UNIVERSIDADE ESTADUAL DE MARINGÁ

CENTRO DE CIÊNCIAS EXATAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

(Mestrado)

LUCAS MAURÍCIO RUAN

Girogrupo de Möbius em álgebras de Clifford

Maringá-PR

2014

LUCAS MAURÍCIO RUAN

Girogrupo de Möbius em álgebras de Clifford

Dissertação apresentada ao programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra.

Orientador: Prof. Dr. Osvaldo Germano do Rocio.

Co-Orientador: Prof. Dr. Eduardo Brandani da Silva.

Maringá-PR

2014

GIROGRUPO DE MÖBIUS EM ÁLGEBRAS DE CLIFFORD

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como partes dos requisitos necessários para a obtenção do título de Mestre em Matemática pela Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Osvaldo Germano do Rocio(Orientador) - UEM

(Presidente)

Eduardo Brandani da Silva(Co-orientador) - UEM

Antonio Aparecido de Andrade - Unesp

Érica Zancanella Fornaroli - UEM

Aprovada em: 26 Março de 2014.

Local de defesa: Auditório do Departamento de Matemática, Bloco F67, campus da Universidade Estadual de Maringá.

Dedicatória

À Deus e a minha família.

Agradecimentos

À Deus pela minha vida.

Ao meu orientador Osvaldo Germano do Rocio pela sua paciência, dedicação, sugestões para a elaboração desta dissertação e por acreditar em mim.

Ao meu co-orientador Eduardo Brandani da Silva pelos bons conselhos, dicas e por conseguir as referências para o desenvolvimento desta dissertação de que tanto precisei.

Aos meus professores da graduação e do mestrado, pelos conhecimentos repassados.

A minha esposa Ana Claudia, pela compreensão, amizade, carinho e amor dedicado a mim nesses dois anos de trabalho.

A minha família pelo enorme apoio nesta etapa da minha vida e desde quando iniciei a graduação.

Aos amigos do truco e do colégio: Paulinho, Bigão, Godoy, Machado, B2, Rambão e Ice.

Aos amigos do mestrado: Altair, João Pitot, Ronaldo, Teló, Tatiane e Rafael.

À Universidade Estadual de Maringá, Departamento de Matemática e a CAPES, pelo apoio financeiro.

Muito Obrigado!

Resumo

No presente trabalho exibiremos relações que ligam as álgebras de Clifford associadas ao espaço vetorial $\mathbb{R}^n$, munido de produto interno negativo, matrizes de Vahlen e transformações de Möbius em um espaço paravetorial estendido $\widehat{W} = (\mathbb{R} \oplus \mathbb{R}^n) \cup \{\infty\}$ com o laço de Möbius ou girogrupo de Möbius. Com isso descreveremos, de forma compacta, uma fórmula para a operação do girogrupo de Möbius $a \oplus b = (a+b)(1+\overline{a}b)^{-1}$, onde o lado direito é dado em termos dos elementos da álgebra de Clifford, generalizando o girogrupo de Möbius do disco unitário complexo.

Palavras-chave: Álgebras de Clifford, matriz de Vahlen, transformação de Möbius, B-laços, grupos involutivos e girogrupos.

Abstract

In this paper we display links between the Clifford algebras associated with vector space $\mathbb{R}^n$, provided with negative inner product matrices Vahlen and Möbius transformations in an extended paravector space $\widehat{W} = (\mathbb{R} \oplus \mathbb{R}^n) \cup \{\infty\}$ with Möbius loop or Möbius gyrogroup. With that describe, in a compact form, a formula for operating Möbius gyrogroup $a \oplus b = (a + b)(1 + \overline{a}b)^{-1}$, where the right side is given in terms of the elements of the Clifford algebra, generalizing the Möbius gyrogroup unit complex disc.

Keywords: Clifford algebra, Vahlen matrices, Möbius transformations, B-loop, involutive group and gyrogroup.

Sumário

Introdução

A adição de Möbius no disco unitário complexo $\mathbb{D} = \{z \in \mathbb{C} \mid |z| < 1\}$ definida por

$$u \oplus v = \frac{u+v}{1+\overline{u}v} \tag{1}$$

fornece a $\mathbb{D}$ uma estrutura de um B-laço, ou seja, um girogrupo girocomutativo com a propriedade da raiz quadrada única.

O fato de que $(\mathbb{D}, \oplus)$ é um girogrupo girocomutativo é abordado por Abraham A. Ungar, em **[19]**, através das transformações de Möbius que preservam $\mathbb{D}$ da forma

$$z \mapsto e^{i\theta}\frac{a+z}{1+\overline{a}z},$$

onde $a, z \in \mathbb{D}$, $\theta \in \mathbb{R}$ fixo e $\overline{a}$ é o conjugado de a.

Tal fato, induz uma operação binária $\oplus$ em $\mathbb{D}$, definida por

$$a \oplus z := \frac{a+z}{1+\overline{a}z},$$

a qual é não-comutativa e não-associativa. No entanto, essas situações podem ser *reparadas* com a introdução da aplicação $gyr : \mathbb{D} \times \mathbb{D} \to Aut(\mathbb{D}, \oplus)$ definida por

$$gyr[a, z] = \frac{a \oplus z}{z \oplus a} = \frac{1+a\overline{z}}{1+\overline{a}z},$$

onde $Aut(\mathbb{D}, \oplus)$ o grupo dos automorfismos de $(\mathbb{D}, \oplus)$, sendo que $gyr[a, b]$ geometricamente age como uma rotação em torno da origem do disco $\mathbb{D}$. Dessa forma, sendo $a, b, c \in \mathbb{D}$, conseguimos as relações:

$$a \oplus b = gyr[a, b](b \oplus a) \quad (\textit{girocomutatividade})$$

$$a \oplus (b \oplus c) = (a \oplus b) \oplus gyr[a,b](c) \quad (giroassociatividade).$$

Após, Ungar reescreve a adição de Möbius dada por (1), da seguinte forma

$$u \oplus v = \frac{(1 + 2\langle u, v\rangle + \|v\|^2)u + (1 - \|u\|^2)v}{1 + 2\langle u, v\rangle + \|u\|^2|v|^2}. \tag{2}$$

Essa nova relação mostra que, a adição de Möbius pode ser vista como uma equação vetorial restrita ao disco unitário do espaço vetorial $\mathbb{R}^2$. Tal fato, motivou Ungar a generalizar a adição de Möbius para o disco unitário de um $\mathbb{R}$-espaço vetorial V, munido de produto interno e norma derivada do produto interno, por definir a adição de Möbius conforme dado em (2). Essa abordagem é citada, mas o autor não apresenta uma prova de tal fato.

Para uma abordagem clássica das transformações de Möbius em várias dimensões nos referimos a [**1**], [**5**] e [**22**]. Sendo V um espaço vetorial sobre $\mathbb{R}$ de dimensão finita, Alhfors, em [**1**], observa que uma abordagem natural das transformações de Möbius em várias dimensões é através dos números de Clifford que são elementos do subespaço vetorial $\mathbb{R} \oplus V$ da álgebra de Clifford $\mathcal{C}\ell_{0,n} = \mathcal{C}_n$. Após esse trabalho, as álgebras de Clifford se tornaram uma ferramenta comum para o estudo das transformações de Möbius, conforme pode ser visto em [**22**]. Em [**5**], Ferreira faz o que é afirmado por Ungar, ou seja, um estudo do girogrupo de Möbius do espaço paravetorial $\mathbb{R} \oplus V$, cujos elementos são os números de Clifford de $\mathcal{C}\ell_{0,n}$, mostrando algebricamente que munindo o disco unitário do espaço paravetorial com a adição de Möbius dada em (1), obtém-se uma generalização do girogrupo de Möbius na álgebra de Clifford $\mathcal{C}_n$.

Com o mesmo foco algébrico, Jimmie Lawson, em [**12**], aborda o girogrupo de Möbius de uma maneira diferente, através da união de assuntos variados, tais como: álgebras de Clifford reais em um espaço vetorial com produto interno negativo, matrizes de Vahlen, transformações de Möbius e teoria dos laços, em especial os K-laços. Essa abordagem é diferente da de Ungar e Ferreira, pois Lawson primeiramente exibe uma fórmula simples para a operação binária do laço de Möbius, ou seja, do disco unitário do espaço paravetorial $W = \mathbb{R} \oplus \mathbb{R}^n$, o qual é um K-laço, definida por

$$v \oplus u = (v + u)(1 + \overline{u}v)^{-1}, \tag{3}$$

onde $v, u \in \{w \in \mathbb{R} \oplus V \; |\|w\| < 1\}$.

Em seguida, Lawson observa que os conceitos de K-laços e girogrupos girocomutativos são equivalentes, mostrando dessa forma que a operação dada em (3) vale para o girogrupo de Möbius $B_n = \{w \in \mathbb{R} \oplus V \mid \|w\| < 1\} \subset \mathcal{C}_n$. Com isso, podemos concluir que a adição de Möbius do girogrupo de Möbius B_n funciona de maneira análoga para o caso *trivial* do girogrupo de Möbius $\mathbb{D} = B_1$, conforme dado em (1).

Os girogrupos, os quais generalizam o conceito de grupo, aparecem em 1988, sendo o primeiro girogrupo o girogrupo de Einstein, cuja a operação binária é não-comutativa e não-associativa. Outro exemplo de um girogrupo é o girogrupo de Möbius, o qual é um modelo concreto da teoria abstrata de girogrupos, sendo que seu estudo direciona a uma melhor compreensão das transformações de Lorentz da teoria da relatividade especial, uma vez que o grupo de Lorentz atua no disco de todas as possíveis velocidades simétricas via aplicações conformes. Ainda, possuem mais uma aplicação na fisíca para os modelos descritos por equações invariantes sob transformações conformes. A girolinguagem é devidoa a Ungar.

Nessa dissertação, exploramos detalhadamente o trabalho realizado por Lawson, o qual dá uma visão algébrica para o girogrupo de Möbius B_n, através do formalismo das álgebras de Clifford $\mathcal{C}_n$. A partir de um espaço vetorial $V = \mathbb{R}^n$, munido de produto interno e norma, determinamos a álgebra de Clifford associada e construímos o espaço paravetorial $\mathbb{R} \oplus V$ que é o espaço vetorial das somas diretas de escalar com vetor. Este espaço paravetorial será o ambiente para o estudo do girogrupo de Möbius no disco unitário. Uma vez que cada número de Clifford não-nulo tem um inverso podemos definir transformações de Möbius no espaço paravetorial $\mathbb{R} \oplus V$. Nossos resultados em espaços paravetoriais permanecem válidos aos espaços vetoriais por restrição.

O primeiro capítulo fornece as notações, terminologias e resultados preliminares essenciais para o desenvolvimento dos demais capítulos, onde abordamos um exemplo de álgebra quociente que dará significado a primeira definição do capítulo seguinte.

No segundo capítulo, exploramos alguns tópicos gerais das álgebras de Clifford, do ponto de vista algébrico, tais como: a sua construção, automorfismo principal e anti-automorfismo principal e centro da álgebra de Clifford. Após, focaremos nas álgebras de Clifford reais. Apresentamos o espaço paravetorial da álgebra de Clifford e definiremos o grupo de Clifford do espaço paravetorial, o qual será descrito de duas formas, em que uma dessas formas aparece a aplicação adjunta torcida.

No terceiro capítulo, definimos duas aplicações sobre o espaço paravetorial que caracterizam as transformações de Möbius. Veremos também as matrizes de Vahlen, as quais induzem transformações de Möbius. Por fim veremos as translações de Möbius, que são transformações de Möbius que preservam o disco unitário do espaço paravetorial.

O quarto capítulo apresenta, de forma direta, alguns tópicos de teoria dos laços. Um fato notável, é a relação obtida entre as álgebras de Clifford, transformações de Möbius e matrizes de Vahlen com a teoria de laços, permitindo falar no laço de Möbius.

O último capítulo trata dos girogrupos, onde veremos dois resultados importantes, sendo que o primeiro é a equivalência entre girogrupos comutativos com a propriedade da raiz quadrada única e os B-laços, e o outro resultado é a generalização do caso do girogrupo do disco unitário complexo, ou seja, do girogrupo de Möbius.

Capítulo 1

Preliminares

Neste primeiro capítulo abordaremos alguns conceitos da álgebra em geral, os quais servirão de suporte para o desenvolvimento deste trabalho. O capítulo está dividido em quatro partes: na primeira, apresentaremos algumas definições e resultados básicos de álgebra, ilustrando com exemplos algumas dessas definições e alguns desses resultados; na segunda, apresentamos brevemente a álgebra quociente; já na terceira, abordaremos a álgebra tensorial $T(V)$ de um espaço vetorial V; por fim, na última parte, veremos que, ao tomarmos um ideal específico de $T(V)$, obtemos algumas propriedades da álgebra quociente $T(V)/I$.

1.1 Noções de Álgebra e Álgebra linear

Com o objetivo de fixar notações e conceitos que serão utilizados em capítulos posteriores, apresentaremos algumas definições e resultados da álgebra e álgebra linear e daremos alguns exemplos desses fatos.

