F \cap T(F) = \emptyset$;
3. $W = \bigcup\{T(\overline{F}) : T \in G\}$.

Como cada $T \in G$ é uma transformação linear temos que o conjunto

$$V_T = \{\mathbf{x} \in \mathbb{R}^n : T(\mathbf{x}) = \mathbf{x}\}$$

é um subespaço de $\mathbb{R}^n$ e $V_T = \ker(T - I)$. Se $T \neq I$, então V_T é um subespaço próprio de $\mathbb{R}^n$. Logo, pela Proposição 2.1, temos que

$$\mathbb{R}^n \neq \bigcup\{V_T : T \neq I \in G\}.$$

Assim, podemos escolher um ponto $\mathbf{x}_0 \in \mathbb{R}^n - V_T$. Portanto, $G_{\mathbf{x}_0} = \{I\}$ e pelo Corolário 1.1,

$$|O(\mathbf{x}_0)| = [G : G_{\mathbf{x}_0}] = |G|.$$

Se

$$G = \{T_0, T_1, \ldots, T_{M-1}\},$$

com $T_0 = I$ e $T_i(\mathbf{x}_0) = \mathbf{x}_i$, então

$$O(\mathbf{x}_0) = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{M-1}\}.$$

Se $i \neq 0$, então o segmento de reta de extremos $\mathbf{x}_0$ e $\mathbf{x}_i$ é

$$L_i = [\mathbf{x}_0, \mathbf{x}_i] = \{\mathbf{x}_0 + \lambda(\mathbf{x}_i - \mathbf{x}_0) : 0 \leq i \leq 1\}.$$

Logo, $\mathbf{x}_i - \mathbf{x}_0$ é um vetor paralelo a L_i. Como o ponto médio é o vetor $\frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i)$ temos que

$$d(\mathbf{x}_0, \frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i)) = d(\mathbf{x}_i, \frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i)), \forall i = 0, \ldots, M-1.$$

Se $H_i = \langle \mathbf{x}_0 - \mathbf{x}_i \rangle^{\perp}$, então $\frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i) \in H_i$, pois

$$\begin{aligned} \langle \frac{1}{2}(\mathbf{x}_0 + \mathbf{x}_i), \mathbf{x}_0 - \mathbf{x}_i \rangle &= \frac{||\mathbf{x}_0||^2 - ||\mathbf{x}_i||^2}{2} \\ &= \frac{||\mathbf{x}_0||^2 - ||T_i\mathbf{x}_0||^2}{2} \\ &= \frac{||\mathbf{x}_0||^2 - ||\mathbf{x}_0||^2}{2} = 0. \end{aligned}$$

Portanto, H_i é o "bissector perpendicular" de L_i.

Seja $\mathbf{x} \in \mathbb{R}^n$. Então $\mathbf{x} \perp (\mathbf{x}_0 - \mathbf{x}_i)$ se, e somente se, $d(\mathbf{x}, \mathbf{x}_0) = d(\mathbf{x}, \mathbf{x}_i)$. Assim, como $T_i\mathbf{x}_0 = x_i$ temos que

$$H_i = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, \mathbf{x}_0) = d(\mathbf{x}, \mathbf{x}_i)\}.$$

O conjunto

$$X_i = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, \mathbf{x}_0) \leq d(\mathbf{x}, \mathbf{x}_i)\}, 1 \leq i \leq M-1.$$

é chamado *semi-espaço* de $\mathbb{R}^n$ determinado por H_i e pode ser pensado como o conjunto de todos os pontos que estão no mesmo lado de H_i como $\mathbf{x}_0$.

Teorema 2.1 *Com as notações acima, o conjunto*

$$F = \bigcap_{i=1}^{M-1} X_i^0$$

é uma região fundamental para G em $\mathbb{R}^n$.

Demonstração. Como cada X_i^0 é aberto temos que F é aberto. Se $T_i \neq I$, então

$$T_i(F) = T_i\left(\bigcap_{j=1}^{M-1} X_j^0\right)$$

ou

$$\begin{aligned} T_i(F) &= T_i(\{\mathbf{x} : d(\mathbf{x},\mathbf{x}_0) < d(\mathbf{x},\mathbf{x}_j), 1 \leq j \leq M-1\}) \\ &= \{T_i(\mathbf{x}) : d(T_i(\mathbf{x}), T_i(\mathbf{x}_0)) < d(T_i(\mathbf{x}), T_iT_j(\mathbf{x}_0)), 1 \leq j \leq M-1\} \\ &= \{\mathbf{y} : d(\mathbf{y},\mathbf{x}_i) < (d\mathbf{y}, T_k(\mathbf{x}_0)), 0 \leq k \leq M-1, k \neq i\} \end{aligned}$$

pois

$$\{T_iT_j : 1 \leq j \leq M-1\} = G - \{T_i\}.$$

Assim,

$$T_i(X_j^0) = \{\mathbf{x} : d(\mathbf{x},\mathbf{x}_i) < d(\mathbf{x},\mathbf{x}_j)\}$$

para todos i e j, com $j \neq i$. Se $\mathbf{x} \in F \cap T_i(F)$, então

$$d(\mathbf{x},\mathbf{x}_0) < d(\mathbf{x},\mathbf{x}_i) \text{ e } d(\mathbf{x},\mathbf{x}_i) < d(\mathbf{x},\mathbf{x}_0),$$

o que é impossível. Assim, $F \cap T_i(F) = \emptyset$, para todo $T_i \neq I$. Finalmente, se $\mathbf{x} \in \mathbb{R}^n$, escolha um índice i para o qual $d(\mathbf{x},\mathbf{x}_i)$ seja minima e, portanto, $d(\mathbf{x},\mathbf{x}_i) \leq d(\mathbf{x},\mathbf{x}_j)$ para todo j. Como

$$T_i(\overline{F}) = \{\mathbf{x} : d(\mathbf{x},\mathbf{x}_i) \leq d(\mathbf{x},\mathbf{x}_j)\}, 0 \leq j \leq M-1.$$

temos que $\mathbf{x} \in T_i(F)$. Portanto,

$$\mathbb{R}^n = \bigcup\{T_i(\overline{F}) : 0 \leq i \leq M-1\}$$

e F é uma região fundamental para G em $\mathbb{R}^n$. ■

Seja

$$\begin{aligned} V_0 &= V_0(G) \\ &= \{T \in G : T(\mathbf{x}) = \mathbf{x}, \forall \mathbf{x} \in \mathbb{R}^n\} \\ &= \bigcap\{V_T : T \in G\}. \end{aligned}$$

Então V_0 é um subespaço de $O(\mathbb{R}^n)$ tal que $T(\mathbf{x}) = \mathbf{x}$, para todo $\mathbf{x} \in V_0$ e $T \in G$, isto é, $T|_{V_0} = I$. Em particular,

$$T(V_0) = V_0, \forall T \in G.$$

Assim,

$$T(V_0^{\perp}) = V_0^{\perp}, \forall T \in G.$$

Como

$$\mathbb{R}^n = V_0 \oplus V_0^{\perp}$$

temos que $T = I \oplus T^{\perp}$, para todo $T \in G$, onde $T^{\perp} = T|_{V_0^{\perp}}$. É fácil verificar que o grupo

$$G^{\perp} = \{T^{\perp} : T \in G\} \leq O(V_0^{\perp})$$

é isomorfo ao grupo $O(\mathbb{R}^n)$ e $V_0(G^{\perp}) = \{\mathbf{0}\}$. Como todo elemento $G^{\perp}$ pode ser estendido a um elemento de G, não há perda de generalidade em adimitir, no que segue, que $V_0(G) = \{\mathbf{0}\}$, isto é, G age efetivamente em $\mathbb{R}^n$,

$$* : G \times \mathbb{R}^n \to \mathbb{R}^n, *(T, \mathbf{x}) = T(\mathbf{x}).$$

2.2 Sistema de Raízes

Sejam G um grupo de reflexão finito e $\mathbf{r} \in \mathbb{R}^n$. Considere $S_{\mathbf{r}} \in O(\mathbb{R}^n)$ uma reflexão no hiperplano $H_{\mathbf{r}} = \langle \mathbf{r} \rangle^{\perp}$ ao longo de $\langle \mathbf{r} \rangle$. Então, pela Equação (1.3),

$$S_{\mathbf{r}}(\mathbf{x}) = \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{r} \rangle}{\langle \mathbf{r}, \mathbf{r} \rangle}\mathbf{r}, \mathbf{x} \in \mathbb{R}^n.$$

Neste caso, dizemos que $S_{\mathbf{r}}$ é uma reflexão de $H_{\mathbf{r}}$ determinada por $\mathbf{r}$. Será escolhido, para cada reflexão S (e, portanto, para cada hiperplano H) um único vetor normal $\mathbf{r}$ com comprimento fixado. O vetor normal $\mathbf{r}$ e seu oposto $-\mathbf{r}$ são chamados *raízes* de G. O conjunto Δ de todas as raízes de G é chamado o *sistema de raiz* de G, isto é,

$$\Delta = \{\pm\mathbf{r} \in \mathbb{R}^n : S_{\mathbf{r}} \in G\}.$$

Proposição 2.2 *Se $\mathbf{r} \in \mathbb{R}^n$ é uma raiz de G, então $T(\mathbf{r})$ é uma raiz de G, para todo $T \in O(\mathbb{R}^n)$. Além disso, se $T(\mathbf{r}) = \mathbf{x}_0$, então*

$$S_{\mathbf{x}_0} = TS_{\mathbf{r}}T^{-1} \in G, \forall T \in O(\mathbb{R}^n). \tag{2.1}$$

Demonstração. Seja $H_{\mathbf{r}} = \langle \mathbf{r} \rangle^{\perp}$ o hiperplano em $\mathbb{R}^n$. Então

$$\langle \mathbf{r}, \mathbf{h} \rangle = 0, \forall \mathbf{h} \in H_{\mathbf{r}}.$$

Logo,

$$\langle T(\mathbf{r}), T(\mathbf{h}) \rangle = 0, \forall \mathbf{h} \in H_{\mathbf{r}},$$

isto é,

$$\langle T(\mathbf{r}), \mathbf{k} \rangle = 0, \forall \mathbf{k} \in T(H_{\mathbf{r}}).$$

Assim, $T(H_{\mathbf{r}}) = \langle T(\mathbf{r}) \rangle^{\perp}$ é um hiperplano em $\mathbb{R}^n$, para todo $T \in O(\mathbb{R}^n)$.e $T(\mathbf{r})$ é uma raiz de G. Finalmente, como $\mathbb{R}^n = H_{\mathbf{r}} \oplus \langle \mathbf{r} \rangle$ temos que

$$\begin{aligned} TS_{\mathbf{r}}T^{-1}(\mathbf{x}) &= TS_{\mathbf{r}}(T^{-1}(\mathbf{x})) \\ &= T\left(T^{-1}(\mathbf{x}) - 2\frac{\langle T^{-1}(\mathbf{x}), \mathbf{r} \rangle}{\langle \mathbf{r}, \mathbf{r} \rangle}\mathbf{r}\right) \\ &= \mathbf{x} - 2\frac{\langle \mathbf{x}, T(\mathbf{r}) \rangle}{\langle T(\mathbf{r}), T(\mathbf{r}) \rangle}T(\mathbf{r}) \\ &= \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{x}_0 \rangle}{\langle \mathbf{x}_0, \mathbf{x}_0 \rangle}\mathbf{x}_0 \\ &= S_{\mathbf{x}_0}(\mathbf{x}), \forall \mathbf{x} \in \mathbb{R}^n. \end{aligned}$$

Portanto,

$$S_{\mathbf{x}_0} = TS_{\mathbf{r}}T^{-1} \in G, \forall T \in O(\mathbb{R}^n).$$

■

Corolário 2.2 *Seja Δ um sitema de raiz para G. Então*:

1. $\Delta \cap \langle \mathbf{r} \rangle = \{\mathbf{r}, -\mathbf{r}\}$, *para todo* $\mathbf{r} \in \Delta$;

2. $S_{\mathbf{r}}(\Delta) = \Delta$, *para todo* $\mathbf{r} \in \Delta$.