Definição 1.1.1. Um espaço vetorial A sobre um corpo $\mathbb{F}$ é uma $\mathbb{F}$-*álgebra* (ou uma *álgebra sobre* $\mathbb{F}$) se existir uma operação binária $\cdot$ em A, que satisfaz:

i) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *e* $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, $\forall a, b, c \in A$.

ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in A$.

iii) *Existe um elemento* $u \in A$ *tal que* $u \cdot a = a \cdot u = a$, $\forall a \in A$. *Tal elemento é único, será denotado por* 1_A *e denominado elemento identidade.*

iv) $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$, $\forall \lambda \in \mathbb{F}$, $\forall a, b \in A$.

Observação 1.1.2. *Para evitar trivialidades, assumimos que* $1_A \neq 0_A$, *onde* 0_A *é o elemento neutro do espaço vetorial* A.

A *dimensão* de uma $\mathbb{F}$-álgebra A, denotada por $\dim_{\mathbb{F}} A$, é a dimensão do $\mathbb{F}$-espaço vetorial A.

Um *homomorfismo* entre $\mathbb{F}$-álgebras $(A, \cdot)$ e $(A', \odot)$ é uma aplicação $f : A \to A'$ que satisfaz:

i) f é uma transformação $\mathbb{F}$-linear(ou simplesmente, transformação linear).

ii) $f(1_A) = 1_{A'}$.

iii) $f(a \cdot b) = f(a) \odot f(b)$, $\forall a, b \in A$.

Mais ainda, dizemos que a aplicação $f : A \to A'$ é um:

iv) *isomorfismo* se f for bijetora e um homomorfismo.

v) *automorfismo* se f for um isomorfismo e $A = A'$.

vi) *anti-automorfismo* se f for bijetora e satisfazer *i)*, *ii)* e $f(a \cdot b) = f(b) \odot f(a)$, $\forall a, b \in A$.

Observação 1.1.3. *Para toda* $\mathbb{F}$*-álgebra* A, *existe um isomorfismo natural* $\mathbb{F} \cong \mathbb{F}1_A$.

Exemplo 1.1.4. *Vejamos algumas álgebras:*

i) *Todo corpo* $\mathbb{F}$ *é uma* $\mathbb{F}$*-álgebra unidimensional. O conjunto dos números complexos* $\mathbb{C}$ *e o conjunto dos números quatérnios reais* $\mathbb{H} = \{a + bi + cj + dk \mid i^2 = j^2 = k^2 = -1 \text{ e } a, b, c, d \in \mathbb{R}\}$ *são* $\mathbb{R}$*-álgebras, com* $\dim_{\mathbb{R}} \mathbb{C} = 2$ *e* $\dim_{\mathbb{R}} \mathbb{H} = 4$.

ii) *Sejam X um conjunto não-vazio e A uma $\mathbb{F}$-álgebra. O $\mathbb{F}$-espaço vetorial de todas as aplicações de X em A, denotado por A^X, munido da operação $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in X$ e $\forall f, g \in A^X$, é uma $\mathbb{F}$-álgebra.*

iii) *Seja $\mathbb{M}(n, \mathbb{F})$ o $\mathbb{F}$-espaço vetorial de todas as matrizes de ordem $n \times n$ com entradas em $\mathbb{F}$, munido da operação multiplicação usual de matrizes. Com estas operações $\mathbb{M}(n, \mathbb{F})$ é uma $\mathbb{F}$-álgebra, com dimensão n^2.*

iv) *O $\mathbb{F}$-espaço vetorial $\mathbb{F}[X]$ dos polinômios a uma indeterminada sobre $\mathbb{F}$, munido da multiplicação usual de polinômios, é uma $\mathbb{F}$-álgebra, de dimensão não-finita.*

v) *O $\mathbb{R}$-espaço vetorial $\mathbb{R}^2$ com a operação produto $(a, b) \cdot (c, d) = (ac + bd, ad + bc)$, é uma $\mathbb{R}$-álgebra de dimensão 2.*

Observação 1.1.5. *Note que $0_A \cdot a = a \cdot 0_A = 0_A$, $\forall a \in A$, para qualquer $\mathbb{F}$-álgebra A.*

Definição 1.1.6. Seja A uma $\mathbb{F}$-álgebra. Um subconjunto não-vazio $S \subset A$ é uma *subálgebra* de A se S é um subespaço vetorial de A que contém 1_A e para quaisquer $a, b \in S$, implicar que $a \cdot b \in S$.

Observação 1.1.7. *Seja A uma $\mathbb{F}$-álgebra e seja J um conjunto de índices. Se S_i é uma subálgebra de A, para todo $i \in J$, então $\bigcap_{i \in J} S_i$ é uma subálgebra de A.*

Definição 1.1.8. Seja A uma $\mathbb{F}$-álgebra e seja $X \subset A$ um subconjunto não-vazio. A *subálgebra de A gerada por X*, denotada por $\langle X \rangle$, é a interseção de todas as subálgebras de A que contêm X.

Observação 1.1.9. *Se A é uma $\mathbb{F}$-álgebra e $X \subset A$ é um subconjunto não-vazio, então $\langle X \rangle$ é o conjunto de todas as somas finitas da forma $\lambda_0 1_A + \sum_I \lambda_I x_I$, onde $I = (i_1, \ldots, i_k)$, $k \leq 1$, $x_I = x_{i_1} \cdot \ldots \cdot x_{i_k}$ com $x_{i_1}, \ldots, x_{i_k} \in X$ e $\lambda_0, \lambda_I \in \mathbb{F}$.*

Definição 1.1.10. Uma *forma bilinear simétrica* sobre um $\mathbb{F}$-espaço vetorial V é uma aplicação $B : V \times V \to \mathbb{F}$ tal que, para cada $v, u, w \in V$ e todo $\lambda \in \mathbb{F}$ satisfaz:

i) $B(v + \lambda w, u) = B(v, u) + \lambda B(w, u)$ e $B(v, u + \lambda w) = B(v, u) + \lambda B(v, w)$.

ii) $B(v, u) = B(u, v)$.

Dizemos que dois vetores $v, u \in V$ são *ortogonais* em relação à B, quando $B(v, u) = 0$.

Definição 1.1.11. Seja V um $\mathbb{F}$-espaço vetorial munido de uma forma bilinear simétrica. Dizemos que B é *não-degenerada* se para todo $v \in V, v \neq 0_V$, existe $u \in V, u \neq 0_V$ tal que $B(v, u) \neq 0$.

Um corpo $\mathbb{F}$ tem *característica diferente de dois* se $2 \neq 0$, onde $2 = 1 + 1 \in \mathbb{F}$. Neste trabalho, iremos sempre considerar $\mathbb{F}$ um corpo com essa propriedade.

Definição 1.1.12. Uma *forma quadrática* sobre um $\mathbb{F}$-espaço vetorial V é uma aplicação $Q : V \to \mathbb{F}$ tal que:

i) $Q(\lambda v) = \lambda^2 Q(v)$, $\forall \lambda \in \mathbb{F}$, $\forall v \in V$.

ii) A aplicação $B_Q : V \times V \to \mathbb{F}$ definida por $B_Q(v, u) := \frac{1}{2}[Q(v + u) - Q(v) - Q(u)]$ é uma forma bilinear simétrica sobre V.

Observação 1.1.13. *Existe uma forma bilinear simétrica $B : V \times V \to \mathbb{F}$ se, e somente se, existe uma forma quadrática $Q : V \to \mathbb{F}$. De fato: se $v \in V$, então $Q(v) := B(v, v)$ é uma forma quadrática (chamada forma quadrática associada à B). A recíproca é imediata.*

Proposição 1.1.14. *Seja V um $\mathbb{F}$-espaço vetorial de dimensão finita, munido de uma forma bilinear simétrica B. Então existe uma base $\mathfrak{B}$ de V tal que $B(e, e') = 0$, $\forall e, e' \in \mathfrak{B}$, com $e \neq e'$, isto é, existe uma base ortogonal em relação à B.*

Demonstração: Ver **[9]**, pg. 316. ■

De acordo com a proposição 1.1.14, existe uma base de V tal que a matriz da forma bilinear B é diagonal. Com a hipótese de B ser não-degenerada, veremos que a matriz da forma bilinear B é invertível em qualquer base de V. Esse é o enunciado da seguinte:

Proposição 1.1.15. *Seja V um $\mathbb{F}$-espaço vetorial de dimensão finita n, munido de uma forma bilinear simétrica B. Se $\mathfrak{B}_V$ é uma base ortogonal em relação à B de V e B é não-degenerada, então:*

i) *$Q(e_i) \neq 0$, para todo $e_i \in \mathfrak{B}_V$, $1 \leq i \leq n$.*

ii) *A matriz $[B]_{\mathfrak{B}}$ é invertível, para toda base $\mathfrak{B}$ de V.*

Demonstração:

i) Da proposição 1.1.14, existe uma base $\mathfrak{B}_V$ ortogonal em relação à B. Como B é não-degenerada, temos que, dado $e_i \in \mathfrak{B}_V$, com $1 \leq i \leq n$, existe $v = \sum_{j=1}^{n} x_j e_j \in V$, $v \neq 0_V$, tal que $B(v, e_i) \neq 0$. Assim, $B(v, e_i) = x_i B(e_i, e_i) \neq 0 \Rightarrow x_i \neq 0$ e $B(e_i, e_i) \neq 0$. Logo, $Q(e_i) = B(e_i, e_i) \neq 0$.

ii) Seja $[B]_{\mathfrak{B}_V}$ a matriz de B em relação à base $\mathfrak{B}_V$. Pelo item i) e por ser $[B]_{\mathfrak{B}_V}$ uma matriz diagonal, temos que $\det[B]_{\mathfrak{B}_V} = Q(e_1) \ldots Q(e_n) \neq 0$. Logo, a matriz de B em relação a base $\mathfrak{B}_V$ é invertível.

Considere uma base $\mathfrak{B}$ de V. Dados $v, u \in V$, sabemos que a matriz mudança de base de $\mathfrak{B}$ para $\mathfrak{B}_V$, denotada por $[I]^{\mathfrak{B}}_{\mathfrak{B}_V}$, é uma matriz invertível e satisfaz $[v]_{\mathfrak{B}_V} = [I]^{\mathfrak{B}}_{\mathfrak{B}_V}[v]_{\mathfrak{B}}$. Assim, obtemos as relações:

$$B(v, u) = [v]^t_{\mathfrak{B}}[B]_{\mathfrak{B}}[u]_{\mathfrak{B}} \ \mathbf{(1)}$$

$$B(v, u) = [v]^t_{\mathfrak{B}_V}[B]_{\mathfrak{B}_V}[u]_{\mathfrak{B}_V} = [v]^t_{\mathfrak{B}}([I]^{\mathfrak{B}}_{\mathfrak{B}_V})^t[B]_{\mathfrak{B}_V}[I]^{\mathfrak{B}}_{\mathfrak{B}_V}[u]_{\mathfrak{B}} \ \mathbf{(2)}$$

Logo, (1) e (2) implicam que $[B]_{\mathfrak{B}} = ([I]^{\mathfrak{B}}_{\mathfrak{B}_V})^t [B]_{\mathfrak{B}_V} [I]^{\mathfrak{B}}_{\mathfrak{B}_V}$, mostrando que $[B]_{\mathfrak{B}}$ é invertível se, e somente se, $[B]_{\mathfrak{B}_V}$ é invertível. ■

Vejamos alguns exemplos.

Exemplo 1.1.16. *Seja V um $\mathbb{F}$-espaço vetorial com base $\{e_i\}_{i=1}^n$.*

i) Considere $V = \mathbb{R}^n$ e $p, q \in \mathbb{N}$ tais que $p + q = n$. Dados $v = \sum_{i=1}^{n} x_i e_i, u = \sum_{i=1}^{n} y_i e_i$, $x_i, y_i \in \mathbb{R}$, a aplicação $Q_{p,q}(v) = x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_{p+q}^2$ é uma forma quadrática, cuja forma bilinear simétrica associada é $B_{p,q}(v, u) = \sum_{i=1}^{p} x_i y_i - \sum_{i=p+1}^{n} x_i y_i$. E mais, $B_{p,q}$ é não-degenerada.

ii) No item i), tomando $p = n$ e $q = 0$, obtemos que $B_{n,0}$ é o produto interno usual de $\mathbb{R}^n$, o qual é uma forma bilinear simétrica e não-degenerada.

iii) Ainda em i), tomando $p = 0$ e $q = n$, obtemos que $B_{0,n}$ é a aplicação produto interno usual negativo, denotada e dada por $-\langle v, u\rangle = -x_1 y_1 - \ldots - x_n y_n$, a qual é uma forma bilinear simétrica e não-degenerada.

iv) Seja $V = \mathbb{C}^n$. A aplicação $B : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ dada por $B((z_1, \ldots, z_n), (w_1, \ldots, w_n)) = z_1 w_1 + \ldots + z_1 w_n$, $\forall z_i, w_i \in \mathbb{C}$, $1 \leq i \leq n$ é uma forma bilinear, simétrica e não-degenerada.