Exemplo 2.1 *Pela Proposição* 1.8*, obtemos que*

$$\begin{aligned} H_2^3 &= \langle S_{\mathbf{r}_1}, S_{\mathbf{r}_2} \rangle \\ &= \{I, S_{\mathbf{r}_1}S_{\mathbf{r}_2}, (S_{\mathbf{r}_1}S_{\mathbf{r}_2})^2, S_{\mathbf{r}_1}, S_{\mathbf{r}_2}, S_{\mathbf{r}_1}(S_{\mathbf{r}_1}S_{\mathbf{r}_2})^2\}, \end{aligned}$$

onde $S_{\mathbf{r}_1}$ e $S_{\mathbf{r}_2}$ são reflexões de $H_{\mathbf{r}_1}$ e $H_{\mathbf{r}_2}$ determinadas pelas raízes

$$\mathbf{r}_1 = (0, 1) \ \ e \ \ \mathbf{r}_2 = (\frac{\sqrt{3}}{2}, -\frac{1}{2}).$$

Como H_2^3 contém mais uma reflexão

$$S_{\mathbf{r}_3} = S_{\mathbf{r}_1}(S_{\mathbf{r}_1}S_{\mathbf{r}_2})^2 = S_{\mathbf{r}_2}S_{\mathbf{r}_1}S_{\mathbf{r}_2}^{-1} = S_{S_{\mathbf{r}_2}(\mathbf{r}_1)},$$

determinada pela raiz

$$\mathbf{r}_3 = S_{\mathbf{r}_2}(\mathbf{r}_1) = (\frac{\sqrt{3}}{2}, \frac{1}{2})$$

temos que

$$\Delta = \{\pm\mathbf{r}_1, \pm\mathbf{r}_2, \pm\mathbf{r}_3\}$$

é o sistema de raízes de H_2^3.

Exemplo 2.2 *Pela Proposição* 1.11

$$\mathcal{B}_n = \langle S, S_2, S_3, \ldots, S_n\rangle,$$

onde, $S^2 = I$ *e, para* $k = 1, \ldots, n-1$,

$$S_{k+1}(\mathbf{e}_k) = \mathbf{e}_{k+1}, S_{k+1}(\mathbf{e}_{k+1}) = \mathbf{e}_k \ \ e \ \ S_{k+1}(\mathbf{e}_j) = \mathbf{e}_j, \forall j \notin \{k, k+1\}.$$

Um vetor $\mathbf{r} \in \mathbb{R}^n$ *é uma raiz para* $\mathcal{B}_n$ *se, e somente se,* $S(\mathbf{r}) = -\mathbf{r}$ *e* $S_{k+1}(\mathbf{r}) = -\mathbf{r}$, $k = 1, \ldots, n-1$. *Como*

$$\mathbf{r} = \sum_{i=1}^{n} x_i\mathbf{e}_i$$

temos que

$$S_{k+1}(\mathbf{r}) = -\mathbf{r} \Leftrightarrow x_{k+1} = -x_k \ \ e \ \ x_j = 0, \forall j \notin \{k, k+1\}.$$

Assim,

$$\Delta = \{\pm\mathbf{e}_i, 1 \leq i \leq n\} \cup \{\pm(\mathbf{e}_i - \mathbf{e}_j), 1 \leq j < i \leq n\}$$

é o sistema de raízes para $\mathcal{B}_n$.

Exemplo 2.3 *Pela Proposição* 1.10

$$\mathcal{A}_n = \langle T_1, T_2, \ldots, T_{n+1}\rangle,$$

onde $T_k = S_k|_W$, $W = \langle X\rangle$ *com*

$$X = \{\mathbf{e}_i - \mathbf{e}_j : i \neq j \ \ e \ \ 1 \leq i, j \leq n+1\}$$

e

$$S_k(\mathbf{e}_k) = \mathbf{e}_{k+1}, S_k(\mathbf{e}_{k+1}) = \mathbf{e}_k \ \ e \ \ S_k(\mathbf{e}_j) = \mathbf{e}_j, \forall j \notin \{k, k+1\},$$

com , $k = 1, \ldots, n$. *É fácil verificar que*

$$\{\mathbf{e}_1 - \mathbf{e}_{n+1}, \ldots, \mathbf{e}_n - \mathbf{e}_{n+1}\}$$

é uma base de W. *Logo,*

$$W = \langle(1, 1, \ldots, 1)\rangle^{\perp}.$$

Assim, de modo análogo ao Exemplo 2.2*,*

$$\Delta = \{\pm(\mathbf{e}_i - \mathbf{e}_j), 1 \leq j < i \leq n+1\}$$

é o sistema de raízes para $\mathcal{A}_n$*.*

Lema 2.2 *Sejam* U *e* W *subespaços de* $\mathbb{R}^n$*. Então*:

1. $U^{\perp\perp} = U$;
2. $(U+W)^{\perp} = U^{\perp} \cap W^{\perp}$;
3. $(U \cap W)^{\perp} = U^{\perp} + W^{\perp}$.

Demonstração. Vamos demonstrar apenas o item 3. Como $U \cap W \subseteq U, W$ temos que $U^{\perp}, W^{\perp} \subseteq (U \cap W)^{\perp}$ e $U^{\perp} + W^{\perp} \subseteq (U \cap W)^{\perp}$. Por outro lado,

$$\begin{aligned}
\dim(U \cap W)^{\perp} &= n - \dim(U \cap W) \\
&= n - \dim(U) - \dim(W) + \dim(U+W) \\
&= -n + \dim(U+W) + \dim(U^{\perp}) + \dim(W^{\perp}) \\
&= -\dim(U+W)^{\perp} + \dim(U^{\perp}) + \dim(W^{\perp}) \\
&= -\dim(U^{\perp} \cap W^{\perp}) + \dim(U^{\perp}) + \dim(W^{\perp}) \\
&= \dim(U^{\perp} + W^{\perp}).
\end{aligned}$$

Portanto, $(U \cap W)^{\perp} = U^{\perp} + W^{\perp}$. ■

Proposição 2.3 *Suponhamos que*

$$G = \langle S_{\mathbf{r}_1}, \ldots, S_{\mathbf{r}_k} \rangle,$$

onde

$$\Delta = \{\mathbf{r}_1, \ldots, \mathbf{r}_k\}$$

é um sistema de raízes para G *e* $S_{\mathbf{r}_i}$ *são reflexões de* $H_{\mathbf{r}_i}$ *determinadas pelas raízes* $\mathbf{r}_i$*,* $i = 1, \ldots, k$*. Então* G *age efetivamente sobre* $\mathbb{R}^n$ *se, e somente se,* Δ *contém uma base para* $\mathbb{R}^n$*.*

Demonstração. Seja

$$W = \bigcap_{i=1}^{k} H_{\mathbf{r}_i}.$$

Como $S_{\mathbf{r}_i}(\mathbf{h}) = \mathbf{h}$, para todo $\mathbf{h} \in H_{\mathbf{r}_i}$, $i = 1, \ldots, k$, temos que $T(\mathbf{w}) = \mathbf{w}$, para todo $\mathbf{w} \in W$ e $T \in G$, isto é, $T|_W = I$. Assim,

$$W \subseteq V_0(G).$$

Por outro lado, se $\mathbf{x} \in V_0(G)$, então $S_{\mathbf{r}_i}(\mathbf{x}) = \mathbf{x}$, $i = 1, \ldots, k$, isto é, $\mathbf{x} \in H_{\mathbf{r}_i}$, $i = 1, \ldots, k$. Logo, $\mathbf{x} \in W$ e

$$W = V_0(G).$$

Portanto, G age efetivamente sobre $\mathbb{R}^n$ se, e somente se, $W = \{\mathbf{0}\}$ se, e somente se, $W^\perp = \mathbb{R}^n$. Pelo Lema 2.2,

$$\begin{aligned} W^\perp &= \left(\bigcap_{i=1}^{k} H_{\mathbf{r}_i}\right)^\perp \\ &= \sum_{i=1}^{k} H_{\mathbf{r}_i}^\perp, \end{aligned}$$

Logo, $W^\perp = \langle \Delta \rangle$, pois $H_{\mathbf{r}_i}^\perp = \langle \mathbf{r}_i \rangle$, $i = 1, \ldots, k$. Portanto, G age efetivamente sobre $\mathbb{R}^n$ se, e somente se, $\mathbb{R}^n = \langle \Delta \rangle$. ■

Já vimos que todo grupo de reflexão finito G é gerado por reflexões $S_{\mathbf{r}}$, com $\mathbf{r} \in \Delta$. Note que nem todas as raízes $\mathbf{r}$ são necessárias para gerar o grupo G, pois $\mathbf{r}$ e $-\mathbf{r}$ determinam a mesma reflexão. Isto nos conduz a uma partição do conjunto Δ em conjunto de raízes "positivas" e "negativas."

Como Δ é finito e $\mathbf{0} \notin \Delta$ temos, pelo Corolário 2.1, que existe $\mathbf{t} \in \mathbb{R}^n$ tal que $\langle \mathbf{t}, \mathbf{r} \rangle \neq 0$, para todo $\mathbf{r} \in \Delta$. Então os subconjuntos

$$\Delta_{\mathbf{t}}^+ = \{\mathbf{r} \in \Delta : \langle \mathbf{t}, \mathbf{r} \rangle > 0\}$$

e

$$\Delta_{\mathbf{t}}^- = \{\mathbf{r} \in \Delta : \langle \mathbf{t}, \mathbf{r} \rangle < 0\}$$

são chamados sistema de *raízes positivas* e *negativas*, em relação a $\mathbf{t}$, respectivamente. Note que,

$$\mathbf{r} \in \Delta_{\mathbf{t}}^+ \Leftrightarrow -\mathbf{r} \in \Delta_{\mathbf{t}}^-,$$

pois $\langle \mathbf{t}, -\mathbf{r} \rangle = -\langle \mathbf{t}, \mathbf{r} \rangle$. Logo,

$$\Delta = \Delta_{\mathbf{t}}^{+} \dot{\bigcup} \Delta_{\mathbf{t}}^{-} \text{ e } \left|\Delta_{\mathbf{t}}^{+}\right| = \left|\Delta_{\mathbf{t}}^{-}\right| = \frac{1}{2}\left|\Delta\right|.$$

Dizemos que o subconjunto minimal Π de $\Delta_{\mathbf{t}}^{+}$ é uma *base-raiz* ou uma $\mathbf{t}$-*base* para Δ se para cada $\mathbf{r} \in \Delta_{\mathbf{t}}^{+}$ temos que

$$\mathbf{r} = \sum a_i \mathbf{r}_i,$$

onde $\mathbf{r}_i \in \Pi$ e $a_i \in \mathbb{R}_+$. Neste caso, dizemos que os $\mathbf{r}_i \in \Pi$ são *raízes simples* e $S_{\mathbf{r}_i}$ são *reflexões simples.*

Exemplo 2.4 *Sejam H_2^3 o grupo diedral e*

$$\Delta = \{\pm\mathbf{r}_1, \pm\mathbf{r}_2, \pm\mathbf{r}_3\}$$

o sistema de raízes de H_2^3 dado no Exemplo 2.1*. Então tomando $\mathbf{t} = \mathbf{r}_3$, obtemos que*

$$\Delta_{\mathbf{t}}^{+} = \{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3\} \text{ e } \Delta_{\mathbf{t}}^{-} = \{-\mathbf{r}_1, -\mathbf{r}_2, -\mathbf{r}_3\}.$$

Assim,

$$\Pi = \{\mathbf{r}_1, \mathbf{r}_2\}$$

é uma $\mathbf{t}$-base para Δ.

Exemplo 2.5 *Sejam $\mathcal{A}_2$ o grupo de reflexão e*

$$\Delta = \{\pm\mathbf{r}_1, \pm\mathbf{r}_2, \pm\mathbf{r}_3\}$$

o sistema de raízes de $\mathcal{A}_2$ dado no Exemplo 2.3*. Então tomando $\mathbf{t} = \mathbf{r}_3 = (-1, 0, 1) \in \mathbb{R}^3$, obtemos que*

$$\Delta_{\mathbf{t}}^{+} = \{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3\} \text{ e } \Delta_{\mathbf{t}}^{-} = \{-\mathbf{r}_1, -\mathbf{r}_2, -\mathbf{r}_3\}.$$

Assim,

$$\Pi = \{\mathbf{r}_1, \mathbf{r}_2\}$$

é uma $\mathbf{t}$-base para Δ. Note que $\mathcal{A}_2$ é isomorfo a H_2^3.