1.2 Álgebra quociente

Seja A um conjunto não-vazio e seja R uma relação de equivalência sobre A. Denotamos $(a, b) \in R$ por aRb. Dado $a \in A$, o conjunto $[a]_R = \{x \in A \mid xRa\}$ é chamado de *classe de equivalência* de $a \in A$. O conjunto de todas as classes de equivalência de A pela relação de equivalência R, denotado por $A/R = \{[a]_R \mid a \in A\}$, é chamado de *conjunto quociente*.

Dada uma $\mathbb{F}$-álgebra A, um subconjunto não-vazio $I \subset A$ é um *ideal* de A se para quaisquer $x, y \in I$ e todo $a \in A$, implicar que $x - y \in I$ e $a \cdot x,\ x \cdot a \in I$. Assim, se R é a relação sobre $A \times A$ definida por $aRb \Leftrightarrow a - b \in I$, então R é uma relação de equivalência. Sendo $\lambda \in \mathbb{F}$ e $a, b \in A$, e munindo o conjunto quociente A/R das operações $[a]_R + [b]_R = [a+b]_R$, $\lambda[a]_R = [\lambda a]_R$ e $[a]_R \cdot [b]_R = [a \cdot b]_R$, as quais são bem definidas, temos que A/R é uma $\mathbb{F}$-álgebra. O elemento neutro e a identidade de A/R são, nesta ordem, $[0_A]_R$ e $[1_A]_R$.

A $\mathbb{F}$-álgebra acima é denominada *álgebra quociente* de A por I (ou de A módulo I), a qual denotamos por A/I e seus elementos por $a + I$, com $a \in A$. Neste caso, a projeção canônica $\pi : A \to A/I$ é um homomorfismo.

1.3 Álgebra Tensorial

Nesta seção veremos algumas noções de álgebra tensorial, as quais serão necessárias para o desenvolvimento deste trabalho.

Dados $\mathbb{F}$-espaços vetoriais V, U e W, uma *aplicação bilinear* de $V \times U$ em W é uma aplicação $B : V \times U \to W$ que satisfaz $B(v, u + \lambda u') = B(v, u) + \lambda B(v, u')$ e $B(v + \lambda' v', u) = B(v, u) + \lambda' B(v', u)$, $\forall v, v' \in V$, $\forall u, u' \in U$ e $\forall \lambda, \lambda' \in \mathbb{F}$.

Definição 1.3.1. Sejam V, U espaços vetoriais sobre $\mathbb{F}$. Um *produto tensorial* de V por U é um par $(V \otimes_{\mathbb{F}} U, \otimes)$ que satisfaz as seguintes condições:

i) $V \otimes_{\mathbb{F}} U$ é um $\mathbb{F}$-espaço vetorial e $\otimes : V \times U \to V \otimes_{\mathbb{F}} U$ é uma aplicação bilinear de $V \times U$ em $V \otimes_{\mathbb{F}} U$.

ii) Se $\{e_i \mid i \in I\}$ é uma base para V e $\{f_j \mid j \in J\}$ é uma base para U, então $\{e_i \otimes f_j \mid i \in I, j \in J\}$ é uma base para $V \otimes_{\mathbb{F}} U$.

Uma prova de que o produto tensorial é único, a menos de isomorfismo, é dada em [**13**]. Para não carregar a notação, denotaremos $V \otimes_{\mathbb{F}} U$ simplesmente por $V \otimes U$.

Proposição 1.3.2. *Sejam V, U e W $\mathbb{F}$-espaços vetoriais. São isomorfos como espaços vetoriais:*

i) $\mathbb{F} \otimes V \cong V$.

ii) $V \otimes U \cong U \otimes V$.

iii) $(V \otimes U) \otimes W \cong V \otimes (U \otimes W)$.

iv) $(V \oplus U) \otimes W \cong (V \otimes W) \oplus (U \otimes W)$.

Demonstração: Ver [**13**], pg. 62. ■

Observação 1.3.3. *De acordo com a proposição* 1.3.2*, não há ambiguidade nos seguintes produtos tensoriais:* $(V \otimes V) \otimes V \cong V \otimes (V \otimes V) \cong V \otimes V \otimes V$.

Definição 1.3.4. Seja $\{V_i \mid i \in \mathbb{N}\}$ uma família de $\mathbb{F}$-espaços vetoriais. A *soma direta (externa)* dos espaços vetoriais V_i, denotada por $\bigoplus_{i \in \mathbb{N}} V_i$, é o espaço vetorial formado por todas as sequências $(v_i)_{i \in \mathbb{N}}$, $v_i \in V_i$, para os quais existe um $i_0 \in \mathbb{N}$ tal que $v_i = 0_{V_i}$ para todo $i > i_0$, com as operações $(v_i)_{i \in \mathbb{N}} + (u_i)_{i \in \mathbb{N}} = (v_i + u_i)_{i \in \mathbb{N}}$ e $\lambda(v_i)_{i \in \mathbb{N}} = (\lambda v_i)_{i \in \mathbb{N}}$, $\forall \lambda \in \mathbb{F}$, $\forall v_i, u_i \in V_i$.

Denotamos o elemento neutro de cada V_i, simplesmente por 0.

Para cada $i \in \mathbb{N}$, a aplicação $\iota_i : V_i \to \bigoplus_{i \in \mathbb{N}} V_i$ definida por $\iota_i(v_i) = (v_j)_{j \in \mathbb{N}}$, onde

$$v_j = \begin{cases} 0 & , \text{se } j \neq i \\ v_i & , \text{se } j = i \end{cases}$$

é uma transformação linear e injetora, a qual é denominada de *inclusão*.

Seja V um $\mathbb{F}$-espaço vetorial e definamos $V^{\otimes 0} := \mathbb{F}$, $V^{\otimes 1} := V$ e $V^{\otimes i} := V^{\otimes(i-1)} \otimes V^{\otimes 1}$, para cada natural $i \geq 2$. Denotemos por $T(V)$ o espaço vetorial $\bigoplus_{i\in\mathbb{N}} V^{\otimes i}$. Podemos tornar o espaço vetorial $T(V)$ uma álgebra.

Dados $a, b \in T(V)$, existem $k, \ell \in \mathbb{N}$ tais que $a = (v_0, v_1, \ldots, v_k, 0, \ldots)$ e $b = (u_0, u_1, \ldots, u_\ell, 0 \ldots)$, onde $v_i \in V^{\otimes i}$, $u_j \in V^{\otimes j}$.

Defina uma aplicação $\otimes : T(V) \times T(V) \to T(V)$ por

$$a \otimes b := (v_0u_0, v_0u_1 + v_1u_0, v_0u_2 + v_1u_1 + v_2u_0, \ldots, v_ku_\ell, 0, \ldots)$$

onde $v_i \in V^{\otimes i}$, $u_j \in V^{\otimes j}$ e $v_iu_j \in V^{\otimes(i+j)}$ é tal que

$$v_iu_j = \begin{cases} v_0u_0, \text{ se } i = j = 0 \\ v_0u_j, \text{ se } i = 0 \ e \ j \neq 0 \\ u_0v_i, \text{ se } i \neq 0, \ e \ j = 0 \\ v_i \otimes u_j, \text{ se } i \neq 0 \ e \ j \neq 0 \end{cases}.$$

Para todos $a, b, c \in T(V)$ e $\lambda \in \mathbb{F}$, valem as seguintes propriedades que tornam $T(V)$ uma $\mathbb{F}$-álgebra:

i) $a \otimes (b + c) = (a \otimes b) + (a \otimes c)$ e $(a + b) \otimes c = (a \otimes c) + (b \otimes c)$.

ii) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

iii) Existe $1_T \in T(V)$ tal que $1_T \otimes a = a \otimes 1_T = a$, a saber $1_T = (1, 0, 0, \ldots)$.

iv) $\lambda(a \otimes b) = (\lambda a) \otimes b = a \otimes (\lambda b)$.

Definição 1.3.5. Chamamos a $\mathbb{F}$-álgebra $T(V)$ de *álgebra tensorial* sobre V.

Fixado um ideal $I \subset T(V)$, de acordo com a segunda seção, para todo $\lambda \in \mathbb{F}$ e quaisquer $a, b \in T(V)$ temos as seguintes operações na álgebra quociente $T(V)/I$:

$$(a + I) + (b + I) = (a + b) + I, \ \lambda(a + I) = (\lambda a) + I \ e \ (a + I) \cdot (b + I) = (a \otimes b) + I,$$

em que $0_{T/I} = 0_T + I$ é o elemento neutro e $1_{T/I} = 1_T + I$ é a identidade de $T(V)/I$.

Exemplo 1.3.6. *Se* $\dim_{\mathbb{R}} V = 1$, *então* $T(V) \cong \mathbb{R}[X]$. *Basta definir a transformação linear por* $(1, 0, \ldots) \mapsto 1_{\mathbb{R}[X]}$ *e* $(0, e, 0, \ldots) \mapsto X$.

Exemplo 1.3.7. *Seja* $\mathbb{R}\langle X, Y\rangle$ *a* $\mathbb{R}$*-álgebra dos polinômios nas indeterminadas não-comutativas* X *e* Y. *Se* $\dim_{\mathbb{R}} V = 2$, *então* $T(V) \cong \mathbb{R}\langle X, Y\rangle$. *De fato: basta definir uma transformação linear por* $(1, 0, \ldots) \mapsto 1_{\mathbb{R}\langle X,Y\rangle}$, $(0, e_1, 0, \ldots) \mapsto X$ *e* $(0, e_2, 0, \ldots) \mapsto Y$.

1.4 A álgebra quociente $\frac{T(V)}{I_B}$

Nesta seção veremos que ao considerar um ideal particular da álgebra tensorial de V, obtemos algumas propriedades interessantes a respeito da álgebra quociente.

Teorema 1.4.1. *Seja* V *um* $\mathbb{F}$*-espaço vetorial, munido de uma forma bilinear simétrica e não-degenerada* B. *Se* $I_B \subset T(V)$ *é o ideal formado pelos elementos da forma* $\sum_{i=1}^{k} a_i \otimes (v_1 \otimes u_1 + u_1 \otimes v_1 - 2B(v, u)1_T) \otimes b_i$, *sendo* $a_i, b_i, v_1 = (0, v, 0, \ldots), u_1 = (0, u, 0, \ldots) \in T(V)$, $v, u \in V$, $k \in \mathbb{N}^*$ *e* 1_T *a identidade de* $T(V)$, *então existe uma transformação linear* $\gamma : V \to T(V)/I_B$ *satisfazendo as seguintes condições:*

i) $\mathbb{F}1_{T/I_B}$ *e* $\gamma(V)$ *são subespaços vetoriais distintos em* $T(V)/I_B$, *onde* $1_{T/I_B}$ *é a identidade de* $T(V)/I_B$.

ii) $\gamma(v) \cdot \gamma(u) + \gamma(u) \cdot \gamma(v) = 2B(v, u)1_{T/I_B}$, $\forall v, u \in V$.

iii) A álgebra $T(V)/I_B$ *é gerada por* $\gamma(V)$.

iv) Se $(A, \centerdot)$ *é uma* $\mathbb{F}$*-álgebra e* $f : V \to A$ *é uma transformação linear tal que* $f(v) \centerdot f(u) + f(u) \centerdot f(v) = 2B(v, u)1_A$, *então existe um único homomorfismo* $\widetilde{f} : T(V)/I_B \to A$ *tal que* $\widetilde{f} \circ \gamma = f$.

Demonstração: Defina a aplicação $\gamma := \pi \circ \iota : V \to T(V)/I_B$, onde $\iota : V \to T(V)$ é a inclusão e $\pi : T(V) \to T(V)/I_B$ é a projeção canônica. Temos que $\gamma(v) = \pi(\iota(v)) = \pi(v_1) = v_1 + I_B$, onde $v \in V$ e $v_1 = (0, v, 0, \ldots) \in T(V)$.

i) Segue da observação 1.1.3 e do fato de γ ser uma transformação linear, pois essa é a composição de transformações lineares, que $\mathbb{F}1_{T/I_B}$ e $\gamma(V)$ são subespaços vetoriais de $T(V)/I_B$. Ainda, todo elemento de $\mathbb{F}1_{T/I_B}$ é da forma $(\lambda, 0, 0, \ldots) + I_B$, já em $\gamma(V)$, todo elemento é da forma $(0, v, 0, \ldots) + I_B$, mostrando que $\mathbb{F}1_{T/I_B} \neq \gamma(V)$.

ii) Se $v_1, u_1 \in T(V)$, então $(v_1 + I_B) \cdot (u_1 + I_B) = (v_1 \otimes u_1) + I_B$. Note que:

$$v_1 \otimes u_1 = \frac{1}{2}(v_1 \otimes u_1 - u_1 \otimes v_1 + 2B(v,u)1_T) + \underbrace{\frac{1}{2}(v_1 \otimes u_1 + u_1 \otimes v_1 - 2B(v,u)1_T)}_{\in I_B}$$

Logo, vale que $(v_1 + I_B) \cdot (u_1 + I_B) = \frac{1}{2}(v_1 \otimes u_1 - u_1 \otimes v_1 + 2B(v,u)1_T) + I_B$.