Proposição 2.4 *Sejam $\mathbf{r}_i, \mathbf{r}_j \in \Pi$, com $i \neq j$, e $a_i, a_j \in \mathbb{R}_+^*$. Então $\mathbf{x} = a_i\mathbf{r}_i - a_j\mathbf{r}_j \notin \Delta_{\mathbf{t}}^{+}$ e $\mathbf{x} = a_i\mathbf{r}_i - a_j\mathbf{r}_j \notin \Delta_{\mathbf{t}}^{-}$.*

Demonstração. Suponhamos, por absurdo, que $\mathbf{x} \in \Delta_{\mathbf{t}}^{+}$. Então existem $b_k \in \mathbb{R}_+$ tais que

$$\begin{aligned} \mathbf{x} &= a_i\mathbf{r}_i - a_j\mathbf{r}_j \\ &= \sum_{k=1}^{m} b_k\mathbf{r}_k \end{aligned}$$

onde

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_m\}.$$

Assim, se $a_i \leq b_i$, então

$$(b_i - a_i)\,\mathbf{r}_i + (b_j + a_j)\,\mathbf{r}_j + \sum_{k\neq i,j} b_k\mathbf{r}_k = \mathbf{0}.$$

Logo,

$$\begin{aligned} 0 &= \left\langle \mathbf{t}, (b_i - a_i)\,\mathbf{r}_i + (b_j + a_j)\,\mathbf{r}_j + \sum_{k\neq i,j} b_k\mathbf{r}_k \right\rangle \\ &= (b_i - a_i)\,\langle \mathbf{t}, \mathbf{r}_i\rangle + (b_j + a_j)\,\langle \mathbf{t}, \mathbf{r}_j\rangle + \sum_{k\neq i,j} b_k\langle \mathbf{t}, \mathbf{r}_k\rangle \\ &\geq a_j\langle \mathbf{t}, \mathbf{r}_j\rangle > 0, \end{aligned}$$

o que é uma contradição. Se $a_i > b_i$, então

$$(a_i - b_i)\,\mathbf{r}_i = (b_j + a_j)\,\mathbf{r}_j + \sum_{k\neq i,j} b_k\mathbf{r}_k. \tag{2.2}$$

Assim, dividindo a Equação (2.2) por $a_i - b_i$, obtemos que

$$\mathbf{r}_i = \frac{(b_j + a_j)}{(a_i - b_i)}\mathbf{r}_j + \sum_{k\neq i,j} \frac{b_k}{(a_i - b_i)}\mathbf{r}_k,$$

e, assim, $\Pi - \{\mathbf{r}_i\} \subset \Pi$ seria uma $\mathbf{t}$-base para $\Delta_{\mathbf{t}}^{+}$, o que contradiz a minimalidade de Π. Portanto, $\mathbf{x} \notin \Delta_{\mathbf{t}}^{+}$. De modo análogo, demonstra-se que $\mathbf{x} \notin \Delta_{\mathbf{t}}^{-}$, pois $\mathbf{x} \in \Delta_{\mathbf{t}}^{+} \Leftrightarrow -\mathbf{x} \in \Delta_{\mathbf{t}}^{-}$. ■

Proposição 2.5 *Sejam $\mathbf{r}_i, \mathbf{r}_j \in \Pi$, com $i \neq j$. Sejam S_i e S_j as reflexões ao longo de $\langle \mathbf{r}_i\rangle$ e $\langle \mathbf{r}_j\rangle$, respectivamente. Então $S_i(\mathbf{r}_j) \in \Delta_{\mathbf{t}}^{+}$ e $\langle \mathbf{r}_i, \mathbf{r}_j\rangle \leq 0$.*

Demonstração. Pela Proposição 2.2, temos que $S_i(\mathbf{r}_j) \in \Delta$. Logo, $S_i(\mathbf{r}_j) \in \Delta_{\mathbf{t}}^{+}$ ou $S_i(\mathbf{r}_j) \in \Delta_{\mathbf{t}}^{-}$. Como

$$S_i(\mathbf{r}_j) = \mathbf{r}_j - 2\frac{\langle \mathbf{r}_j, \mathbf{r}_i\rangle}{\langle \mathbf{r}_i, \mathbf{r}_i\rangle}\mathbf{r}_i$$

temos, pela Proposição 2.4, que

$$\frac{\langle \mathbf{r}_j, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle} \leq 0.$$

Assim,

$$\langle \mathbf{r}_i, \mathbf{r}_j \rangle \leq 0,$$

pois $\langle \mathbf{r}_i, \mathbf{r}_i \rangle > 0$. Portanto, $S_i(\mathbf{r}_j) \in \Delta_{\mathbf{t}}^+$. ■

Observação 2.1 *Geometricamente* $\langle \mathbf{r}_i, \mathbf{r}_j \rangle \leq 0$ *significa que o ângulo entre os vetores* $\mathbf{r}_i$ *e* $\mathbf{r}_j$ *é obtuso.*

Proposição 2.6 *Suponhamos que existam* $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m \in \mathbb{R}^n$ *tais que*

$$\langle \mathbf{x}_i, \mathbf{x} \rangle > 0, 1 \leq i \leq m,$$

para algum $\mathbf{x} \in \mathbb{R}^n$. *Se* $\langle \mathbf{x}_i, \mathbf{x}_j \rangle \leq 0$, *para* $i \neq j$, *então*

$$\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m\}$$

é linearmente independente.

Demonstração. Suponhamos, por absurdo, que

$$\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m\}$$

seja linearmente dependente. Então existem $c_1, \ldots, c_n$ escalares não todos nulos tais que

$$\sum_{i=1}^{m} c_i \mathbf{x}_i = \mathbf{0}.$$

Re-enumerando, se necessário, podemos supor que

$$\sum_{i=1}^{k} a_i \mathbf{x}_i = \sum_{i=k+1}^{m} b_i \mathbf{x}_i$$

com todos $a_i \geq 0$, $b_i \geq 0$ e algum $a_i > 0$. Então

$$0 \leq \left\| \sum_{i=1}^{k} a_i \mathbf{x}_i \right\|^2 = \left\langle \sum_{i=1}^{k} a_i \mathbf{x}_i, \sum_{j=1}^{k} a_j \mathbf{x}_j \right\rangle$$

$$= \left\langle \sum_{i=1}^{k} a_i \mathbf{x}_i, \sum_{j=k+1}^{m} b_j \mathbf{x}_j \right\rangle$$

$$= \sum_{i=1}^{k} \sum_{j=k+1}^{m} a_i b_j \langle \mathbf{x}_i, \mathbf{x}_j \rangle \leq 0.$$

Logo,

$$\sum_{i=1}^{k} a_i \mathbf{x}_i = \mathbf{0}.$$

Assim,

$$\begin{aligned} 0 &= \left\langle \sum_{i=1}^{k} a_i \mathbf{x}_i, \mathbf{x} \right\rangle \\ &= \sum_{i=1}^{k} a_i \langle \mathbf{x}_i, \mathbf{x} \rangle > 0, \end{aligned}$$

o que é uma contradição, pois $a_i > 0$ e $\langle \mathbf{x}_i, \mathbf{x} \rangle > 0$, para algum i. ■

Teorema 2.2 *Sejam G um grupo de reflexões finitas de $O(\mathbb{R}^n)$ e*

$$\Delta = \{\mathbf{r}_1, \ldots, \mathbf{r}_k\}$$

um sistema de raízes para G. Se Π é uma $\mathbf{t}$-base para Δ, então Π é uma base para $\mathbb{R}^n$.

Demonstração. Pela Proposição 2.3, $\mathbb{R}^n = \langle \Delta \rangle$. Como cada $\mathbf{r} \in \Delta$ é uma combinação linear das raízes em Π, temos que $\mathbb{R}^n = \langle \Pi \rangle$. Finalmente, pelas Proposições 2.5 e 2.6, temos que Π é linearmente independente. Portanto, Π é uma base para $\mathbb{R}^n$. ■

Proposição 2.7 *Existe apenas uma $\mathbf{t}$-base para Δ.*

Demonstração. Sejam

$$\Pi_1 = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\} \text{ e } \Pi_2 = \{\mathbf{s}_1, \ldots, \mathbf{s}_n\}$$

duas $\mathbf{t}$-bases para Δ. Então, pelo Teorema 2.2, Π_1 e Π_2 são bases para $\mathbb{R}^n$. Logo, existem únicos $b_{ij} \in \mathbb{R}_+$ tais que

$$\mathbf{s}_j = \sum_{i=1}^{n} b_{ij} \mathbf{r}_i, 1 \leq j \leq n.$$

De modo análogo, existem únicos $a_{ij} \in \mathbb{R}_+$ tais que

$$\mathbf{r}_j = \sum_{i=1}^{n} a_{ij} \mathbf{s}_i, 1 \leq j \leq n.$$

Logo,

$$\begin{aligned}\mathbf{r}_j &= \sum_{i=1}^{n} a_{ij}\mathbf{s}_i \\ &= \sum_{i=1}^{n}\left(a_{ij}\sum_{k=1}^{n} b_{ki}\mathbf{r}_k\right) \\ &= \sum_{k=1}^{n}\left(\sum_{i=1}^{n} a_{ij}b_{ki}\right)\mathbf{r}_k.\end{aligned}$$

Assim,

$$\sum_{i=1}^{n} a_{ij}b_{ki} = \begin{cases} 1 & \text{se } j = k \\ 0 & \text{se } j \neq k. \end{cases}$$

Se $\mathbf{A} = (a_{ij})$ é a matriz de mudança da base Π_2 para a base Π_1 e $\mathbf{B} = (b_{ij})$ é a matriz de mudança da base Π_1 para a base Π_2, então

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}. \tag{2.3}$$

Sejam

$$\mathbf{a}_i = (a_{i1}, \ldots, a_{in}) \text{ e } \mathbf{b}_j = (b_{1j}, \ldots, b_{nj})$$

as linhas e as colunas de $\mathbf{A}$ e $\mathbf{B}$, respectivamente. Então, pela Equação 2.3,

$$\langle \mathbf{a}_1, \mathbf{b}_j \rangle = 0, j = 2, \ldots, n,$$

em $\mathbb{R}^n$. Assim, existe no máximo um i tal que $b_{ij} = 0$, $j = 2, \ldots, n$, pois caso contrário, $\mathbf{b}_2, \ldots, \mathbf{b}_n$ seria linearmente dependentes, o que é impossível. Logo, $\mathbf{a}_1$ tem no máximo um $a_{1j} \neq 0$, $j = 1, 2, \ldots, n$. De modo análogo, demonstra-se que $\mathbf{a}_i$ tem no máximo um $a_{ij} \neq 0$, $j = 1, 2, \ldots, n$. Como $\mathbf{A}$ é invertível temos que existe exatamente um elemento positivo em cada linha e coluna de $\mathbf{A}$, Logo,

$$\mathbf{r}_j = a_{ij}\mathbf{s}_i, a_{ij} \in \mathbb{R}_+^*, 1 \leq i \leq n,$$

ou seja, toda raiz de Π_1 é um múltiplo positivo de uma raiz de Π_2. Pelo item 1. do Corolário 2.2, obtemos que $a_{ij} = 1$, assim, $\mathbf{A}$ é uma matriz de permutação. Portanto, $\Pi_1 = \Pi_2$. ■

Proposição 2.8 *Sejam*

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\}$$

a $\mathbf{t}$*-base para* Δ *e* S_i *a reflexão ao longo de* $\langle \mathbf{r}_i \rangle$*. Se* $\mathbf{r} \in \Delta_{\mathbf{t}}^+$*, com* $\mathbf{r} \neq \mathbf{r}_i$*, então* $S_i(\mathbf{r}) \in \Delta_{\mathbf{t}}^+$*, isto é,* $S_i(\Pi - \{\mathbf{r}_i\}) = \Pi - \{\mathbf{r}_i\}$.

Demonstração. Se $\mathbf{r} \in \Pi$, então pela Proposição 2.5 $S_i(\mathbf{r}) \in \Delta_{\mathbf{t}}^+$. Se $\mathbf{r} \notin \Pi$, então pelo Teorema 2.2, Π é um base para $\mathbb{R}^n$. Logo, existem únicos $a_i \in \mathbb{R}_+$ tais que

$$\mathbf{r} = \sum_{i=1}^{n} a_i \mathbf{r}_i$$

e pelo menos dois a_i são estritamente positivos. Assim, podemos assumir que $\mathbf{r}_i \neq \mathbf{r}_1$ e $a_1 > 0$. Logo,

$$\begin{aligned} S_i(\mathbf{r}) &= \sum_{j=1}^{n} a_j S_i(\mathbf{r}_j) \\ &= \sum_{j=1}^{n} a_j \left(\mathbf{r}_j - 2\frac{\langle \mathbf{r}_j, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle} \mathbf{r}_i \right) \\ &= a_1 \mathbf{r}_1 + \sum_{j=2}^{n} a_j \mathbf{r}_j - 2 \left(\sum_{j=1}^{n} a_j \frac{\langle \mathbf{r}_j, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle} \mathbf{r}_i \right). \end{aligned}$$

Como $S_i(\mathbf{r}) \in \Delta$ temos que $S_i(\mathbf{r}) \in \Delta_{\mathbf{t}}^+$ ou $S_i(\mathbf{r}) \in \Delta_{\mathbf{t}}^-$. Mas $a_1 > 0$ implica que todos os coeficientes de $S_i(\mathbf{r})$ são positivos, isto é, $S_i(\mathbf{r}) \in \Delta_{\mathbf{t}}^+$. ■

Corolário 2.3 *Sejam Δ_1^+ e Δ_2^+ sistemas de raízes positivas para Δ, relativo a um vetor $\mathbf{t}$. Então existe $S \in G$ tal que*

$$\Delta_2^+ = S(\Delta_1^+).$$

Demonstração. Sabemos que

$$\left|\Delta_1^+\right| = \left|\Delta_2^+\right| = \frac{1}{2}\left|\Delta\right|$$

Para demonstrar o corolário, vamos usar indução sobre

$$k = \left|\Delta_1^+ \cap (-\Delta_2^+)\right|$$

Se $k = 0$, então $\Delta_2^+ = \Delta_1^+$ e nada há para ser demonstrado. Suponhamos que o resultado seja válido para $k - 1$ e $k > 0$. Seja Π uma $\mathbf{t}$-base para Δ_1^+. Então

$$\Pi \cap \Delta_2^+ \neq \Pi,$$

pois $\Delta_1^+ \cap (-\Delta_2^+) \neq \emptyset$. Assim, podemos escolher $\mathbf{r} \in \Pi$ tal que $\mathbf{r} \in -\Delta_2^+$. Logo, pela Proposição 2.8, obtemos que

$$\left|S_{\mathbf{r}}(\Delta_1^+) \cap (-\Delta_2^+)\right| = \mathbf{r} - 1.$$

Logo, pela hipótese de indução, existe $T \in G$ tal que

$$\Delta_2^+ = T(S_{\mathbf{r}}(\Delta_1^+)).$$

Portanto, existe $S = TS_{\mathbf{r}} \in G$ tal que

$$\Delta_2^+ = S(\Delta_1^+).$$

■

Seja

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\}$$

uma $\mathbf{t}$-base para Δ e S_i a reflexão ao longo de $\langle \mathbf{r}_i \rangle$. Vamos denotar por $G_{\mathbf{t}}$ o grupo gerado por $S_1, \ldots, S_n$, isto é,

$$G_{\mathbf{t}} = \langle S_1, \ldots, S_n \rangle.$$

Proposição 2.9 *Seja $\mathbf{x} \in \mathbb{R}^n$ um vetor fixado. Então existe $T \in G_{\mathbf{t}}$ tal que $\langle T(\mathbf{x}), \mathbf{r}_i \rangle \geq 0$, para todo $\mathbf{r}_i \in \Pi$.*

Demonstração. Seja

$$\mathbf{x}_0 = \frac{1}{2} \sum_{\mathbf{r} \in \Delta_{\mathbf{t}}^+} \mathbf{r}$$

Como G é um grupo finito temos que existe $T \in G$ tal que $\langle T(\mathbf{x}), \mathbf{x}_0 \rangle$ seja maximal. Seja S_i é reflexão ao longo de $\langle \mathbf{r}_i \rangle$, onde $\mathbf{r}_i \in \Pi \subseteq \Delta_{\mathbf{t}}^+$. Então, pela Proposição 2.8, temos, para $\mathbf{r} \neq \mathbf{r}_i$, que $S_i(\mathbf{r}) \in \Delta_{\mathbf{t}}^+$ e

$$\begin{aligned}
S_i(\mathbf{x}_0) &= S_i\left(\frac{1}{2}\mathbf{r}_i + \frac{1}{2}\sum_{\mathbf{r} \in \Delta_{\mathbf{t}}^+} \mathbf{r}\right) \\
&= \left(\frac{1}{2}S_i(\mathbf{r}_i) + \frac{1}{2}\sum_{\mathbf{r} \in \Delta_{\mathbf{t}}^+} S_i(\mathbf{r})\right) \\
&= -\frac{1}{2}\mathbf{r}_i + \frac{1}{2}\sum_{\mathbf{r} \in \Delta_{\mathbf{t}}^+} \mathbf{r} \\
&= -\frac{1}{2}\mathbf{r}_i - \frac{1}{2}\mathbf{r}_i + \frac{1}{2}\mathbf{r}_i + \frac{1}{2}\sum_{\mathbf{r} \in \Delta_{\mathbf{t}}^+} \mathbf{r} \\
&= -\mathbf{r}_i + \mathbf{x}_0.
\end{aligned}$$

Assim, pela maximilidade de $\langle T(\mathbf{x}), \mathbf{x}_0 \rangle$, obtemos que

$$\begin{aligned} \langle T(\mathbf{x}), \mathbf{x}_0 \rangle &\geq \langle S_i T(\mathbf{x}), \mathbf{x}_0 \rangle \\ &= \langle T(\mathbf{x}), S_i(\mathbf{x}_0) \rangle \\ &= \langle T(\mathbf{x}), \mathbf{x}_0 - \mathbf{r}_i \rangle \\ &= \langle T(\mathbf{x}), \mathbf{x}_0 \rangle - \langle T(\mathbf{x}), \mathbf{r}_i \rangle . \end{aligned}$$

Portanto,

$$\langle T(\mathbf{x}), \mathbf{r}_i \rangle \geq 0, \forall \mathbf{r}_i \in \Pi.$$

■

Proposição 2.10 *Seja* $\mathbf{r} \in \Delta_{\mathbf{t}}^+$. *Então* $T(\mathbf{r}) \in \Pi$, *para algum* $T \in G_{\mathbf{t}}$.

Demonstração. Como $\Pi \subseteq \Delta_{\mathbf{t}}^+$ temos que $\mathbf{r} \in \Pi$ ou $\mathbf{r} \notin \Pi$. Se $\mathbf{r} \in \Pi$, então existe $T = I \in G_{\mathbf{t}}$ tal que $T(\mathbf{r}) = \mathbf{r} \in \Pi$. Se $\mathbf{r} \notin \Pi$, então pelas Proposições 2.5 e 2.6 e pelo Teorema 2.2, obtemos que

$$\langle \mathbf{r}, \mathbf{r}_{i_1} \rangle > 0$$

para alguma raiz $\mathbf{r}_{i_1} \in \Pi$, caso contrário, $\Pi \cup \{\mathbf{r}\}$ seria linearmente independente, o que é impossível pois Π é uma base de $\mathbb{R}^n$. Seja

$$\mathbf{a}_1 = S_i(\mathbf{r}) = \mathbf{r} - 2\frac{\langle \mathbf{r}, \mathbf{r}_{i_1} \rangle}{\langle \mathbf{r}_{i_1}, \mathbf{r}_{i_1} \rangle}\mathbf{r}_{i_1}.$$

Então, pela Proposição 2.8, obtemos que $\mathbf{a}_1 \in \Delta_{\mathbf{t}}^+$ e

$$\begin{aligned} \langle \mathbf{a}_1, \mathbf{t} \rangle &= \langle \mathbf{r} - 2\frac{\langle \mathbf{r}, \mathbf{r}_{i_1} \rangle}{\langle \mathbf{r}_{i_1}, \mathbf{r}_{i_1} \rangle}\mathbf{r}_{i_1}, \mathbf{t} \rangle \\ &= \langle \mathbf{r}, \mathbf{t} \rangle - 2\frac{\langle \mathbf{r}, \mathbf{r}_{i_1} \rangle}{\langle \mathbf{r}_{i_1}, \mathbf{r}_{i_1} \rangle} \langle \mathbf{r}_{i_1}, \mathbf{t} \rangle \\ &< \langle \mathbf{r}, \mathbf{t} \rangle \end{aligned}$$

Se $\mathbf{a}_1 \in \Pi$, então existe

$$T = S_{i_1} \in G_t.$$

tal que $T(\mathbf{a}_1) \in \Pi$. Se $\mathbf{a}_1 \notin \Pi$, aplicando o processo acima para $\mathbf{a}_1$, obtemos $\mathbf{r}_{i_2} \in \Pi$ e

$$\mathbf{a}_2 = S_{i_2}(\mathbf{a}_1) = S_{i_2} S_{i_1}(\mathbf{r}) \in \Delta_{\mathbf{t}}^+$$

com $\langle \mathbf{a}_2, \mathbf{t} \rangle < \langle \mathbf{a}_1, \mathbf{t} \rangle$. Se $\mathbf{a}_2 \in \Pi$, então existe

$$T = S_{i_2} S_{i_1} \in G_t$$

tal que $T(\mathbf{a}_2) \in \Pi$. Continuando o processo acima (em no máximo $\left|\Delta_{\mathbf{t}}^{+}\right|$ etapas) obtemos $\mathbf{a}_k \in \Pi$ e

$$\mathbf{a}_k = S_{i_k}(\mathbf{a}_{k-1}) = S_{ik} \cdots S_{i_1}(\mathbf{r})$$

com

$$\langle \mathbf{a}_k, \mathbf{t} \rangle < \cdots < \langle \mathbf{a}_2, \mathbf{t} \rangle < \langle \mathbf{a}_1, \mathbf{t} \rangle .$$

Portanto, existe

$$T = S_{i_k} \cdots S_{i_1} \in G_t$$

tal que $T(\mathbf{a}_k) \in \Pi$. ■

Proposição 2.11 *$G = G_t$.*

Demonstração. Como

$$G = \langle S_r : \mathbf{r} \in \Delta \rangle \text{ e } S_{-\mathbf{r}} = S_{\mathbf{r}}$$

basta demonstrar que se $\mathbf{r} \in \Delta_{\mathbf{t}}^{+}$, então $S_{\mathbf{r}} \in G_t$. Suponhamos que $\mathbf{r} \in \Delta_{\mathbf{t}}^{+}$. Então, pela Proposição 2.10, existe $T \in G_t$ tal que $T(\mathbf{r}) \in \Pi$. Escolhendo

$$T(\mathbf{r}) = \mathbf{r}_i$$

obtemos pela Proposição 2.2 que

$$S_{\mathbf{r}} = T^{-1} S_i T \in G_t$$

■

Proposição 2.12 *Sejam*

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\}$$

uma $\mathbf{t}$-base para Δ e $\mathbf{r}_i, \mathbf{r}_j \in \Pi$. Então existe um inteiro $p_{ij} \geq 1$ tal que

$$\frac{\langle \mathbf{r}_i, \mathbf{r}_j \rangle}{\|\mathbf{r}_i\| \, \|\mathbf{r}_j\|} = -\cos\left(\frac{\pi}{p_{ij}}\right),$$

onde $(S_{\mathbf{r}_i} S_{\mathbf{r}_j})^{p_{ij}} = I$.

Demonstração. Se $i = j$, então existe $p_{ij} = 1$. Suponhamos que $i \neq j$ e W o subespaço gerado por $\mathbf{r}_i$ e $\mathbf{r}_j$. Então W é um subespaço de $\mathbb{R}^n$ com $\dim W = 2$. Sejam $S_i = S_{\mathbf{r}_i}$ e $S_j = S_{\mathbf{r}_j}$ as reflexões ao longo de $\langle \mathbf{r}_i \rangle$ e $\langle \mathbf{r}_j \rangle$, respectivamente. Seja

$$\mathcal{H} = \langle S_i, S_j \rangle \leq G.$$

Como

$$S_i|_{W^\perp} = S_j|_{W^\perp} = I$$

temos que

$$\mathcal{H} \simeq H_2^m \times \{I\},$$

onde $\mathcal{H}_2^m$ é um grupo diedral em $O(W)$. Seja

$$\mathbf{t} = \mathbf{t}_1 + \mathbf{t}_2,$$

com $\mathbf{t}_1 \in W$ e $\mathbf{t}_2 \in W^\perp$.

Afirmação: $\{\mathbf{r}_i, \mathbf{r}_j\}$ é uma $\mathbf{t}_1$-base para H_2^m en W.
De fato, se $\{\mathbf{r}_i, \mathbf{r}_j\}$ não for uma $\mathbf{t}_1$-base para H_2^m en W, então podemos escolher uma raiz $\mathbf{r}$ de H_2^m em W tal que $\{\mathbf{r}, \mathbf{r}_j\}$ seja uma $\mathbf{t}_1'$-base para H_2^m, para algum $\mathbf{t}_1' \in W$, onde $\mathbf{r}, \mathbf{r}_i$ e $\mathbf{r}_j$ são todos $\mathbf{t}_1'$-positivo. Considerado como um espaço vetorial em $\mathbb{R}^n$, $\mathbf{r}$ é uma raiz de $\mathcal{H}$ e, assim, de G. Logo, existem $a_i, a_j \in \mathbb{R}_+^*$ tais que

$$\mathbf{r} = a_i\mathbf{r}_i - b_j\mathbf{r}_j,$$

o que é impossível, pela Proposição 2.4.