Na igualdade acima, trocando v_1 por u_1 e somando os resultados, obtemos a relação: $(v_1 + I_B) \cdot (u_1 + I_B) + (u_1 + I_B) \cdot (v_1 + I_B) = 2B(v,u)1_T + I_B$. Como $\gamma(v) = v_1 + I_B$ e $1_T + I_B = 1_{T/I_B}$, segue que

$$\gamma(v) \cdot \gamma(u) + \gamma(u) \cdot \gamma(v) = 2B(v,u)1_{T/I_B}.$$

iii) Dado $a \in T(V)/I_B$, existe $k \in \mathbb{N}$ tal que $a = (a_0, a_1, \ldots, a_k, 0, \ldots) + I_B$, onde $a_i \in V^{\otimes i}$, $0 \leq i \leq k$. Temos que $a = ((a_0, 0, \ldots) + I_B) + ((0, a_1, 0, \ldots) + I_B) + \ldots + ((\ldots, 0, a_k, 0 \ldots) + I_B)$ tal que $(\ldots, 0, a_i, 0 \ldots) \in V^{\otimes i}$.

Para cada $a_i \in V^{\otimes i}$, existe $x_{j_1,\ldots,j_i} \in \mathbb{F}$, $j_1, \ldots, j_i \in J$, para algum conjunto de índices J, tais que $a_i = \sum x_{j_1\ldots j_i} e_{j_1} \otimes \ldots \otimes e_{j_i}$, onde $e_{j_1}, \ldots, e_{j_i}$ são elementos de alguma base de V. Logo, temos que

$$(\ldots, 0, a_i, 0 \ldots) + I_B = \sum x_{j_1\ldots j_i} \underbrace{((0, e_{j_1}, 0, \ldots) + I_B)}_{\in \gamma(V)} \cdot \ldots \cdot \underbrace{((0, e_{j_i}, 0, \ldots) + I_B)}_{\in \gamma(V)}$$

e, portanto, $a = \sum_{i=0}^{k}(\ldots,0,a_i,0,\ldots) + I_B \in \langle\gamma(V)\rangle$. Portanto, $T(V)/I_B \subset \langle\gamma(V)\rangle$ e sendo a inclusão contrária óbvia, segue que $T(V)$ é a $\mathbb{F}$-álgebra gerada por $\gamma(V)$.

iv) Seja $(A, \centerdot)$ uma $\mathbb{F}$-álgebra e seja $f : V \to A$ uma transformação linear tal que $f(v) \centerdot f(u) + f(u) \centerdot f(v) = 2B(v,u)1_A$, $\forall v,u \in V$, sendo 1_A a identidade de A. Para cada $i \in \mathbb{N}$, definamos as aplicações $f_i : V^{\otimes i} \to A$ dadas por $f_0(\lambda) = \lambda 1_A$, $f_1(v) = f(v)$, $f_i(v_1 \otimes \ldots \otimes v_i) = f(v_1) \centerdot \ldots \centerdot f(v_i)$, $\forall \lambda \in \mathbb{F}$, $\forall v, v_1, \ldots, v_i \in V$. É fácil ver que tais aplicações são transformações lineares.

Agora, sendo $a = (a_0, a_1, \ldots, a_k, 0, \ldots) \in T(V)$, onde $k \in \mathbb{N}$, definimos a seguinte aplicação $\phi : T(V) \to A$ por

$$\phi(a) = f_0(a_0) + f_1(a_1) + \ldots + f_k(a_k).$$

Vamos mostrar que ϕ é um homomorfismo de álgebras. Note que, ϕ é uma transformação linear, pois é uma soma de transformações lineares. Pela definição, $\phi(1_T) = 1_A$, restando mostrar que se $a, b \in T(V)$, então $\phi(a \otimes b) = \phi(a) \centerdot \phi(b)$. De fato, observe que se $(\ldots, 0, v_1 \otimes \ldots \otimes v_i, 0, \ldots), (\ldots, 0, u_1 \otimes \ldots \otimes u_j, 0, \ldots) \in T(V)$, onde $v_1, \ldots, v_i, u_1, \ldots, u_j \in V$ e $i, j \in \mathbb{N}$, então $f_{i+j}((v_1 \otimes \ldots \otimes v_i)(u_1 \otimes \ldots u_j)) = f(v_1) \centerdot \ldots f(v_i) \centerdot f(u_1) \centerdot \ldots \centerdot f(u_j) = f_i(v_1 \otimes \ldots \otimes v_i) \centerdot f_j(u_1 \otimes \ldots, \otimes u_j)$.

Em seguida, tomemos $a = (a_0, a_1, \ldots, a_k, 0, \ldots), b = (b_0, b_1, \ldots, b_m, 0, \ldots) \in T(V)$.

Temos que:

$$\begin{aligned}
\phi(a\otimes b) &= \phi(a_0b_0, a_0b_1+a_1b_0, \ldots, a_0b_i+\ldots+a_ib_0, \ldots, a_kb_m, 0, \ldots)\\
&= f_0(a_0b_0)+f_1(a_0b_1+a_1b_0)+\ldots\\
&\quad +f_i(a_0b_i+\ldots+a_ib_0)+\ldots+f_{k+m}(a_kb_m)\\
&= f_0(a_0)\centerdot f_0(b_0)+f_{0+1}(a_0b_1)+f_{1+0}(a_1b_0)+\ldots\\
&\quad f_{0+i}(a_0b_i)+\ldots+f_{j+(i-j)}(a_jb_{i-j})+\ldots+f_{i+0}(a_ib_0)\\
&\quad +\ldots+f_k(a_k)\centerdot f_m(b_m)\\
&= f_0(a_0)\centerdot(b_0)+f_0(a_0)\centerdot f_1(b_1)+f_1(a_1)\centerdot f_0(b_0)+\ldots\\
&\quad f_0(a_0)\centerdot f_i(b_i)+\ldots+f_j(a_j)\centerdot f_{i-j}(b_{i-j})+\ldots+f_i(a_i)\centerdot f_0(b_0)\\
&\quad +\ldots+f_k(a_k)\centerdot f_m(b_m)\\
&= (f_0(a_0)+f_1(a_1)+\ldots+f_k(a_k))\centerdot(f_0(b_0)+f_1(b_1)+\ldots f_m(b_m))\\
&= \phi(a)\centerdot\phi(b).
\end{aligned}$$

Note que $\ker\phi := \{v\in T(V) \mid \phi(v)=0_A\}\subset T(V)$ é um ideal.

E mais, sendo $v_1=(0,v,0,\ldots,), u_1=(0,u,0,\ldots)\in T(V)$, com $v,u\in V$, temos que $\phi(v_1\otimes u_1+u_1\otimes v_1-2B(v,u)1_T)=\underbrace{f_1(v)\centerdot f_1(u)+f_1(u)\centerdot f_1(v)}_{=f(v)\centerdot f(u)+f(u)\centerdot f(v)=2B(v,u)1_A}-2B(v,u)1_A=0_A$, logo, $I_B\subset\ker\phi$. Logo, podemos definir a aplicação $\widetilde{f}: T(V)/I_B\to A$ por $\widetilde{f}(a+I_B)=\phi(a)$, $a\in T(V)$, a qual se trata de um homomorfismo. De fato: $\widetilde{f}$ está bem definida pois se $a+I_B, b+I_B\in T(V)/I_B$ são tais que $a+I_B=b+I_B$, então $a-b\in I_B$. Assim, $\phi(a-b)=\phi(a)-\phi(b)=0$, ou seja, $\phi(a)=\phi(b)$. Logo, $\widetilde{f}(a+I_B)=\widetilde{f}(b+I_B)$.

Se $a + I_B, b + I_B \in T(V)/I_B$ e $\lambda \in \mathbb{F}$, então

$$\begin{aligned}
\widetilde{f}((a+I_B)\cdot(b+I_B)) &= \widetilde{f}((a\otimes b)+I_B)\\
&= \phi(a\otimes b) = \phi(a)\,\boldsymbol{.}\,\phi(b)\\
&= \widetilde{f}(a+I_B)\,\boldsymbol{.}\,\widetilde{f}(b+I_B),
\end{aligned}$$

$$\begin{aligned}
\widetilde{f}((a+I_B)+\lambda(b+I_B)) &= \widetilde{f}((a+\lambda b)+I_B)\\
&= \phi(a+\lambda b) = \phi(a)+\lambda\phi(b)\\
&= \widetilde{f}(a+I_B)+\lambda\widetilde{f}(b+I_B),
\end{aligned}$$

$$\widetilde{f}(1_{T/I_B}) = \widetilde{f}(1_T + I_B) = \phi(1_T) = 1_A.$$

Agora, se $v \in V$, $(\widetilde{f}\circ\gamma)(v) = \widetilde{f}(\gamma(v)) = \widetilde{f}((0,v,0,\ldots)+I_B) = \phi(0,v,0,\ldots) = f(v)$.

Resta provar a unicidade de $\widetilde{f}$. Seja $\widetilde{g} : T(V)/I_B \to A$ um homomorfismo tal que $\widetilde{g}\circ\gamma = f$. Dado $v \in V$, temos que $(\widetilde{g}\circ\gamma)(v) = \widetilde{g}(\gamma(v)) = f(v) = \widetilde{f}(\gamma(v))$. Pelo item iii), segue que $\widetilde{g} = \widetilde{f}$.

■

Exemplo 1.4.2. *De acordo com o item iii) de* 1.1.16*, se* $B = B_{0,1}$*, então* $T(V)/I_{B_{0,1}} \cong \mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}$.

Capítulo 2

Álgebras de Clifford

Neste capítulo, introduziremos os elementos essenciais das álgebras de Clifford para a compreensão do restante do trabalho. As álgebras de Clifford foram introduzidas pelo matemático-filósofo William Kingdon Clifford em 1876, as quais generalizam o conceito de números complexos e quatérnios, possuindo aplicações na geometria e na física. Para o desenvolvimento deste texto, focaremos apenas em algumas (das muitas) propriedades da álgebra de Clifford.

2.1 Introdução às álgebras de Clifford

Nesta seção, veremos que dado um espaço vetorial V munido de uma forma bilinear simétrica e não-degenerada $B : V \times V \to \mathbb{F}$ é possível associar, por meio de uma transformação linear, uma álgebra, chamada álgebra de Clifford. Apresentaremos três aplicações, sendo uma um automorfismo e as outras duas anti-automorfismos, onde uma dessas aplicações decompõe toda álgebra de Clifford como soma direta de sua parte par com a parte ímpar. Após, assumindo que a dimensão de V é finita, poderemos descrever uma base da álgebra de Clifford, que nesse caso será finita. Encerramos a seção, vendo que o centro da álgebra de Clifford depende da dimensão de V e ilustramos toda a seção com alguns exemplos.

Definição 2.1.1. Seja $\mathbb{F}$ um corpo de característica diferente de dois e seja V um $\mathbb{F}$-

espaço vetorial, munido de uma forma bilinear simétrica e não-degenerada B. Uma *álgebra de Clifford universal* associada à (V, B), denotada por $\mathcal{C}\ell(V, B)$, é um par $(\mathcal{C}\ell(V, B), \mu)$ tal que $\mathcal{C}\ell(V, B)$ é uma $\mathbb{F}$-álgebra e $\mu : V \to \mathcal{C}\ell(V, B)$ é uma transformação linear, satisfazendo as seguintes propriedades:

i) $\mathbb{F}\mathbf{1}$ e $\mu(V)$ são subespaços vetoriais distintos em $\mathcal{C}\ell(V, B)$, onde $\mathbf{1}$ é a identidade da álgebra $\mathcal{C}\ell(V, B)$.

ii) $\mu(v) \cdot \mu(u) + \mu(u) \cdot \mu(v) = 2B(v, u)\mathbf{1}$, $\forall v, u \in V$. Chamamos essa identidade de *condição de Clifford*.

iii) $\mathcal{C}\ell(V, B)$ é a $\mathbb{F}$-álgebra gerada por $\mu(V)$.

iv) Dada uma $\mathbb{F}$-álgebra $(A, \odot)$ e uma transformação $\mathbb{F}$-linear $\phi : V \to A$ tal que $\phi(v) \odot \phi(u) + \phi(u) \odot \phi(v) = 2B(v, u)1_A$, $\forall v, u \in V$, existe um único homomorfismo entre as álgebras $\mathcal{C}\ell(V, B)$ e A que estende μ, ou seja, existe um único homomorfismo $\widetilde{\phi} : \mathcal{C}\ell(V, B) \to A$ tal que $\widetilde{\phi} \circ \mu = \phi$.

Chamamos *iv)* de *propriedade universal* e a aplicação ϕ de *aplicação de Clifford*. Caso ocorram apenas as condições i), ii) e iii), chamamos o par $(\mathcal{C}\ell(V, B), \mu)$ de álgebra de Clifford. Em particular, a aplicação μ também é uma aplicação de Clifford.