O menor dos ângulos entre os vetores duais de $\mathbf{r}_i$ e $\mathbf{r}_j$ em W deve ser $\frac{2\pi}{2m}$, pois o cone gerado por eles é uma região fundamental para H_2^m. Se θ é o menor dos ângulos entre $\mathbf{r}_i$ e $\mathbf{r}_j$, então $\theta = \pi - \varphi$. Seja $p_{ij} = m$. Então

$$\begin{aligned} \frac{\langle \mathbf{r}_i, \mathbf{r}_j \rangle}{\|\mathbf{r}_i\| \, \|\mathbf{r}_j\|} &= \cos\theta \\ &= \cos(\pi - \varphi) \\ &= -\cos\varphi \\ &= -\cos\left(\frac{\pi}{p_{ij}}\right). \end{aligned}$$

Finalmente, pelo item 2. da Observação 1.3, obtemos que $(S_{\mathbf{r}_i} S_{\mathbf{r}_j})^{p_{ij}} = I$. ■

Observação 2.2 *Pelas Proposições* 2.11 *e* 2.12, *obtemos que*

$$G = \left\langle S_{\mathbf{r}_i} : \mathbf{r}_i \in \Pi \ \ e \ \ S_{\mathbf{r}_i}^2 = I, S_{\mathbf{r}_j}^2 = I, (S_{\mathbf{r}_i} S_{\mathbf{r}_j})^{p_{ij}} = I \right\rangle.$$

Pela Observação 2.2, todo elemento de $S \in G$ pode ser escrito na forma

$$S = S_{\mathbf{r}_1} \cdots S_{\mathbf{r}_k}, \mathbf{r}_i \in \Pi, i = 1, \ldots, k.$$

Definimos o *comprimento* de $S \in G$, denotado por $l(S)$, como o menor inteiro positvo k, para o qual uma expressão

$$S = S_{\mathbf{r}_1} \cdots S_{\mathbf{r}_k}$$

exista. Convencionamos que $l(I) = 0$. Note que $l(S) = 1$ se, e somente se, $T = S_{\mathbf{r}}$, para algum $\mathbf{r} \in \Delta$. É fácil verificar que

$$\begin{aligned} l(S) &= l\left(S^{-1}\right) \\ \det(S) &= (-1)^{l(S)}. \end{aligned}$$

Assim, $l(ST)$ e $l(S) + l(T)$ têm a mesma paridade, isto é,

$$l(ST) \leq l(S) + l(T) \text{ e } l(S) + l(T) \equiv l(ST) \pmod 2.$$

Seja Δ um sistema de raízes para G. O número de raízes positivas enviadas em raízes negativas por $S \in G$, denotado por $n(S)$, é definido como

$$n(S) = \left|\Delta_{\mathbf{t}}^+ \cap S^{-1}(\Delta_{\mathbf{t}}^-)\right|.$$

Note que $n(S) = n(S^{-1})$, pois

$$\begin{aligned} \Delta_{\mathbf{t}}^+ \cap S^{-1}(\Delta_{\mathbf{t}}^-) &= S^{-1}(S(\Delta_{\mathbf{t}}^+) \cap \Delta_{\mathbf{t}}^-) \\ &= -S^{-1}(\Delta_{\mathbf{t}}^+ \cap S(\Delta_{\mathbf{t}}^-)) \end{aligned}$$

Teorema 2.3 (Iwahori) *Sejam*

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\}$$

uma $\mathbf{t}$*-base para* Δ *e* $S_i = S_{\mathbf{r}_i}$ *as reflexões ao longo de* $\langle \mathbf{r}_i \rangle$*, respectivamente. Se* $S \in G$*, Então*

$$n(SS_i) = \begin{cases} n(S) + 1 & se\ , S(\mathbf{r}_i) \in \Delta_{\mathbf{t}}^+ \\ n(S) - 1 & se\ , S(\mathbf{r}_i) \in \Delta_{\mathbf{t}}^- \end{cases}$$

e

$$n(S_iS) = \begin{cases} n(S) + 1 & se\ , S^{-1}(\mathbf{r}_i) \in \Delta_{\mathbf{t}}^+ \\ n(S) - 1 & se\ , S^{-1}(\mathbf{r}_i) \in \Delta_{\mathbf{t}}^- \end{cases}.$$

■

Observação 2.3 *Pode ser demonstrado que* $n(S) = l(S)$*, para todo* $S \in G$*.*

A presentação de G obtido na Observação 2.2, demonstra que G é determinado, a menos de isomorfismo, pelos inteiros p_{ij}, associados a $\mathbf{r}_i, \mathbf{r}_j \in \Pi$. Um maneira conveniente para decodificar estas informações em uma figura é a construção de um gráfico Γ, o qual é chamado um *gráfo Coxeter* de G.

Capítulo 3

Códigos de Grupo Ótimos

Neste capítulo descreveremos como a cardinalidade $M = |C|$ e a distância mínima Euclidiana $d_{\min}$ de um "código de grupo" de um grupo de reflexão finito pode ser calculada facilmente. Estes resultados são a chave para a construção de códigos de grupo ótimos.

3.1 Introdução

Neste seção apresentaremos algumas definições e reultados básicos sobre códigos de grupo, o leitor interessado em mais detalhes pode consultar [1].

Um (M, n)-*código esférico* é um subconjunto

$$\mathbf{S} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M\}$$

de vetores distintos de $\mathbb{R}^n$ tais que:

1. $\mathbf{S}$ gera $\mathbb{R}^n$ como um espaço vetorial ($n \leq M$);

2. Todos os vetores de $\mathbf{S}$ tem a mesma norma, isto é, estão sobre uma esfera de raio r.

Um (M, n)-*código de grupo* C é um (M, n)-código esférico tal que existe um subgrupo finito G de $O(n, \mathbb{R})$ ($O(\mathbb{R}^n)$) e um vetor unitário $\mathbf{x} \in \mathbb{R}^n$ tal que

$$O(\mathbf{x}) = \{\mathbf{O}\mathbf{x}^t : \mathbf{O} \in G\} = C$$

ou, equivalentemente, C é a órbita de $\mathbf{x}$. Neste caso.

$$|O(\mathbf{x})| = \frac{|G|}{|G_{\mathbf{x}}|}.$$

O código de grupo C é dito gerado pelo *vetor inicial* $\mathbf{x}$ *e o grupo* G. Além disso, a *taxa normalizada* do código de grupo C é dada por

$$R = \frac{1}{n}\log_2 M$$

bits por dimensão.

Dado $\mathbf{x} \in C$, a *região de decisão* associada a $\mathbf{x}$ é dada por

$$\begin{aligned} V(\mathbf{x}) &= \{\mathbf{z} \in \mathbb{R}^n : \|\mathbf{z}-\mathbf{x}\| \leq \|\mathbf{z}-\mathbf{y}\|, \forall \mathbf{y} \in C\} \\ &= \{\mathbf{z} \in \mathbb{R}^n : \langle \mathbf{z}, \mathbf{x}-\mathbf{y}\rangle \geq 0, \forall \mathbf{y} \in C\}. \end{aligned}$$

Note que, $V(\mathbf{x})$ satisfaz às seguintes condições:

1. $V(\mathbf{x}) + V(\mathbf{x}) \subseteq V(\mathbf{x})$;
2. $\mathbb{R}_+ V(\mathbf{x}) \subseteq V(\mathbf{x})$;
3. $\overline{V(\mathbf{x})} = V(\mathbf{x})$.

Além disso, $W = V(\mathbf{x}) \cap (-V(\mathbf{x}))$ é o maior subespaço de $\mathbb{R}^n$ contido em $V(\mathbf{x})$.

Observação 3.1 *Uma das vantagens de usar um código de grupo é que todas as palavras código têm a mesma probabilidade de erro e a mesma disposição de palavras código vizinhas.*

Teorema 3.1 *Seja C um (M,n)-código de grupo em $\mathbb{R}^n$. Então*:

1. *Todas as regiões fundamentais de C são congruentes, isto é, $\mathbf{O}V(\mathbf{x}) = V(\mathbf{Ox})$, para todo $\mathbf{O} \in G$;*
2. *Todas as palavras código têm a mesma probabilidade de erro*;
3. *O grupo G é isomorfo a um subgrupo transitivo do grupo das permutações em S_M.*

Demonstração. 1. Seja $C = \{\mathbf{x}_1, \ldots, \mathbf{x}_M\}$ um código de grupo em $\mathbb{R}^n$. Sejam $\mathbf{x}_i$ e $\mathbf{x}_j \in C$ com $i \neq j$. Por hipótese, existe $\mathbf{O} \in G$ tal que $\mathbf{Ox}_i = \mathbf{x}_j$. Dado $\mathbf{x} \in R_i$, temos que:

$$\begin{aligned} N(\mathbf{Ox}-\mathbf{x}_j) &= N(\mathbf{Ox}-\mathbf{Ox}_i) \\ &= N(\mathbf{x}-\mathbf{x}_i) \\ &\leq N(\mathbf{x}-\mathbf{x}_k) \\ &= N(\mathbf{Ox}-\mathbf{Ox}_k) \\ &= N(\mathbf{Ox}-\mathbf{x}_l), \end{aligned}$$

onde $j \neq l$ e $\mathbf{x}_l = \mathbf{O}\mathbf{x}_k, \forall \mathbf{x}_k \in C$. Logo, $\mathbf{O}\mathbf{x} \in R_j$. Portanto, $F_j = \mathbf{O}(F_i)$, onde $\mathbf{O} \in G$. 2. Segue de 1. Finalmente, vamos demonstrar 3. Dados $\mathbf{x}_i$ e $\mathbf{x}_j \in C$. Então existe $\mathbf{O} \in G$ tal que $\mathbf{O}\mathbf{x}_i = \mathbf{x}_j$, isto é, $\mathbf{O}$ corresponde a uma permutação $\sigma \in S_M$ tal que $\sigma(i) = j$. Logo, G é isomorfo a um subgrupo transitivo de S_M , pois

$$C = \{\mathbf{O}\mathbf{x} : \mathbf{O} \in G\},$$

para algum $\mathbf{x} \in C$. ■

3.2 Determinação do Vetor Inicial Ótimo

Nesta seção apresentamos as condições para a determinação do vetor inicial ótimo $\mathbf{x}_0$ para um código de grupo, restrito aos grupos de Coxeter irredutíveis. Mostraremos que as regiões de decisão são unicamente determinadas pelo estabilizador $G_{\mathbf{x}_0}$, que assegura a existencia de uma única solução para o problema do vetor inicial. O Corolário do Teorema 3.3 determina a distância mínima do código C em função do vetor inicial. O leitor interessado em mais detalhes pode consultar [7, 9].

Seja G um grupo de reflexão finito com sistema de raízes fixado Δ. Em todo este capítulo

$$V_\Delta = \langle \Delta \rangle.$$

denota o subespaço de $\mathbb{R}^n$ gerado por Δ, no qual G age efetivamente. Seja

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\}$$

uma $\mathbf{t}$-base fixada para G. Então a cada hiperplano $H_{\mathbf{r}_i}$, $\mathbf{r}_i \in \Pi$, está associado dois semi-espaços abertos

$$H^+_{\mathbf{r}_i} = \{\mathbf{x} \in V_\Delta : \langle \mathbf{x}, \mathbf{r}_i \rangle > 0\} \text{ e } H^-_{\mathbf{r}_i} = \{\mathbf{x} \in V_\Delta : \langle \mathbf{x}, \mathbf{r}_i \rangle < 0\}.$$

Então, pelo Teorema 2.1, o conjunto

$$\begin{aligned} F_\Pi &= \bigcap_{i=1}^{n} H^+_{\mathbf{r}_i} \\ &= \{\mathbf{x} \in V_\Delta : \langle \mathbf{x}, \mathbf{r}_i \rangle > 0, i = 1, \ldots, n\} \end{aligned} \tag{3.1}$$

é uma região fundamental para G.

Seja

$$\{\mathbf{s}_1, \ldots, \mathbf{s}_n\}$$

a base dual para a base Π, isto é,

$$\langle \mathbf{r}_i, \mathbf{s}_j \rangle = \delta_{ij}.$$

Assim, uma caracterização alternativa para F_Π é dada por

$$\overline{F}_\Pi = \left\{ \mathbf{x} \in V_\Delta : \mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{s}_i \text{ e } x_i \in \mathbb{R}_+ \right\}, \tag{3.2}$$

pois se $\mathbf{x} \in \overline{F}_\Pi$, então $\langle \mathbf{x}, \mathbf{r}_i \rangle \geq 0$, $i = 1, \ldots, n$. Como

$$\{\mathbf{s}_1, \ldots, \mathbf{s}_n\}$$

é uma base para $\mathbb{R}^n$ temos que existem únicos $x_i \in \mathbb{R}$ tais que

$$\mathbf{x} = \sum_{i=1}^{n} x_i \mathbf{s}_i.$$

Logo,

$$\begin{aligned} \langle \mathbf{x}, \mathbf{r}_j \rangle &= \left\langle \sum_{i=1}^{n} x_i \mathbf{s}_i, \mathbf{r}_j \right\rangle \\ &= \sum_{i=1}^{n} x_i \langle \mathbf{s}_i, \mathbf{r}_j \rangle \\ &= \sum_{i=1}^{n} x_i \delta_{ij} \\ &= x_j, \end{aligned}$$

isto é, $x_i \in \mathbb{R}_+$, $i = 1, \ldots, n$.