No que segue, B denota uma forma bilinear simétrica e não-degenerada sobre o $\mathbb{F}$-espaço vetorial V, Q a forma quadrática associada à B, $\mathfrak{B}_V$ é uma base ortogonal de V em relação à B, e $\mathbf{0}$ e $\mathbf{1}$ denotam os elementos neutro e identidade de $\mathcal{C}\ell(V, B)$, respectivamente.

Observação 2.1.2. *Do teorema* 1.4.1 *e da definição* 2.1.1*, segue que a álgebra quociente $T(V)/I_B$ é uma álgebra de Clifford universal de (V, B), onde I_B é o ideal gerado pelos elementos da forma $v_1 \otimes u_1 + u_1 \otimes v_1 - 2B(v, u)1_T$ sendo $v_1 = (0, v, 0, \ldots), u_1 = (0, u, 0, \ldots) \in T(V)$ e 1_T é a identidade de $T(V)$. Logo, a definição* 2.1.1 *faz sentido.*

Podemos ilustrar a propriedade universal com o seguinte diagrama:

$$\begin{tikzcd} V \arrow[r, "\mu"] \arrow[dr, "\phi"'] & C\ell(V,B) \arrow[d, "\tilde{\phi}"] \\ & A \end{tikzcd}$$

Observação 2.1.3. *Do item iii) da definição* 2.1.1 *temos que, para todo* $a \in \mathcal{C}\ell(V,B)$, *existem* $\lambda_0, \lambda_{i_1 \ldots i_k} \in \mathbb{F}$ *e* $\mu(v_1), \ldots, \mu(v_k) \in \mathcal{C}\ell(V,B)$ *tais que* $a = \lambda_0 \mathbf{1} + \sum \lambda_{i_1 \ldots i_k} \mu(v_1) \cdot \ldots \cdot \mu(v_k)$, *onde* $k \in \mathbb{N}^*$ *e* $i_1, \ldots, i_k \in I$, *para algum conjunto de índices* I.

Observação 2.1.4. *A álgebra de Clifford universal associada à* (V,B) *é única, a menos de isomorfismo. De fato: se* A *e* A' *são álgebras de Clifford universais associadas à* (V,B), *com aplicações de Clifford* $\mu : V \to A$ *e* $\phi : V \to A'$, *respectivamente, então da propriedade universal, existem únicos homomorfismos* $\widetilde{\mu} : A' \to A$ *e* $\widetilde{\phi} : A \to A'$ *tais que* $\widetilde{\mu} \circ \phi = \mu$ *e* $\widetilde{\phi} \circ \mu = \phi$. *Por substituição, segue que:* $\widetilde{\mu} \circ (\widetilde{\phi} \circ \mu) = \mu$ *e* $\widetilde{\phi} \circ (\widetilde{\mu} \circ \phi) = \phi$, *implicando que* $\widetilde{\mu} \circ \widetilde{\phi} = \mathrm{id}_A$ *e* $\widetilde{\phi} \circ \widetilde{\mu} = \mathrm{id}_{A'}$, *uma vez que* A *e* A' *são geradas como* $\mathbb{F}$*-álgebras por* $\mu(V)$ *e* $\phi(V)$, *rescpectivamente. Logo,* $\widetilde{\mu}$ *é invertível, garantindo que* $\widetilde{\mu} : A' \to A$ *é um isomorfismo satisfazendo* $\widetilde{\mu} \circ \phi = \mu$. *O diagrama abaixo ilustra o que foi dito.*

$$\begin{tikzcd} V \arrow[r, "\mu"] \arrow[dr, "\phi"'] & A \arrow[d, shift right, "\tilde{\phi}"'] \\ & A' \arrow[u, shift right, "\tilde{\mu}"'] \end{tikzcd}$$

De acordo com a observação acima, a partir de agora, ao invés de uma álgebra de Clifford universal, diremos a álgebra de Clifford universal.

Note que, se $\dim V = n$, então pela proposição 1.1.14, existe uma base $\mathfrak{B}_V = \{e_1, \ldots, e_n\}$ ortogonal em relação à forma bilinear B de V. Da condição de Clifford, para $1 \leq i, j \leq n$, obtemos as relações:

$$\mu(e_i) \cdot \mu(e_i) = Q(e_i)\mathbf{1}, \ i = j \quad (2.1) \qquad \mu(e_i) \cdot \mu(e_j) = -\mu(e_j) \cdot \mu(e_i), \ i \neq j \quad (2.2)$$

Logo, considerando a base $\mathfrak{B}_V$ de V, pela observação 2.1.4 e usando (2.1) e (2.2), segue que a álgebra de Clifford é gerada por $\{\mu(e_1)^{j_1} \cdot \ldots \cdot \mu(e_n)^{j_n} \mid j_1, \ldots, j_n = 0, 1\}$, onde $\mu(e_1)^0 \cdot \ldots \cdot \mu(e_n)^0 := \mathbf{1}$. Do princípio multiplicativo, há 2^n elementos da forma $\mu(e_1)^{j_1} \cdot \ldots \cdot \mu(e_n)^{j_n}$, implicando que a dimensão máxima da álgebra de Clifford universal é $2^n = 2^{\dim V}$.

Abaixo, segue um resultado que garante quando uma álgebra de Clifford possui a propriedade universal.

Proposição 2.1.5. *Seja (A, μ) uma álgebra de Clifford associada à (V, B) e $\dim V = n$. Se $\dim A = 2^n$, então A é uma álgebra de Clifford universal.*

Demonstração: Seja $\mathfrak{B}_V = \{e_1, \ldots, e_n\}$ uma base ortogonal em relação à B de V e (A, μ) uma álgebra de Clifford associada à (V, B) satisfazendo as condições i), ii) e iii) da definição 2.1.1.

Considere o par (A', ϕ) tal que A' é uma $\mathbb{F}$-álgebra e $\phi : V \to A'$ uma transformação linear tal que $\phi(e_i) \cdot \phi(e_j) + \phi(e_j) \cdot \phi(e_i) = 2B(e_i, e_j)1_{A'}$, $1 \leq i \leq j \leq n$, $e_i, e_j \in \mathfrak{B}_V$. Defina a seguinte aplicação $\widetilde{\phi} : A \to A'$ por $\widetilde{\phi}(\mu(e_{i_1}) \cdot \ldots \cdot \mu(e_{i_k})) = \phi(e_{i_1}) \cdot \ldots \cdot \phi(e_{i_k})$ e $\widetilde{\phi}(1_A) = 1_{A'}$. Claramente, $\widetilde{\phi}$ é um homomorfismo de álgebras tal que $\widetilde{\phi} \circ \mu = \phi$.

Portanto, (A, μ) é uma álgebra de Clifford universal associada à (V, B). ∎

Como iremos trabalhar apenas com álgebras de Clifford universais, omitiremos a partir de agora, a palavra universal. Nos seguintes exemplos, usaremos alguns dos exemplos de álgebras vistos no exemplo 1.1.4 e de formas bilineares e quadráticas, vistos no exemplo 1.1.16.

Exemplo 2.1.6. *Seja V um $\mathbb{F}$-espaço vetorial e Q a forma quadrática associada à B.*

i) Sejam V unidimensional, com base $\{e\}$ e A uma $\mathbb{F}$-álgebra com base $\{1_A, x\}$. Seja $\mu : V \to A$ a transformação linear tal que $\mu(e) = x$. Claramente, o par (A, μ) satisfaz os itens i), ii) e iii) da definição 2.1.1. *Como* $\dim A = 2^1$, *pela proposição* 2.1.5, *segue que (A, μ) é a álgebra de Clifford associada à (V, B), sendo $x^2 = Q(e)1_A$.*

Se $\mathbb{F} = \mathbb{R}$ e $B = B_{0,1}$, então a álgebra de Clifford é a $\mathbb{R}$-álgebra dos números complexos $\mathbb{C}$, onde a aplicação de Clifford é definida por $\mu(e) = i$ satisfazendo $\mu(e)^2 = -1_{\mathbb{C}}$. Neste caso, denotamos a álgebra de Clifford por $\mathcal{C}\ell_{0,1}$.

De maneira análoga, porém tomando $B = B_{1,0}$, segue que $\mathcal{C}\ell_{1,0} \cong \mathbb{R} \oplus \mathbb{R}$, sendo a aplicação de Clifford dada por $\mu(e) = (0, 1)$ e satisfazendo $\mu(e)^2 = (1, 0) = 1_{\mathbb{R}\oplus\mathbb{R}}$, onde $(a, b)(c, d) = (ac + bd, ad + bc)$.

ii) Seja V um $\mathbb{F}$-espaço vetorial com base ortogonal $\{e_1, e_2\}$ em relação à B e considere A uma $\mathbb{F}$-álgebra com base $\{1_A, x, y, z\}$. Definindo a transformação linear $\mu : V \to A$ por $\mu(e_1) = x$ e $\mu(e_2) = y$, segue que (A, μ) é a álgebra de Clifford associada à (V, B), em que $x^2 = Q(e_1)1_A$, $y^2 = Q(e_2)1_A$ e $x \cdot y = -y \cdot x$.

Considerando $\mathbb{F} = \mathbb{R}$ e $B = B_{0,2}$, temos que $\mathcal{C}\ell_{0,2} \cong \mathbb{H}$, onde a aplicação de Clifford é tal que $\mu(e_1) = i$ e $\mu(e_2) = j$, satisfazendo $\mu(e_1)^2 = \mu(e_2)^2 = -1_{\mathbb{H}}$.

Nas mesmas condições, considerando $B = B_{2,0}$ e $B = B_{1,1}$, temos que $\mathcal{C}\ell_{2,0} \cong \mathcal{C}\ell_{1,1} \cong \mathbb{M}(2, \mathbb{R})$, onde $\mathbb{M}(2, \mathbb{R})$ é a $\mathbb{R}$-álgebra das matrizes de ordem 2 *com* *entradas reais. De fato: sendo* $\{1, x, y, x\cdot y\}$ *e* $\{1', x', y', x'\cdot y'\}$ *bases de* $\mathcal{C}\ell_{2,0}$ *e* $\mathcal{C}\ell_{1,1}$ *respectivamente, temos que um elemento de* $\mathcal{C}\ell_{2,0}$ *é da forma* $a_0 1 + a_1 x + a_2 y + a_3 x\cdot y$, *onde* $a_0, a_1, a_2, a_3 \in \mathbb{R}$, *tal que* $x^2 = y^2 = 1$. *Já um elemento de* $\mathcal{C}\ell_{1,1}$ *é da forma* $b_0 1' + b_1 x' + b_2' y' + b_3' x' \cdot y'$, *onde* $b_0, b_1, b_2, b_3 \in \mathbb{R}$, *sendo* $(x')^2 = 1$ *e* $(y')^2 = -1$. *Agora basta ver que as transformações lineares* $\mathcal{C}\ell_{2,0} \to \mathcal{C}\ell_{1,1}$ *e* $\mathcal{C}\ell_{2,0} \to \mathbb{M}(2, \mathbb{R})$ *definidas, respectivamente, por* $1 \mapsto 1'$, $x \mapsto x'$, $y \mapsto y'$, $x \cdot y \mapsto x' \cdot y'$ *e* $1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $x \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $y \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $x \cdot y \mapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, *são isomorfismos, onde* $\left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right\}$ *é uma base para* $\mathbb{M}(2, \mathbb{R})$.

vi) Em $\mathbb{C}$ *toda forma bilinear não-degenerada é da forma descrita no item iv) do exemplo* 1.1.16. *Denotando por* $\mathbb{C}\ell_n$ *a álgebra de Clifford* $\mathcal{C}\ell(\mathbb{C}^n, B)$, $n \in \mathbb{N}^*$, *obtemos, de forma análoga a* $\mathcal{C}\ell_{1,0}$, *que* $\mathbb{C}\ell_1 \cong \mathbb{C} \oplus \mathbb{C}$, *onde* $\mathbb{C} \oplus \mathbb{C}$ *é uma* $\mathbb{C}$-*álgebra, obtida da mesma forma que* $\mathbb{R} \oplus \mathbb{R}$.

Em geral, utilizamos a notação $\mathcal{C}\ell_{p,q}$ para indicar a álgebra de Clifford real associada ao produto interno negativo.

Chamamos a atenção para três situações que ocorrem aqui, mas que podem ser encontradas de forma diferente em textos que tratam sobre álgebra de Clifford, dependendo da definição escolhida.

1ª) As $\mathbb{R}$-álgebras $\mathcal{C}\ell_{0,3}$ e $\mathbb{H} \oplus \mathbb{H}$ não são isomorfas, onde consideramos a operação $(a, b)(c, d) := (ac - b\overline{d}, ad + b\overline{c})$, pois em $\mathbb{H} \oplus \mathbb{H}$ não vale a associatividade.

2ª) Se $Q \equiv 0$, então não existe a álgebra de Clifford $\mathcal{C}\ell(V, 0)$, pois, nesse caso, a forma bilinear associada a forma quadrática é degenerada.

3ª) A primeira condição da definição de álgebra de Clifford, nos impede de definir $\mathcal{C}\ell_{0,0}$ por $\mathbb{R}$.

Neste texto, o conceito de involução abordado é diferente do conceito dado em álgebra em geral. Uma *involução* de um conjunto não-vazio X é uma função $f : X \to X$ tal que $f \circ f = \mathrm{id}_X$ (ou seja $f^2 = \mathrm{id}_X$). Veremos em seguida três aplicações, as quais são involuções não-triviais de álgebras de Clifford.

Observação 2.1.7. *Se f é uma involução, então f é bijetora e $f^{-1} = f$.*

Proposição 2.1.8. *Seja $\mathcal{C}\ell(V,B)$ a álgebra de Clifford associada à (V,B). Se a aplicação $g_0 : V \to \mathcal{C}\ell(V,B)$ é tal que $g_0(v) = -\mu(v)$, $\forall v \in V$, então existe um único automorfismo $g : \mathcal{C}\ell(V,B) \to \mathcal{C}\ell(V,B)$ tal que $g^2 = \mathrm{id}$ e $g \circ \mu = g_0$.*

Demonstração: Note que g_0 é uma aplicação de Clifford, pois pela forma que foi definida é uma transformação linear, satisfazendo a condição de Clifford, ou seja, $g_0(v) \cdot g_0(u) + g_0(u) \cdot g_0(v) = (-\mu(v)) \cdot (-\mu(u)) + (-\mu(u)) \cdot (-\mu(v)) = 2B(v,u)\mathbf{1}$, $\forall v, u \in V$. Logo, pelo item iv) da definição 2.1.1, existe um único homomorfismo $g : \mathcal{C}\ell(V,B) \to \mathcal{C}\ell(V,B)$ tal que $g \circ \mu = g_0$, isto é, $g(\mu(v)) = -\mu(v)$ **(1)**.

Dado $a = \lambda_0\mathbf{1} + \sum \lambda_{i_1 \dots i_k} \mu(v_1) \cdot \ldots \cdot \mu(v_k) \in \mathcal{C}\ell(V,B)$, $k \in \mathbb{N}^*$, segue de (1) que $g(a) = \lambda_0\mathbf{1} + (-1)^k \sum \lambda_{i_1 \dots i_k} \mu(v_1) \cdot \ldots \cdot \mu(v_k)$. Logo, decorre que $g^2 = \mathrm{id}$ e pela observação 2.1.7, g é bijetora e portanto, g é um automorfismo e uma involução.

■

Definição 2.1.9. O automorfismo g da proposição 2.1.8, denotado por $g(a) = \widehat{a}$, $\forall a \in \mathcal{C}\ell(V,B)$, é chamado de *involução graduada* ou *automorfismo canônico.*

Segue direto da proposição 2.1.8, que podemos decompor a álgebra de Clifford em subconjuntos que possuem elementos que são invariantes sob a involução graduada com os elementos que trocam de sinal sob a ação desta, onde a interseção desses subconjuntos é formada apenas pelo elemento neutro.

Proposição 2.1.10. *Seja $\mathcal{C}\ell(V,B)$ a álgebra de Clifford associada à (V,B). Se $A^0 = \{a \in \mathcal{C}\ell(V,B) \mid \widehat{a} = a\}$ e $A^1 = \{a \in \mathcal{C}\ell(V,B) \mid \widehat{a} = -a\}$, então A^0 é uma subálgebra, A^1 um subespaço vetorial e $\mathcal{C}\ell(V,B) = A^0 \oplus A^1$ como subespaços vetoriais.*

Demonstração: Mostremos que A^0 é subálgebra. Como a involução graduada é, em particular, um homomorfismo, segue que $\mathbf{1} \in A^0$. Se $a, b \in A^0$ e $\lambda \in \mathbb{F}$, então

$$\widehat{a + \lambda b} = \widehat{a} + \lambda \widehat{b} = a + \lambda b \in A^0 \text{ e } \widehat{a \cdot b} = \widehat{a} \cdot \widehat{b} = a \cdot b \in A^0.$$

Analogamente, prova-se que A^1 é um subespaço vetorial. Claramente, $\mathcal{C}\ell(V,B) = A^0 + A^1$ e se $a \in A^0 \cap A^1$, então $a = -a$ se, e somente se, $a = \mathbf{0}$, implicando que $\mathcal{C}\ell(V,B) = A^0 \oplus A^1$.

■

Definição 2.1.11. Chamamos a subálgebra A^0 de *parte par* e o subespaço vetorial A^1 de *parte ímpar* da álgebra de Clifford $\mathcal{C}\ell(V,B)$, denotadas por $\mathcal{C}\ell(V,B)^0$ e $\mathcal{C}\ell(V,B)^1$, respectivamente.

Definição 2.1.12. Seja $(\Lambda, +)$ um grupo aditivo. Uma álgebra A é Λ-*graduada* se $A = \bigoplus_{i \in \Lambda} A_i$, onde A_i é subespaço vetorial de A, tal que se $x \in A_i$ e $y \in A_j$, então $x \cdot y \in A_{i+j}$, sendo $i + j \in \Lambda$.

Observação 2.1.13. *Segue da definição acima, que toda álgebra de Clifford é $\mathbb{Z}_2$-graduada.*

Considere a aplicação $\bullet : \mathcal{C}\ell(V,B) \times \mathcal{C}\ell(V,B) \to \mathcal{C}\ell(V,B)$ definida por $a \bullet b := b \cdot a$. É claro que $(\mathcal{C}\ell(V,B), \bullet)$ é uma $\mathbb{F}$-álgebra, a qual é denotada por $\mathcal{C}\ell(V,B)^{\text{op}}$ e que $\mathcal{C}\ell(V,B)^{\text{op}}$ e $\mathcal{C}\ell(V,B)$ são conjuntos iguais.

Proposição 2.1.14. *Seja $\mathcal{C}\ell(V,B)$ a álgebra de Clifford associada à (V,B). Se $r_0 : V \to \mathcal{C}\ell(V,B)^{\text{op}}$ é tal que $r_0(v) = \mu(v), \forall v \in V$, então existe um único anti-automorfismo $r : \mathcal{C}\ell(V,B) \to \mathcal{C}\ell(V,B)$ tal que $r^2 = \text{id}$ e $r \circ \mu = r_0$.*

Demonstração: Claramente, r_0 é uma aplicação de Clifford. Sendo assim, existe um único homomorfismo $r : \mathcal{C}\ell(V, B) \to \mathcal{C}\ell(V, B)^{\text{op}}$ tal que $r \circ \mu = r_0$, isto é, $r(\mu(v)) = \mu(v)$, $\forall v \in V$. Se $a, b \in \mathcal{C}\ell(V, B)$, então $r(a \cdot b) = r(a) \bullet r(b) = r(b) \cdot r(a)$, ou seja, $r : \mathcal{C}\ell(V, B) \to \mathcal{C}\ell(V, B)$ é um anti-homomorfismo.

Por fim, dado $a = \lambda_0 \mathbf{1} + \sum \lambda_{i_1 \ldots i_k} \mu(v_1) \cdot \ldots \mu(v_k) \in \mathcal{C}\ell(V, B)$, $k \in \mathbb{N}^*$, temos que: $r(a) = \lambda_0 \mathbf{1} + \sum \lambda_{i_1 \ldots i_k} \mu(v_k) \cdot \ldots \cdot \mu(v_1)$. Daí segue que r é uma involução e bijetora. Portanto, r é uma involução e um anti-automorfismo. ■

Definição 2.1.15. Chamamos o anti-automorfismo r da proposição 2.1.14, de *reversão* ou *anti-automorfismo principal* e o denotamos por $r(a) = a^*$, $\forall a \in \mathcal{C}\ell(V, B)$.

Já vimos duas involuções na álgebra de Clifford, sendo uma um automorfismo e outra um anti-automorfismo. Veremos que a composição destas duas involuções é comutativa e descreve outra involução.

Proposição 2.1.16. *Se $\mathcal{C}\ell(V, B)$ é a álgebra de Clifford associada à (V, B), então a aplicação $\widehat{(.)} \circ (.)^* : \mathcal{C}\ell(V, B) \to \mathcal{C}\ell(V, B)$ satisfaz $\widehat{(.)} \circ (.)^* = (.)^* \circ \widehat{(.)}$, é uma involução e um anti-automorfismo.*

Demonstração: Se $a = \lambda_0 \mathbf{1} + \sum \lambda_{i_1 \ldots i_k} \mu(v_1) \cdot \ldots \cdot \mu(v_k) \in \mathcal{C}\ell(V, B)$, então $\widehat{a}^* = \widehat{a^*}$, pois $\widehat{\mu(v)^*} = \widehat{\mu(v)} = -\mu(v) = -(\mu(v)^*) = (-\mu(v))^* = \widehat{\mu(v)}^*$. Como $\widehat{(.)} \circ (.)^*$ é uma involução, obtemos a bijetividade. Ainda, para cada $a, b \in \mathcal{C}\ell(V, B)$ e todo $\lambda \in \mathbb{F}$, temos que: $(\widehat{\mathbf{1}})^* = \mathbf{1}$, $\widehat{(a + \lambda b)}^* = (\widehat{a} + \lambda \widehat{b})^* = (\widehat{a})^* + \lambda (\widehat{b})^*$ e $\widehat{(a \cdot b)}^* = (\widehat{a} \cdot \widehat{b})^* = (\widehat{b})^* \cdot (\widehat{a})^*$. ■

Definição 2.1.17. Chamamos o anti-automorfismo da proposição 2.1.16 de *conjugação* e o denotamos por $\widehat{a}^* = \overline{a}$, $\forall a \in \mathcal{C}\ell(V, B)$.

Exemplo 2.1.18. *Veremos nos ítens abaixo que o anti-automorfismo conjugação é uma generalização do conceito de conjugação dos números complexos e quatérnios.*

i) Seja a álgebra de Clifford $\mathcal{C}\ell_{0,1} \cong \mathbb{C}$. *Se* $z = a1_{\mathbb{C}} + bi \in \mathbb{C}$, *com* $a, b \in \mathbb{R}$, *então* $\widehat{z} = \overline{z} = a1_{\mathbb{C}} - bi$ *e* $z^* = z$.

ii) Considerando a álgebra de Clifford $\mathcal{C}\ell_{1,0} \cong \mathbb{R} \oplus \mathbb{R}$, *temos que se* $(x, y) = x(1, 0) + y(0, 1) \in \mathbb{R} \oplus \mathbb{R}$, $x, y \in \mathbb{R}$, *então* $\widehat{(x, y)} = \overline{(x, y)} = (x, -y)$ *e* $(x, y)^* = (x, y)$.

iii) Seja $\mathcal{C}\ell_{0,2} \cong \mathbb{H}$. *Dado* $h = a1_{\mathbb{H}} + bi + cj + dk \in \mathbb{H}$, $a, b, c, d \in \mathbb{R}$, *temos que se* $k = ij$, *então* $\widehat{k} = \widehat{ij} = \widehat{i}\widehat{j} = (-i)(-j) = ij = k$, $k^* = (ij)^* = j^* i^* = ji = -k$ *e* $\overline{k} = \widehat{k}^* = -k$. *Logo,* $\widehat{h} = a\widehat{1_{\mathbb{H}}} - b\widehat{i} - c\widehat{j} + d\widehat{k}$, $h^* = a1_{\mathbb{H}} + bi + cj - dk$ *e* $\overline{h} = \widehat{h}^* = a1_{\mathbb{H}} - bi - cj - dk$.

iv) Se $x = a\mathbf{1} + b\mu(e_1) + c\mu(e_2) + d\mu(e_3) + e\mu(e_1) \cdot \mu(e_2) + f\mu(e_1) \cdot \mu(e_3) + g\mu(e_2) \cdot \mu(e_3) + h\mu(e_1) \cdot \mu(e_2) \cdot \mu(e_3) \in \mathcal{C}\ell_{0,3}$, *então*

$x^* = a\mathbf{1} + b\mu(e_1) + c\mu(e_2) + d\mu(e_3) - e\mu(e_1) \cdot \mu(e_2) - f\mu(e_1) \cdot \mu(e_3) - g\mu(e_2) \cdot \mu(e_3) - h\mu(e_1) \cdot \mu(e_2) \cdot \mu(e_3)$,

$\widehat{x} = a\mathbf{1} - b\mu(e_1) - c\mu(e_2) - d\mu(e_3) + e\mu(e_1) \cdot \mu(e_2) + f\mu(e_1) \cdot \mu(e_3) + g\mu(e_2) \cdot \mu(e_3) - h\mu(e_1) \cdot \mu(e_2) \cdot \mu(e_3)$ *e*

$\overline{x} = a\mathbf{1} - b\mu(e_1) - c\mu(e_2) - d\mu(e_3) - e\mu(e_1) \cdot \mu(e_2) - f\mu(e_1) \cdot \mu(e_3) - g\mu(e_2) \cdot \mu(e_3) + h\mu(e_1) \cdot \mu(e_2) \cdot \mu(e_3)$.