Exemplo 3.1 *É fácil verificar que a base dual para a* $\mathbf{t}$*-base* $\Pi = \{\mathbf{r}_1, \mathbf{r}_2\}$ *dada no Exemplo* 2.4 *é formada pelos vetores*

$$\mathbf{s}_1 = (\frac{1}{\sqrt{3}}, 1) \text{ e } \mathbf{s}_2 = (\frac{2}{\sqrt{3}}, 0).$$

Logo,

$$\mathbf{x} \in \overline{F}_\Pi \Leftrightarrow \mathbf{x} = x_1 \mathbf{s}_1 + x_2 \mathbf{s}_2 \text{ e } x_1, x_2 \in \mathbb{R}_+,$$

isto é,

$$\mathbf{x} = (\frac{1}{\sqrt{3}} x_1 + \frac{2}{\sqrt{3}} x_2, x_1) \text{ e } x_1, x_2 \in \mathbb{R}_+.$$

Portanto,

$$\overline{F}_\Pi = \left\{ (\frac{1}{\sqrt{3}}x_1 + \frac{2}{\sqrt{3}}x_2, x_1) \in \mathbb{R}^2 : x_1, x_2 \in \mathbb{R}_+ \right\}$$

é uma região fundamental para $G = H_2^3$*, a qual é caracterizado pela Equação* (3.1) *ou* (3.2)*. Além disso, pelo item* 2. *da definição de região fundamental, o estabilizador de todo* $\mathbf{x} \in \overline{F}_\Pi$*, é dado por*

$$G_{\mathbf{x}} = \{S \in G : S(\mathbf{x}) = \mathbf{x}\} = \{I\},$$

Lema 3.1 *Seja* Π *a* $\mathbf{t}$*-base de* G*. Então para cada* $\mathbf{y} \in \mathbb{R}^n$ *existem* $S \in G$ *e* $\mathbf{x} \in \overline{F}_\Pi$ *tal que* $\mathbf{x} = S(\mathbf{y})$*. Além disso,*

$$\mathbf{x} - \mathbf{y} = \sum_{i=1}^{n} a_i \mathbf{r}_i,$$

onde $\mathbf{r}_i \in \Pi$ *e* $a_i \in \mathbb{R}_+$*.*

Demonstração. Dados $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, vamos definir

$$\mathbf{y} \leq \mathbf{x} \Leftrightarrow \mathbf{x} - \mathbf{y} = \sum_{i=1}^{n} a_i \mathbf{r}_i,$$

onde $\mathbf{r}_i \in \Pi$ e $a_i \in \mathbb{R}_+$. Então é facil verificar que $\leq$ é uma relação de ordem parcial em $\mathbb{R}^n$. Seja

$$X_{\mathbf{y}} = \{\mathbf{z} \in \mathbb{R}^n : \mathbf{y} \leq \mathbf{z} \text{ e } \mathbf{z} = S(\mathbf{y}), \text{ para algum } S \in G\}.$$

Então $X_{\mathbf{y}} \neq \emptyset$, pois $\mathbf{y} \in X_{\mathbf{y}}$. Assim, $X_{\mathbf{y}}$ contém um elemento maximal, digamos $\mathbf{x} \in X_{\mathbf{y}}$, isto é, $\mathbf{y} \leq \mathbf{x}$ e $\mathbf{x} = T(\mathbf{y})$, para algum $T \in G$. Se $\mathbf{r}_i \in \Pi$, então

$$S_{\mathbf{r}_i}(\mathbf{x}) = \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle}\mathbf{r}_i,$$

ou seja, $S_{\mathbf{r}_i}(\mathbf{x}) \in X_{\mathbf{y}}$, pois

$$\mathbf{y} \leq \mathbf{x} = S_{\mathbf{r}_i}(\mathbf{x}) + 2\frac{\langle \mathbf{x}, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle}\mathbf{r}_i \text{ e } S_{\mathbf{r}_i}(\mathbf{x}) = (S_{\mathbf{r}_i} T)(\mathbf{y}).$$

Logo, pela a maximalidade de $\mathbf{x}$, obtemos que $S_{\mathbf{r}_i}(\mathbf{x}) \leq \mathbf{x}$. Assim,

$$\mathbf{x} - S_{\mathbf{r}_i}(\mathbf{x}) = 2\frac{\langle \mathbf{x}, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle}\mathbf{r}_i \Rightarrow \langle \mathbf{x}, \mathbf{r}_i \rangle \geq 0, i = 1, \ldots n.$$

Portanto, $\mathbf{x} \in \overline{F}_\Pi$. ■

Teorema 3.2 *Seja* Π *a* $\mathbf{t}$*-base de* G*. Então*:

1. *Se* $\mathbf{x}, \mathbf{y} \in \overline{F}_\Pi$ *e* $T(\mathbf{x}) = \mathbf{y}$*, para algum* $T \in G$*, então* $\mathbf{x} = \mathbf{y}$ *e* T *é um produto de reflexões simples fixando* $\mathbf{x}$*. Em particular, se* $\mathbf{x} \in F_\Pi$*, então* $G_{\mathbf{x}} = \{I\}$;

2. Se $\mathbf{y} \in \mathbb{R}^n$*, então* $G_{\mathbf{y}}$ *é gerado por* $S_{\mathbf{r}} \in G_{\mathbf{y}}$*, com* $\mathbf{r} \in \Delta$;

3. Sejam W *um subespaço qualquer de* $\mathbb{R}^n$ *e*

$$\begin{aligned} H &= \{S \in G : S(\mathbf{x}) = \mathbf{x}, \forall \mathbf{x} \in W\} \\ &= \bigcap_{i=1}^{m} G_{\mathbf{x}_i}, \end{aligned}$$

onde $\{\mathbf{x}_1, \ldots, \mathbf{x}_m\}$ *é uma base de* W*. Então* H *é gerado por* $S_{\mathbf{r}} \in H$*, com* $\mathbf{r} \in \Delta$*.*

Demonstração. Para demonstrar 1., usaremos indução sobre

$$l(T) = n(T) = \left|\Delta_{\mathbf{t}}^{+} \cap T^{-1}(\Delta_{\mathbf{t}}^{-})\right|.$$

Se $n(T) = 0$, então $T = I$ e nada há para demonstrar. Se $n(T) > 0$, então $T(\mathbf{r}) \in \Delta_{\mathbf{t}}^{-}$, para algum $\mathbf{r} \in \Pi$, pois $\Delta_{\mathbf{t}}^{+} \cap T^{-1}(\Delta_{\mathbf{t}}^{-}) \neq \emptyset$. Pelo Teorema 2.3, obtemos que

$$n(TS_{\mathbf{r}}) = n(T) - 1.$$

Além disso, como $\mathbf{x}, \mathbf{y} \in \overline{F}_{\Pi}$ e com $T(\mathbf{r}) < 0$, temos que

$$0 \geq \langle \mathbf{y}, T(\mathbf{r}) \rangle = \left\langle T^{-1}(\mathbf{y}), T^{-1}T(\mathbf{r}) \right\rangle = \langle \mathbf{x}, \mathbf{r} \rangle \geq 0.$$

Assim, $\langle \mathbf{x}, \mathbf{r} \rangle = 0$ e $S_{\mathbf{r}}(\mathbf{x}) = \mathbf{x}$. Portanto,

$$TS_{\mathbf{r}}(\mathbf{x}) = \mathbf{y}.$$

Logo, pela hipótese de indução, $\mathbf{x} = \mathbf{y}$ e $TS_{\mathbf{r}}$ é um produto de reflexões simples fixando $\mathbf{x}$, de modo que T também é um produto de reflexões simples fixando $\mathbf{x}$.

2. Dado $\mathbf{y} \in \mathbb{R}^n$, pelo o Lema 3.1, existe $T \in G$ tal que $\mathbf{x} = T(\mathbf{y}) \in \overline{F}_{\Pi}$. Assim, pelo item 1, $G_{\mathbf{x}}$ é gerado por $S_{\mathbf{r}} \in G_{\mathbf{x}}$, com $\mathbf{r} \in \Delta$. É fácil verificar que

$$T^{-1}G_{\mathbf{x}}T = G_{\mathbf{y}}$$

Como o conjugado de reflexões simples são novamente reflexões simples, com respeito as raízes, temos que $G_{\mathbf{y}}$ é gerado por $S_{\mathbf{r}} \in G_{\mathbf{y}}$, com $\mathbf{r} \in \Delta$.

Finalmente, para provar 3., usaremos indução sobre m. Se $m = 1$, então segue do item 2. Suponhamos que o resultado seja válido para $m - 1$ e $m > 1$. Conhecemos que $G_{\mathbf{x}_1}$ é gerado por $S_{\mathbf{r}} \in G_{\mathbf{x}_1}$, com $\mathbf{r} \in \Delta_1 \subseteq \Delta$ e $\mathbf{r}, -\mathbf{r} \in \Delta_1$. Logo, pela Proposição 2.8, obtemos

que $S(\mathbf{r}) = \mathbf{r}$, para todo $\mathbf{r} \in \Pi_1$ e $S \in G_{\mathbf{x}_1}$. Assim, fazendo $W' = \langle \Delta_1 \rangle$ um subespaço de $\mathbb{R}^n$, obtemos, pela hipótese de indução, que

$$H' = \bigcap_{i=2}^{m} G_{\mathbf{x}_i}$$

é gerado por $S_{\mathbf{r}} \in H'$, com $\mathbf{r} \in \Pi_1$. Portanto,

$$G_{\mathbf{x}_1} \subseteq \bigcap_{i=1}^{m} G_{\mathbf{x}_i}$$

e $H = H'$. ■

Seja $\mathbf{x} \in \overline{F}_{\Pi}$. Então $G_{\mathbf{x}}$ é um grupo de reflexões finita. Assim, existe um único, a menos de isomorfismo, gráfo de Coxeter Γ_P associado a $G_{\mathbf{x}}$, o qual é um subgráfo do gráfo de Coxeter Γ para G. Neste caso, o conjunto de vértices Π_P de Γ_P é dado por

$$\Pi_P = \{\mathbf{r} \in \Pi : S_{\mathbf{r}}(\mathbf{x}) = \mathbf{x}\}$$

e será chamado de *raízes passivas* ou, equivalentemente,

$$\Pi_P = \{\mathbf{r} \in \Pi : \langle \mathbf{r}, \mathbf{x} \rangle = 0\},$$

pois

$$\mathbf{x} = S_{\mathbf{r}}(\mathbf{x}) = \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{r} \rangle}{\langle \mathbf{r}, \mathbf{r} \rangle}\mathbf{r} \Rightarrow \langle \mathbf{r}, \mathbf{x} \rangle = 0.$$

O subgráfo Γ_P decompõe-se em componentes conexas Γ_i, isto é,

$$\Gamma_P = \Gamma_1 \dot{\cup} \Gamma_2 \dot{\cup} \cdots \dot{\cup} \Gamma_l.$$

Assim, $G_{\mathbf{x}}$ é isomorfo ao produto direto dos grupos de reflexões finitas G_i, determinados por Γ_i. Em particular,

$$|G_{\mathbf{x}}| = |G_1| \cdots |G_l| \tag{3.3}$$

Corolário 3.1 *Seja*

$$C = \{T(\mathbf{x}) : T \in G\}$$

um código de grupo. Suponhamos que o gráfo de Coxeter Γ_P para $G_{\mathbf{x}}$ seja decomposto em subgráfos de Coxeter Γ_i , $i = 1, \ldots, l$, e seja G_i associados aos Γ_i . Então

$$|C| = \frac{|G|}{|G_{\mathbf{x}}|} = \frac{|G|}{|G_1| \cdots |G_l|}.$$

■

Lema 3.2 *Sejam* Π *uma* $\mathbf{t}$*-base para* G *e* $S_{\mathbf{r}_i}$ *as reflexões simples, com* $\mathbf{r}_i \in \Pi$. *Sejam* $\mathbf{x} \in \overline{F}_\Pi$ *e* $\mathbf{y} \in V_\Delta$ *tal que* $\mathbf{y} \in T(\overline{F}_\Pi)$, *para algum* $T \in G$. *Suponhamos que* $\mathbf{r}_i \in \Pi$ *satisfaça*

$$l\left(S_{\mathbf{r}_i}T\right) = l\left(T\right) - 1.$$

Então $S_{\mathbf{r}_i}(\mathbf{x}) = \mathbf{x}$ *ou* $S_{\mathbf{r}_i}(\mathbf{y}) = \mathbf{y}$, *ou caso contrário,*

$$d\left(\mathbf{x}, \mathbf{y}\right) > d\left(\mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y})\right).$$

Em particular,

$$d\left(\mathbf{x}, \mathbf{y}\right) \geq d\left(\mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y})\right).$$

Demostração. Seja $T \in G$. Então

$$\begin{aligned} d^2(\mathbf{x}, T(\mathbf{y})) &= \|\mathbf{x} - T(\mathbf{y})\|^2 \\ &= \langle \mathbf{x}, \mathbf{x} \rangle + \langle T(\mathbf{y}), T(\mathbf{y}) \rangle - 2 \langle \mathbf{x}, T(\mathbf{y}) \rangle \\ &= \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle - 2 \langle \mathbf{x}, T(\mathbf{y}) \rangle \end{aligned}$$

e

$$\begin{aligned} d^2\left(\mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y})\right) &= \|\mathbf{x} - S_{\mathbf{r}_i}(\mathbf{y})\|^2 \\ &= \langle \mathbf{x}, \mathbf{x} \rangle + \langle S_{\mathbf{r}_i}(\mathbf{y}), S_{\mathbf{r}_i}(\mathbf{y}) \rangle - 2 \langle \mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y}) \rangle \\ &= \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle - 2 \langle \mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y}) \rangle . \end{aligned}$$

Logo,

$$\begin{aligned} d^2(\mathbf{x}, \mathbf{y}) - d^2\left(\mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y})\right) &= 2 \langle \mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y}) \rangle - 2 \langle \mathbf{x}, \mathbf{y} \rangle \\ &= 2 \langle \mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y}) - \mathbf{y} \rangle . \end{aligned}$$

Como

$$S_{\mathbf{r}_i}(\mathbf{y}) - \mathbf{y} = -2\frac{\langle \mathbf{y}, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle}\mathbf{r}_i.$$

temos que $S_{\mathbf{r}_i}(\mathbf{y}) = \mathbf{y}$ se $\langle \mathbf{y}, \mathbf{r}_i \rangle = 0$, acabou. Se $\langle \mathbf{y}, \mathbf{r}_i \rangle \neq 0$, então $\mathbf{y}$ não pertence ao hiperplano $\langle \mathbf{r}_i \rangle^\perp$. Sendo $\mathbf{t} \in F_\Pi$, obtemos que

$$T(\mathbf{t}) \in T(F_\Pi).$$

Assim, $T(\mathbf{t})$ e $\mathbf{y}$ estão no mesmo lado do hiperplano $\langle \mathbf{r}_i \rangle^{\perp}$, pois $(T(\overline{F}_{\Pi}))^0 \cap \langle \mathbf{r}_i \rangle^{\perp} = \emptyset$ e $T(\overline{F}_{\Pi})$ é um conjunto convexo. Logo,

$$\langle \mathbf{y}, \mathbf{r}_i \rangle \ \text{ e } \ \langle T(\mathbf{t}), \mathbf{r}_i \rangle = \left\langle T^{-1}(\mathbf{r}_i), \mathbf{t} \right\rangle$$

têm o mesmo sinal. Como

$$n\left(S_{\mathbf{r}_i} T\right) = n\left(T\right) - 1$$

temos, pelo Teorema 2.3, que $S_{\mathbf{r}_i}^{-1}(\mathbf{r}_i) \in \Delta_{\mathbf{t}}^{-}$. Assim, $S_{\mathbf{r}_i}(\mathbf{y}) - \mathbf{y} = a\mathbf{r}_i$, $a \in \mathbb{R}_{+}^{*}$. Portanto,

$$d^2(\mathbf{x}, \mathbf{y}) - d^2\left(\mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y})\right) = 2a \left\langle \mathbf{x}, \mathbf{r}_i \right\rangle .$$

Finalmente, como $\langle \mathbf{x}, \mathbf{r}_i \rangle \geq 0$ temos que $S_{\mathbf{r}_i}(\mathbf{x}) = \mathbf{x}$ se $\langle \mathbf{x}, \mathbf{r}_i \rangle = 0$ ou

$$d\left(\mathbf{x}, \mathbf{y}\right) > d\left(\mathbf{x}, S_{\mathbf{r}_i}(\mathbf{y})\right).$$

se $\langle \mathbf{x}, \mathbf{r}_i \rangle > 0$. ■

Exemplo 3.2 *Pelo Exemplo* 3.1*, obtemos que*

$$\mathbf{x}_0 = \mathbf{r}_3 = (\frac{\sqrt{3}}{2}, \frac{1}{2}) \in \overline{F}_{\Pi},$$

pois basta tomar

$$x_1 = x_2 = \frac{1}{2}.$$

Escolhendo $T = S_{\mathbf{r}_2} S_{\mathbf{r}_1} S_{\mathbf{r}_2} \in G$*, obtemos* $\mathbf{y} = -\mathbf{x}_0 \in V_{\Delta}$ *tal que* $\mathbf{y} \in T(\overline{F}_{\Pi})$*, pois*

$$\begin{aligned} T(\mathbf{x}_0) &= S_{\mathbf{r}_2} S_{\mathbf{r}_1} S_{\mathbf{r}_2}(\mathbf{x}_0) \\ &= S_{\mathbf{r}_2} S_{\mathbf{r}_1}(\mathbf{r}_1) \\ &= S_{\mathbf{r}_2}(-\mathbf{r}_1) = -\mathbf{x}_0. \end{aligned}$$

Como

$$2 = l\left(S_{\mathbf{r}_i} T\right) = l\left(T\right) - 1$$

temos, pelo Lema 3.2*, que*

$$d\left(\mathbf{x}_0, \mathbf{y}\right) > d\left(\mathbf{x}_0, S_{\mathbf{r}_i}(\mathbf{y})\right),$$

pois $S_{\mathbf{r}_i}(\mathbf{x}_0) \neq \mathbf{x}_0$ *e* $S_{\mathbf{r}_i}(\mathbf{y}) \neq \mathbf{y}$*,* $i = 1, 2$*. Portanto,* $\mathbf{y}$ *é o ponto com a maior distância de* $\mathbf{x}_0$

Seja

$$C = \{T(\mathbf{x}_0) : T \in G\} = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{M-1}\}$$

um código de grupo. Pela item 3. da definição de região fundamental podemos assumir, sem perda de generalidade, que o ponto inicial $\mathbf{x}_0 \in \overline{F}_\Pi$. Assim,

$$\mathbf{x}_0 = \sum_{i=1}^{n} x_i \mathbf{s}_i, x_i \in \mathbb{R}_+, \tag{3.4}$$

ou, equivalentemente, resolver as n equações

$$\langle \mathbf{x}_0, \mathbf{r}_i \rangle = \begin{cases} 0 & \text{se } \mathbf{r}_i \in \Pi_P \\ x_i & \text{se } \mathbf{r}_i \in \Pi - \Pi_p \end{cases}.$$

Pelo Teorema 3.1, para determinar a distância mínima do código C, é suficiente determinar a distância de uma vizinhança do vetor inicial $\mathbf{x}_0$. A prova do próximo teorema demonstra que a vizinhamça mais próxima é obtida pela aplicação de uma reflexão simples no ponto inicial $\mathbf{x}_0$. Assim, a distância mínima é obtida aplicando reflexões simples no ponto inicial $\mathbf{x}_0 \in \overline{F}_\Pi$ e escolhendo o mais próximo dos pontos resultantes, digamos $S_{\mathbf{r}_j}(\mathbf{x}_0)$. Logo,

$$\begin{aligned} d^2(\mathbf{x}_0, S_{\mathbf{r}_j}(\mathbf{x}_0)) &= d^2(\mathbf{x}_0, \mathbf{x}_0 - 2\frac{\langle \mathbf{x}_0, \mathbf{r}_i \rangle}{\langle \mathbf{r}_i, \mathbf{r}_i \rangle}\mathbf{r}_i) \\ &= 4\frac{\langle \mathbf{x}_0, \mathbf{r}_j \rangle^2}{\|\mathbf{r}_j\|^2}, \end{aligned}$$

ou ainda,

$$d(\mathbf{x}_0, S_{\mathbf{r}_j}(\mathbf{x}_0)) = \frac{2x_j}{\|\mathbf{r}_j\|}. \tag{3.5}$$

Teorema 3.3 *Sejam*

$$\Pi = \{\mathbf{r}_1, \ldots, \mathbf{r}_n\}$$

a $\mathbf{t}$*-base para* G *e*

$$\mathbf{x}_0 = \sum_{i=1}^{n} x_i \mathbf{s}_i \in \overline{F}_\Pi$$

Então a distância mínima do código $C = O(\mathbf{x}_0)$ *é dada por*

$$d_{\min}(C) = \min\left\{ \frac{2x_i}{\|\mathbf{r}_i\|} : x_i > 0, 1 \leq i \leq n \right\}$$

Demonstração. Seja $T \in G$ tal que

$$d_{\min}(C) = d(\mathbf{x}_0, T(\mathbf{x}_0)).$$

Podemos assumir que T foi escolhido, de modo que

$$l(T) = \min\{l(S) : S \in G\}.$$

É claro que $T \neq I$, assim, existe $\mathbf{r}_i \in \Pi$ tal que

$$l(S_{\mathbf{r}_i}T) = l(T) - 1 < l(T).$$

Assim, pela minimalidade de $l(T)$, obtemos que $S_{\mathbf{r}_i}(\mathbf{x}_0) \neq \mathbf{x}_0$ e $S_{\mathbf{r}_i}(T(\mathbf{x}_0)) \neq T(\mathbf{x}_0)$ e, assim, pelo Lema 3.2,

$$d(\mathbf{x}_0, S_{\mathbf{r}_i}(T(\mathbf{x}_0))) < d(\mathbf{x}_0, T(\mathbf{x}_0)) = d_{\min}(C).$$

Logo, $\mathbf{x}_0 = S_{\mathbf{r}_i}T(\mathbf{x}_0)$ e $T = S_{\mathbf{r}_i}$. Portanto, pela Equação (3.5), obtemos que

$$d_{\min}(C) = \min\left\{\frac{2x_i}{\|\mathbf{r}_i\|} : x_i > 0, 1 \leq i \leq n\right\}$$

■

Observação 3.2 *A solução para o problema do vetor inicial ótimo agora é imediata, pois $H_{\mathbf{r}_i}$ é o bissector perpendicular do segmento de reta*

$$[\mathbf{x}_0, S_{\mathbf{r}_i}(\mathbf{x}_0)],$$

isto é,

$$d(\mathbf{x}_0, \mathbf{y}) = d(S_{r_i}(\mathbf{x}_0), \mathbf{y}),$$

onde $\mathbf{y} \in H_{r_i}$.