Observação 2.1.19. *Daqui em diante, trabalharemos apenas com álgebras de Clifford tais que a dimensão do espaço vetorial* V *é finita.*

Vamos mostrar que se a dimensão do espaço vetorial V é finita, então a dimensão da álgebra de Clifford sobre ele também é finita. Para isso, falaremos sobre o produto tensorial graduado e enunciaremos um lema.

Sejam $A = A^0 \oplus A^1$ e $B = B^0 \oplus B^1$ $\mathbb{F}$-álgebras $\mathbb{Z}_2$-graduadas. O produto tensorial $(A \otimes B, \otimes)$ munido da operação definida por

$$(a' \otimes b) \cdot (a \otimes b') := (-1)^{ij} (a' \cdot_A a) \otimes (b' \cdot_B b), \text{ onde } a \in A^i \text{ e } b \in B^j \qquad (2.1)$$

é uma $\mathbb{F}$-álgebra $\mathbb{Z}_2$-graduada tal que $A \otimes B = (A \otimes B)^0 \oplus (A \otimes B)^1$, sendo $(A \otimes B)^0 := (A^0 \otimes B^0) \oplus (A^1 \otimes B^1)$ e $(A \otimes B)^1 := (A^0 \otimes B^1) \oplus (A^1 \otimes B^0)$.

O *produto tensorial $\mathbb{Z}_2$-graduado* de A por B, denotado por $A \widehat{\otimes} B$, é o produto tensorial de A por B munido da operação (2.1).

Observação 2.1.20. *Da definição acima, segue que se $\mathcal{C}\ell(V_1, B_1)$ e $\mathcal{C}\ell(V_2, B_2)$ são álgebras de Clifford, então $\mathcal{C}\ell(V_1, B_1) \widehat{\otimes} \mathcal{C}\ell(V_2, B_2)$ é um produto tensorial $\mathbb{Z}_2$-graduado.*

Lema 2.1.21. *Seja $V = V_1 \oplus V_2$ um $\mathbb{F}$-espaço vetorial de dimensão finita e sejam $Q : V \to \mathbb{F}$ uma forma quadrática. Então são válidas as seguintes afirmações:*

i) *$Q_i := Q : V_i \to \mathbb{F}$ é uma forma quadrática sobre V_i, onde Q_i é a forma quadrática sobre V restrita a V_i.*

ii) *Se B, B_1, B_2 são as formas bilineares associadas a Q, Q_1, Q_2, respectivamente, e se $\mathcal{C}\ell(V, B)$, $\mathcal{C}\ell(V_1, B_1)$ e $\mathcal{C}\ell(V_2, B_2)$ são álgebras de Clifford, então $\mathcal{C}\ell(V_1 \oplus V_2, B_1 + B_2)$ e $\mathcal{C}\ell(V_1, B_1) \widehat{\otimes} \mathcal{C}\ell(V_2, B_2)$ são isomorfas.*

Demonstração: *i)* Imediato.

ii) Seja $\mu : V \to \mathcal{C}\ell(V, B)$ uma aplicação de Clifford e considere as restrições $\mu_1 : V_1 \to \mathcal{C}\ell(V_1, B_1)$ e $\mu_2 : V_2 \to \mathcal{C}\ell(V_2, B_2)$ que também são aplicações de Clifford. Defina a seguinte aplicação $T : V_1 \oplus V_2 \to \mathcal{C}\ell(V_1, B_1) \widehat{\otimes} \mathcal{C}\ell(V_2, B_2)$ por $T(v_1 + v_2) = \mu_1(v_1) \otimes \mathbf{1}_1 + \mathbf{1}_2 \otimes \mu_2(v_2)$, onde $v_i \in V_i$ e $\mathbf{1}_i$ é a identidade de $\mathcal{C}\ell(V_i, B_i)$.

Dado $v = v_1 + v_2 \in V$, é fácil ver que T é uma transformação linear tal que

$$\begin{aligned} T(v)^2 = T(v) \cdot T(v) &= \mu_1(v_1)^2 \otimes \mathbf{1}_1 + \mathbf{1}_2 \otimes \mu_2(v_2)^2 \\ &= Q_1(v_1)\mathbf{1}_1 \otimes \mathbf{1}_2 + \mathbf{1}_1 \otimes Q_2(v_2)\mathbf{1}_2 \\ &= (Q_1(v_1) + Q_2(v_2))\mathbf{1}_1 \otimes \mathbf{1}_2 \\ &= Q(v_1 + v_2)(\mathbf{1}_1 \otimes \mathbf{1}_2), \end{aligned}$$

onde $\mathbf{1}_1 \otimes \mathbf{1}_2$ é a identidade do produto tensorial graduado $\mathcal{C}\ell(V_1, B_1)\widehat{\otimes}\mathcal{C}\ell(V_2, B_2)$.

Logo, $T : V \to \mathcal{C}\ell(V_1, B_1)\widehat{\otimes}\mathcal{C}\ell(V_2, B_2)$ é uma aplicação de Clifford. Pela propriedade universal, existe um único homomorfismo $\widetilde{T} : \mathcal{C}\ell(V, B) \to \mathcal{C}\ell(V_1, B_1)\widehat{\otimes}\mathcal{C}\ell(V_2, B_2)$ tal que $\widetilde{T} \circ \mu = T$, sendo $\mu : V \to \mathcal{C}\ell(V, B)$ uma aplicação de Clifford.

Afirmamos que $\widetilde{T}$ é um isomorfismo. De fato, sejam r e s as dimensões de V_1 e V_2, nesta ordem, e $\{e_1, \ldots, e_r, e'_1, \ldots, e'_s\}$ uma base(ortogonal) de V. Sendo $\{i_1, \ldots, i_k\} \subset \{1, \ldots, r\}$ e $\{j_1, \ldots, j_\ell\} \subset \{1, \ldots, s\}$, com $1 \le k \le r$ e $1 \le \ell \le s$, temos que:

$$\widetilde{T}(\mathbf{1}) = \mathbf{1}_1 \otimes \mathbf{1}_2,$$

$$\widetilde{T}(\mu(e_{i_1}) \cdot \ldots \cdot \mu(e_{i_k})) = (\mu_1(e_{i_1}) \otimes \mathbf{1}_2) \ldots (\mu_1(e_{i_k}) \otimes \mathbf{1}_2) = (\mu(e_{i_1}) \cdot \ldots \cdot \mu(e_{i_k})) \otimes \mathbf{1}_2,$$

$$\widetilde{T}(\mu(e'_{j_1}) \cdot \ldots \cdot \mu(e'_{j_\ell})) = (\mathbf{1}_1 \otimes \mu_2(e'_{j_1})) \ldots (\mathbf{1}_1 \otimes \mu_2(e_{j_k})) = \mathbf{1}_1 \otimes (\mu(e'_{j_1}) \cdot \ldots \cdot \mu(e'_{j_k})).$$

Logo,

$$\widetilde{T}(\mu(e_{i_1})\cdot \ldots \cdot\mu(e_{i_k})\cdot\mu(e'_{j_1})\cdot \ldots \mu(e'_{j_\ell})) = (\mu_1(e_{i_1})\cdot \ldots \cdot\mu_1(e_{i_k}))\otimes(\mu_2(e'_{j_1})\cdot \ldots \cdot\mu_2(e'_{j_\ell}))$$

Portanto, $\widetilde{T}$ leva base em base.

■

Teorema 2.1.22. *Se $\mathfrak{B}_V = \{e_1, \ldots, e_n\}$ é finita, então a álgebra de Clifford $\mathcal{C}\ell(V, B)$ é tal que:*

i) *A aplicação de Clifford $\mu : V \to \mathcal{C}\ell(V, B)$ é injetora.*

ii) $\dim\mathcal{C}\ell(V, B) = 2^n$.

iii) $\{\mu(e_{i_1}) \cdot \ldots \cdot \mu(e_{i_k}) \mid I = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\},\ 1 \le i_1 < \ldots < i_k \le n, k \in \mathbb{N}\}$ *é uma base para $\mathcal{C}\ell(V, B)$, onde $\mu(e_{i_0}) = \mu(e_\varnothing) := \mathbf{1}$.*

iv) $\dim\mathcal{C}\ell(V, B)^0 = \dim\mathcal{C}\ell(V, B)^1 = 2^{n-1}$.

Demonstração: Sejam $\mathcal{C}\ell(V,B)$ a álgebra de Clifford e $\mu : V \to \mathcal{C}\ell(V,B)$ uma aplicação de Clifford correspondente.

i) A contra-positiva da definição 1.1.11 é dada por: se $v \in V$ é tal que $B(v,u) = 0$, para todo $u \in V$, então $v = 0_V$. Tome $v \in \ker \mu$ e veja que: $2B(v,u)\mathbf{1} = \mu(v) \cdot \mu(u) + \mu(u) \cdot \mu(v) = \mathbf{0}$. Logo, $B(v,u) = 0$, $\forall u \in V$, isto é, $v = 0$.

ii) Denotando por V_i, o subespaço gerado por $e_i \in \mathfrak{B}_V$, $1 \leq i \leq n$, temos que $V = \bigoplus_{i=1}^{n} V_i$, onde V_i é unidimensional. Pelo item i) do lema 2.1.21 segue que, $Q_i : V_i \to \mathbb{F}$ é uma forma quadrática em V_i. Ainda, $\mu_i : V_i \to \mathcal{C}\ell(V_i, B_i)$ é uma aplicação de Clifford, sendo μ_i a restrição da aplicação de Clifford μ em V_i. Usando o item ii) do mesmo lema, temos que $\mathcal{C}\ell(V,B) \cong \mathcal{C}\ell(V_1,B_1)\widehat{\otimes} \ldots \widehat{\otimes}\, \mathcal{C}\ell(V_n,B_n)$. Logo, $\dim\mathcal{C}\ell(V,B) = \prod_{i=1}^{n} \dim\mathcal{C}\ell(V_i,B_i)$ **(1)**. Mas V_i é unidimensional e conforme o item i) do exemplo 2.1.6 podemos concluir que $\dim\mathcal{C}\ell(V_i,B_i) = 2$.

Portanto, de (1), segue que $\dim\mathcal{C}\ell(V,B) = 2^n$.

iii) Note que, o conjunto dado no enunciado do item iii) gera a álgebra de Clifford. E cada elemento desse conjunto é obtido determinando um subconjunto $I \subset \{1,\ldots,n\}$. Logo, pelo princípio da contagem, o conjunto possui 2^n elementos e por i), segue o resultado.

iv) Veja que, determinar a dimensão de $\mathcal{C}\ell(V,B)^0$ e de $\mathcal{C}\ell(V,B)^1$ é equivalente a determinar o número de subconjuntos $I \subset \{1,\ldots,n\}$ com número par e ímpar de elementos, os quais denotamos por p e i, respectivamente. Logo, $\dim\mathcal{C}\ell(V,B)^0 = p$ e $\dim\mathcal{C}\ell(V)^1 = i$. Da combinatória, temos que $p = i$ e, por outro lado, $p + i = 2^n$, donde segue que $p = i = 2^{n-1}$. ■

Pela definição 2.1.1, observação 1.1.3 e do teorema 2.1.22, segue que $\mathbb{F}$ e V são subespaços distintos em $\mathcal{C}\ell(V,B)$. A partir de agora, escrevemos a condição de Clifford por: $v \cdot u + u \cdot v = 2B(v, u)$, $\forall v, u \in V$ e denotaremos a base de $\mathcal{C}\ell(V, B)$ simplesmente por $\{e_I := e_{i_1} \cdot \ldots \cdot e_{i_k} \mid I = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}, 1 \leq k \leq n\}$, onde $e_{i_k} \in \mathfrak{B}_V$.

O *centro* da álgebra de Clifford $\mathcal{C}\ell(V, B)$, denotado por $\mathcal{Z}(\mathcal{C}\ell(V, B))$, é o conjunto de todos os elementos $a \in \mathcal{C}\ell(V, B)$ tais que $a \cdot b = b \cdot a$, para todo $b \in \mathcal{C}\ell(V, B)$.

Proposição 2.1.23. *Sejam $\mathcal{C}\ell(V, B)$ a álgebra de Clifford associada à (V, B). São válidas as afirmações:*

i) Se $\dim_{\mathbb{F}} V = n$ é par, então $\mathcal{Z}(\mathcal{C}\ell(V, B)) = \mathbb{F}$.

ii) Se $\dim_{\mathbb{F}} V = n$ é ímpar, então $\mathcal{Z}(\mathcal{C}\ell(V, B)) = \mathbb{F} \oplus V^n$, sendo V^n o subespaço gerado por $e_1 \cdot \ldots \cdot e_n$, onde $e_1, \ldots, e_n \in \mathfrak{B}_V$.