Corolário 3.2 *Sejam Π a $\mathbf{t}$-base para G e*

$$H = \langle S_{\mathbf{r}} \in G : \mathbf{r} \in \Pi_P \rangle.$$

Então o vetor inicial ótimo $\mathbf{x}_0$ do código de grupo $C = O(\mathbf{x}_0)$, com $G_{\mathbf{x}_0} = H$ e distância mínima $d = d_{\min}(C)$ é dado por

$$\mathbf{x}_0 = \sum_{\mathbf{r}_i \in \Pi - \Pi_P} \frac{d\|\mathbf{r}_i\|}{2}\mathbf{s}_i.$$

Demonstração. Como

$$d = d(\mathbf{x}_0, S_{\mathbf{r}_i}(\mathbf{x}_0)) = \frac{2x_i}{\|\mathbf{r}_i\|} \text{ e } \mathbf{x}_0 = \sum_{i=1}^{n} x_i\mathbf{s}_i$$

temos que

$$\mathbf{x}_0 = \sum_{\mathbf{r}_i \in \Pi - \Pi_P} \frac{d\|\mathbf{r}_i\|}{2}\mathbf{s}_i.$$

■

Observação 3.3 *A fórmula da distância mínima quadrática para um vetor inicial* $\mathbf{x}_0$*, com* $\|\mathbf{x}_0\| = 1$*, é dada por*

$$d^2_{\min}(C) = \frac{4}{\sum\limits_{r_i \in \Pi - \Pi_P} \sum\limits_{r_j \in \Pi - \Pi_P} (\|\mathbf{r}_i\| \, \|\mathbf{r}_j\|) \langle \mathbf{s}_i, \mathbf{s}_j \rangle}.$$

Teorema 3.4 *Sejam* Π *uma* $\mathbf{t}$*-base fixada para* G *e* $\mathbf{x}_0 \in \overline{F}_\Pi$ *o vetor inicial do código de grupo*

$$C = \{S(\mathbf{x}_0) : S \in G\}.$$

Então a região de decisão para $\mathbf{x}_0$ *é dada por*

$$V(\mathbf{x}_0) = \bigcup_{T \in G_{\mathbf{x}_0}} T(\overline{F}_\Pi)$$

onde

$$T(\overline{F}_\Pi) = \{\mathbf{y} \in V_\Delta : \langle T(\mathbf{y}), \mathbf{r} \rangle \geq 0, \forall \mathbf{r} \in \Pi\}.$$

Demonstração. Vamos provar primeiro que

$$\overline{F}_\Pi \subseteq V(\mathbf{x}_0).$$

Dado $\mathbf{y} \in F_\Pi$ e suponhamos, por absurdo, que $\mathbf{y} \in V(\mathbf{x}_1)$, com $\mathbf{x}_1 \in C$ e $\mathbf{x}_1 \neq \mathbf{x}_0$. Escolhendo $S \in G$ tal que

$$l(S) = \min \{l(R) : R \in G\} \text{ e } \mathbf{x}_1 = S(\mathbf{x}_0).$$

É claro que $T \neq I$, assim, existe $\mathbf{r}_i \in \Pi$ tal que

$$l(S_{\mathbf{r}_i} S) = l(S) - 1 < l(S).$$

Logo, pela minimalidade de S, obtemos que $S_{\mathbf{r}_i}(\mathbf{y}) \neq \mathbf{y}$ e $S_{\mathbf{r}_i}(\mathbf{x}_1) \neq \mathbf{x}_1$ e, assim, pelo Lema 3.2,

$$d(\mathbf{x}_1, S_{\mathbf{r}_i}(\mathbf{y})) < d(\mathbf{x}_1, \mathbf{y}),$$

o que é uma contradição. Como $V(\mathbf{x}_0)$ é um conjunto fechado temos que $\overline{F}_\Pi \subseteq V(\mathbf{x}_0)$.

Se $\mathbf{y} \in V(\mathbf{x})$, então $T(\mathbf{y}) \in V(T(\mathbf{x}))$, para todo $T \in G$. Em particular, $T(\overline{F}_\Pi) \subseteq V(\mathbf{x}_0)$, para todo $T \in G_{\mathbf{x}_0}$.

Para provar a inclusão inversa é suficiente mostrar que: dado $\mathbf{y} \in V(\mathbf{x}_0)^0$ temos que $\mathbf{y} \in T(\overline{F}_\Pi)$, pois $T(\overline{F}_\Pi)$ é fechado. Seja $T \in G$ tal que $\mathbf{y} \in T(\overline{F}_\Pi)$. Note, pelas observações

acima, que podemos trocar $\mathbf{y}$ por algum vetor $S(\mathbf{y})$, desde que $S \in G_{\mathbf{x}_0}$. Isto significa que podemos escolher T tal que

$$l(S) = \min\{l(R) : R \in G\}$$

e, além disso, para todo $\mathbf{r}_i \in \Pi_P$,

$$l\left(S_{\mathbf{r}_i} T\right) > l\left(T\right)$$

seja satisfeita.

Afirmação: $T = I$.

De fato, se $T \neq I$, então existe uma reflexão simples $S_{\mathbf{r}_i}$ tal que

$$l\left(S_{\mathbf{r}_i} T\right) = l\left(T\right) - 1.$$

Logo, $\mathbf{r}_i \notin \Pi_P$ e $S_{\mathbf{r}_i}(\mathbf{x}_0) \neq \mathbf{x}_0$ e, assim, pelo Lema 3.2, obtemos que

$$d\left(\mathbf{y}, S_{\mathbf{r}_i}(\mathbf{x}_0)\right) = d\left(S_{\mathbf{r}_i}(\mathbf{x}_0), \mathbf{x}_0\right) \leq d\left(\mathbf{y}, \mathbf{x}_0\right),$$

o que é uma contradição, pois $\mathbf{y} \in V(\mathbf{x}_0)^0$. ■

Observação 3.4 *O Teorema* 3.4 *mostra que as regiões de decodificações são unicamente determinadas pelo estabilizador $G_{\mathbf{x}_0}$. Esta propriedade assegura que existe uma única solução para o problema do vetor inicial, quando o estabilizador é fixado. Em particular, quando $G_{\mathbf{x}_0} = \{I\}$, o Teorema* 3.4 *implica que a região fundamental F de um grupo de reflexão finito é única, a menos de isometria.*

Exemplo 3.3 *Seja G o grupo das reflexões do retângulo (não quadrado) em $\mathbb{R}^2$ com as raízes simples*

$$\mathbf{r}_1 = (1, 0) \ \ e \ \ \mathbf{r}_2 = (0, 1),$$

isto é,

$$\begin{aligned} G &= \langle S_{\mathbf{r}_1}, S_{\mathbf{r}_2} \rangle \\ &= \{I, S_{\mathbf{r}_1}, S_{\mathbf{r}_2}, S_{\mathbf{r}_1} S_{\mathbf{r}_2}\}, \end{aligned}$$

onde $S_{\mathbf{r}_1}$ e $S_{\mathbf{r}_2}$ são reflexões de $H_{\mathbf{r}_1}$ e $H_{\mathbf{r}_2}$ determinadas pelas raízes $\mathbf{r}_1$ e $\mathbf{r}_2$. Logo,

$$\Delta = \{\pm\mathbf{r}_1, \pm\mathbf{r}_2\}$$

é um sistema de raízes de G. *Escolhendo* $\mathbf{t} = (1,1) \in \mathbb{R}^2$, *obtemos que*

$$\Pi = \{\mathbf{r}_1, \mathbf{r}_2\}$$

é uma $\mathbf{t}$*-base para* G. *Neste caso,*

$$\overline{F}_\Pi = \{(x_1, x_2) \in V_\Delta : x_1 \geq 0 \ \ e \ \ x_2 \geq 0\},$$

pois Π *é uma base autodual, e pela Equação* (3.4) *e normalizando, obtemos que*

$$\mathbf{x}_0 = \frac{1}{\sqrt{2}}(1,1) \in \overline{F}_\Pi,$$

também, pelo item 2. *da definição de região fundamental, o estabilizador de todo* $\mathbf{x} \in \overline{F}_\Pi$, *é* $G_\mathbf{x} = \{I\}$. *O código de grupo de comprimento* 2

$$C = O(\mathbf{x}_0) = \{\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(-1,1), \frac{1}{\sqrt{2}}(-1,-1), \frac{1}{\sqrt{2}}(1,-1)\}$$

com distância mínima (*cf. Observação* 3.3)

$$\begin{aligned} d^2_{\min}(C) &= \frac{4}{\|\mathbf{r}_1\|^2 \|\mathbf{s}_1\|^2 + \|\mathbf{r}_2\|^2 \|\mathbf{s}_2\|^2} \\ &= \frac{4}{2} \\ &= 2 \end{aligned}$$

e taxa normalizada

$$R = \frac{1}{2}\log_2 4 = 1$$

bits por dimensão. Além disso, a região de decisão é dada por

$$\begin{aligned} V(\mathbf{x}_0) &= \bigcup_{T \in G_{\mathbf{x}_0}} T(\overline{F}_\Pi) \\ &= \overline{F}_\Pi. \end{aligned}$$

Note que, G *é isomorfo a* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exemplo 3.4 *Seja* $\mathcal{A}_2$ *dado no Exemplo* 2.5 *com*

$$\Pi = \{\mathbf{r}_1, \mathbf{r}_2\}$$

uma $\mathbf{t}$*-base para* G *e base dual*

$$\mathbf{s}_1 = (-\frac{2}{3}, \frac{1}{3}, \frac{1}{3}) \ \ e \ \ \mathbf{s}_2 = (-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3}).$$

Neste caso,

$$\begin{aligned} V_\Delta &= \left\{\mathbf{x} \in \mathbb{R}^3 : \langle \mathbf{x}, (1,1,1)\rangle = 0\right\} \\ &= \langle \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3\rangle. \end{aligned}$$

Assim,

$$\begin{aligned} \overline{F}_\Pi &= \left\{\mathbf{x} \in V_\Delta : \mathbf{x} = \sum_{i=1}^{2} x_i \mathbf{s}_i \ \ e \ \ x_i \in \mathbb{R}_+\right\} \\ &= \left\{\left(\frac{-2x_1 - x_2}{3}, \frac{x_1 - x_2}{3}, \frac{x_1 + 2x_2}{3}\right) : x_1 \geq 0 \ \ e \ \ x_2 \geq 0\right\}. \end{aligned}$$

Pela Equação (3.4) *e normalizando, obtemos que*

$$\mathbf{x}_0 = \frac{1}{\sqrt{6}}(-2,1,1) \in \overline{F}_\Pi$$

e $G_{\mathbf{x}_0} = \{I, S_{\mathbf{r}_2}\}$*, pois*

$$\begin{aligned} S_{\mathbf{r}_2}(\mathbf{x}_0) &= \mathbf{x}_0 - 2\frac{\langle \mathbf{x}_0, \mathbf{r}_2\rangle}{\langle \mathbf{r}_2, \mathbf{r}_2\rangle}\mathbf{r}_2 \\ &= \mathbf{x}_0. \end{aligned}$$

O código de grupo de comprimento 3

$$C = O(\mathbf{x}_0) = \{\frac{1}{\sqrt{6}}(-2,1,1), \frac{1}{\sqrt{6}}(1,-2,1), \frac{1}{\sqrt{6}}(1,1,-2)\}$$

com mínima distância (*cf. Observação* 3.3)

$$\begin{aligned} d^2_{\min}(C) &= \frac{4}{\|\mathbf{r}_1\|^2 \|\mathbf{s}_1\|^2} \\ &= \frac{4}{\frac{2}{3} \cdot 2} \\ &= 3 \end{aligned}$$

e taxa normalizada

$$R = \frac{1}{3}\log_2 3$$

bits por dimensão. Além disso, a região de decisão é dada por

$$\begin{aligned} V(\mathbf{x}_0) &= \bigcup_{T \in G_{\mathbf{x}_0}} T(\overline{F}_\Pi) \\ &= \overline{F}_\Pi \cup S_{\mathbf{r}_2}(\overline{F}_\Pi), \end{aligned}$$

onde

$$S_{\mathbf{r}_2}(\overline{F}_\Pi) = \left\{\left(\frac{-2x_1 - x_2}{3}, \frac{x_1 + 2x_2}{3}, \frac{x_1 - x_2}{3}\right) : x_1 \geq 0 \ \ e \ \ x_2 \geq 0\right\}.$$

Observação 3.5 *O leitor interessado em algoritmos de decodificações para os códigos de grupos gerados por grupos de Coxeter irredutíveis pode consultar* [*12, 14*].

Referências Bibliográficas

[1] Blake, I. F. and Mullin, R. C., *The Mathematical Theory of Coding*. Academic Press. New York. 1975.

[2] Bourbaki, N., Éléments de Mathèmatique, Groupes et Algébres de Lie. Paris, Hermann, ch 4-5, 1968,

[3] Cameron, P. J., "Finite permutation groups and finite simple groups." *Bull. London Math. Soc.* 13, pp. 1-22, 1981.

[4] Dixon, J. D. and Mortimer, B.C., *Permutation groups*. Springer-Verlag, New Yor, 1996.

[5] Gantmacher, F. R., *The Theory of Matrices*, Vol. 1, New Jersey, Prentice-Hall, 1991.

[6] Garcia, A. e Y. Lequain, I. *Álgebra*:: *Um curso de introdução*. Projeto Euclides - IMPA. Rio Janeiro, 1988.

[7] Grove, L. C. and Benson, C. T., *Finite Reflection Groups*. New York: Springer-Verlag, 1985.

[8] Gonçalves, A. *Tópicos em representação de grupos.* 9º Colóquio Brasileiro de Matemática. Poços de Caldas. 1973.

[9] Humphreys, J. E. *Reflection Groups and Coxeter Groups*. Cambridge Univ. Press, 1990.

[10] Lima, E. L, *Espaços Métricos*. Projeto Euclides - IMPA. Rio Janeiro, 1977.

[11] Lourêdo, A. T., *Códigos de Permutação para o Canal Gaussiano*, João Pessoa, 2000. 102 f. Dissertação (Mestrado em Matemática) - CCEN - UFPB.

[12] Mittelholzer, T. and Lahtonen, J. "Group Codes Generated by Finite Reflection Groups," *IEEE Trans. Inform. Theory*, vol. 42, 519-528, 1996.

[13] Passman, D.S., *Permutation Gruops*. New York, Benjamin, 1968.

[14] Slepian, D., "Permutation Modulation," *Proc. IEEE Trans. Inform. Theory*, vol. 53, 228-236, 1965.