Demonstração: Ver [**18**], pg. 13. ∎

Exemplo 2.1.24. *Abaixo segue a confirmação de que vale a comutatividade em $\mathbb{C}$ e a não-comutatividade em $\mathbb{H}$.*

i) Sendo a álgebra de Clifford $\mathcal{C}\ell_{0,1} \cong \mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ com dimensão 2, temos que $\mathcal{Z}(\mathbb{C}) = \mathbb{R} \oplus \mathbb{R}i = \mathbb{C}$, pois $\dim_{\mathbb{R}} V = 1$ é ímpar. Mais ainda, $\mathbb{C}^0 = \mathbb{R}$ e $\mathbb{C}^1 = \mathbb{R}i$.

ii) Seja $\mathcal{C}\ell_{1,0} \cong \mathbb{R} \oplus \mathbb{R}$ de dimensão 2. Temos que $\mathcal{Z}(\mathbb{R} \oplus \mathbb{R}) = \mathbb{R} \oplus \mathbb{R}$, $(\mathbb{R} \oplus \mathbb{R})^0 = \mathbb{R} \oplus \{0\}$ e $(\mathbb{R} \oplus \mathbb{R})^1 = \{0\} \oplus \mathbb{R}$. O mesmo vale para $\mathbb{C}\ell_1 \cong \mathbb{C} \oplus \mathbb{C}$.

iii) Como $\mathcal{C}\ell_{0,2} \cong \mathbb{H}$ e $\dim_{\mathbb{R}} \mathbb{H} = 4$ ($\dim_{\mathbb{R}} V = 2$ é par), segue que $\mathcal{Z}(\mathbb{H}) = \mathbb{R}$, $\mathbb{H}^0 = \mathbb{R} \oplus \mathbb{R}k$ e $\mathbb{H}^1 = \mathbb{R}i \oplus \mathbb{R}j$.

2.2 O Grupo de Clifford

Particularizamos nosso estudo para as álgebras de Clifford reais, onde focaremos no estudo dos números de Clifford, que são os elementos do espaço paravetorial $\mathbb{R} \oplus \mathbb{R}^n$ da álgebra de Clifford $\mathcal{C}\ell_{0,n}$. Dessa forma, definiremos o grupo de Clifford como sendo o grupo obtido por produtos finitos de números de Clifford, o qual é subgrupo formado por elementos invertíveis da álgebra de Clifford. Daremos duas caracterizações para o grupo de Clifford. Para isto, relembraremos alguns conceitos, tais como: grupo ortogonal e especial ortogonal, reflexão e ação; e também, um teorema que relaciona transformações ortogonais com reflexões. Encerramos com algumas propriedades do grupo de Clifford. Daremos exemplos no decorrer da seção.

Denotamos a álgebra de Clifford associada à $(\mathbb{R}^n, -\langle .,. \rangle)$, ou seja, $\mathcal{C}\ell_{0,n}$, simplesmente por $\mathcal{C}_n$, onde $-\langle .,. \rangle$ é o produto interno negativo e denotaremos a operação multiplicação pela justaposição. Logo, $v_1v_2+v_2v_1 = -2\langle v_1, v_2 \rangle$ e $-\|v\|^2 = v^2$, $\forall v_1, v_2, v \in V$. Estaremos sempre considerando $\{e_1, \ldots, e_n\}$ uma base ortogonal de $\mathbb{R}^n$ em relação à $-\langle .,. \rangle$ e $\{e_I := e_{i_1} \ldots e_{i_k} \mid I = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\},\ 1 \leq i_1 < \ldots < i_k \leq 1,\ k \in \mathbb{N}\}$ uma base da álgebra de Clifford $\mathcal{C}_n$.

Definição 2.2.1. Um *número de Clifford* é um elemento da forma $x_0 + v \in \mathcal{C}_n$, onde $x_0 \in \mathbb{R}$ e $v = x_1e_1 + \ldots + x_ne_n \in \mathbb{R}^n$. O conjunto $\mathbb{R} \oplus \mathbb{R}^n$ de todos os números de Clifford, denotado por W, é chamado de *espaço paravetorial.*

Um elemento $a \in \mathcal{C}_n$ é *invertível* se existir $b \in \mathcal{C}_n$ tal que $ab = ba = 1$. Nesse caso, b é único, será denotado por a^{-1} e chamado de *inverso* de a. O grupo de todos os elementos invertíveis de $\mathcal{C}_n$ é denotado por $U(\mathcal{C}_n)$.

Considerando a aplicação $N' : \mathcal{C}_n \times \mathcal{C}_n \to \mathcal{C}_n$ definida por $N'(a, b) = \frac{1}{2}(a\overline{b} + b\overline{a})$, podemos obter outra aplicação $N : \mathcal{C}_n \to \mathcal{C}_n$ definida por $N(a) := N'(a, a)$, a qual é denominada *aplicação norma.* Se N' é restrita a $W \times W$, então N' é uma forma bilinear simétrica, sendo $N(w) := N'(w, w)$ uma norma. Com efeito: se $w = x_0 + v \in W$, onde $x_0 \in \mathbb{R}$ e $v \in \mathbb{R}^n$, então $w\overline{w} = \overline{w}w = (x_0 + v)(x_0 - v) = x_0^2 + \|v\|^2 = N(w)$, pois x_0 pertence ao centro de $\mathcal{C}_n$ e $v^2 = -\|v\|$. Da relação $w\overline{w} = \overline{w}w = N(w)$ segue o afirmado. Logo, (W, N) é um *espaço normado*, permitindo usar a notação $\|w\|^2 := N(w)$ e $\langle w, u\rangle := N'(w, u)$, $\forall w, u \in W$.

Proposição 2.2.2. *Um elemento $w \in W \subset \mathcal{C}_n$ é invertível se, e somente se, $w \neq 0$, sendo $w^{-1} = \left(\frac{1}{\|w\|^2}\right)\overline{w}$.*

Demonstração: É imediato da igualdade $w\overline{w} = \overline{w}w = \|w\|^2$. ∎

Motivados pela proposição acima, consideramos o subconjunto do grupo dos elementos invertíveis de $\mathcal{C}_n$ formado por produtos finitos de elementos não-nulos de W. Na verdade, tal subconjunto é um subgrupo de $U(\mathcal{C}_n)$, conforme nosso próximo resultado.

Proposição 2.2.3. *Considere a álgebra de Clifford $\mathcal{C}_n$. Se X denota o seguinte conjunto $\{w_1 \cdot \ldots \cdot w_k \mid \|w_i\| \neq 0,\ 1 \leq i \leq k,\ w_i \in W\}$, então $X \subset U(\mathcal{C}_n)$ é um subgrupo.*

Demonstração: Claramente, $1 \in X$ e fechado em relação a operação induzida. Se $w_1 \cdot \ldots \cdot w_k \in X$, então $(w_1 \cdot \ldots \cdot w_k)^{-1} = w_k^{-1} \cdot \ldots \cdot w_1^{-1} \in X$, pois $\|w_i^{-1}\| = \frac{1}{\|w_i\|} \neq 0$. ∎

Definição 2.2.4. O subgrupo X da proposição 2.2.3, denotado por Γ_n, é chamado de *grupo de Clifford* da álgebra de Clifford $\mathcal{C}_n$, ou seja,

$$\Gamma_n = \{a \in U(\mathcal{C}_n) \mid a = w_1 \cdot \ldots \cdot w_k,\ \|w_i\| \neq 0,\ 1 \leq i \leq k\}.$$

Exemplo 2.2.5. *Vejamos alguns grupos de Clifford, onde X^* denota a álgebra X sem o elemento nulo.*

i) Considerando $\mathcal{C}_1 \cong \mathbb{C}$, onde identificamos V com $\mathbb{R}i$, temos que $W = \mathbb{R} \oplus \mathbb{R}i = \mathbb{C}$. Logo, a aplicação norma é a norma usual dos números complexos e $\Gamma_1 = \mathbb{C}^*$.

ii) Sendo $\mathcal{C}_2 \cong \mathbb{H}$ e identificando V com $\mathbb{R}i \oplus \mathbb{R}j$, então $\Gamma_2 = \mathbb{H}^*$.

iii) Se $n > 2$, então $\Gamma_n \neq \mathcal{C}_n^*$. Tome $1+e_1e_2e_3 \in \mathcal{C}_n$ e veja que $(1+e_1e_2e_3)(1-e_1e_2e_3) = 0$. Logo, $1 + e_1e_2e_3$ é divisor próprio do zero em $\mathcal{C}_n$, ou seja, $1 + e_1e_2e_3$ não é invertível e portanto $\Gamma_n \subsetneq \mathcal{C}_n^*$.

Observação 2.2.6. *O item ii) do exemplo acima será provado mais adiante.*

Nosso objetivo agora é apresentar outra caracterização para o grupo de Clifford. Para isso, introduziremos alguns conceitos sobre transformações ortogonais, reflexões e rotações. Em seguida, apresentaremos um certo grupo, onde obteremos a aplicação representação adjunta torcida, permitindo estabelecer a igualdade entre esse novo grupo e o grupo de Clifford.

No que segue, consideramos V um $\mathbb{F}$-espaço vetorial, munido de uma forma bilinear simétrica B.

Definição 2.2.7. Uma *transformação ortogonal* de (V, B) é uma transformação linear bijetora $f : V \to V$ satisfazendo $B(f(v), f(u)) = B(v, u)$, $\forall v, u \in V$. Nesse caso, dizemos que f *preserva* a forma bilinear B.

O conjunto das transformações ortogonais de (V, B), denotado por $O_V(B)$, é um grupo com respeito a composição de funções, denominado *grupo ortogonal* de (V, B).

Proposição 2.2.8. *Seja $\mathfrak{B}$ uma base de V. Se $f : V \to V$ é uma transformação linear, então $f \in O_V(B)$ se, e somente se, $[f]^t_{\mathfrak{B}}[B]_{\mathfrak{B}}[f]_{\mathfrak{B}} = [B]_{\mathfrak{B}}$, onde $[f]_{\mathfrak{B}}$ e $[B]_{\mathfrak{B}}$ denotam a matriz da transformação linear f e da forma bilinear B, respectivamente, em relação a base $\mathfrak{B}$.*

Demonstração: Dada uma base $\mathfrak{B}$ de V, da álgebra linear, temos que se $v, u \in V$, então $B(f(v), f(u)) = [f(v)]^t_{\mathfrak{B}}[B]_{\mathfrak{B}}[f(u)]_{\mathfrak{B}}$, sendo $[f(v)]_{\mathfrak{B}} = [f]_{\mathfrak{B}}[v]_{\mathfrak{B}}$ e $[f(u)]_{\mathfrak{B}} = [f]_{\mathfrak{B}}[u]_{\mathfrak{B}}$. Logo, seguem as relações $B(f(v), f(u)) = [v]_{\mathfrak{B}}[f]^t_{\mathfrak{B}}[B]_{\mathfrak{B}}[f]_{\mathfrak{B}}[u]_{\mathfrak{B}}$ **(1)** e $B(v, u) = [v]_{\mathfrak{B}}[B]_{\mathfrak{B}}[u]_{\mathfrak{B}}$ **(2)**.

Portanto, pela arbitrariedade de v e u, e de (1) e (2), segue o desejado.

■

Corolário 2.2.9. *Se f é uma transformação ortogonal, então* $\det[f]_{\mathfrak{B}} = \pm 1$.

Demonstração: Imediato das proposições 1.1.15 e 2.2.8, e da igualdade $\det[f]_{\mathfrak{B}}^t = \det[f]_{\mathfrak{B}}$.

■

Definição 2.2.10. Uma transformação ortogonal $f \in O_V(B)$ é chamada de *reflexão* se $\det[f]_{\mathfrak{B}} = 1$, e de *rotação* se $\det[f]_{\mathfrak{B}} = -1$, onde $\mathfrak{B}$ é uma base de V.

O subconjunto do grupo ortogonal, formado por todas as rotações, denotado por $SO_V(B)$, é um subgrupo, denominado de *grupo especial ortogonal* de (V, B).

Para o nosso caso, denotaremos o conjunto de todas as transformações ortogonais de $(W, \langle .,. \rangle)$ por $O(n, \mathbb{R})$. Também denotamos o grupo especial ortogonal por $SO(n, \mathbb{R})$.

Defina o seguinte conjunto $Y := \{a \in U(\mathcal{C}_n) \mid aw\widehat{a}^{-1} \in W, \forall w \in W\}$ e vejamos que tal conjunto é um subgrupo. De fato: claramente, $1 \in Y$. Se $a \in Y$, então a aplicação $\rho_a : W \to W$ dada por $\rho_a(w) = aw\widehat{a}^{-1}$ está bem definida. Note que, $\rho_{ab} = \rho_a \circ \rho_b$ e que ρ_a é uma transformação linear bijetora, pois como ρ_a é injetora, pelo teorema do núcleo-imagem, segue a sobrejetividade. Logo, $\rho_a^{-1} = \rho_{a^{-1}}$, isto é, $a^{-1} \in Y$.

Definição 2.2.11. Chamamos a aplicação $\rho : Y \to GL(W)$ definida $\rho(a) := \rho_a : W \to W$ tal que $\rho_a(w) = aw\widehat{a}^{-1}$, de *representação adjunta torcida*, onde $GL(W)$ é o grupo das transformações lineares bijetoras em W.

Proposição 2.2.12. *Considere a álgebra de Clifford $\mathcal{C}_n$, $\rho : Y \to GL(W)$ a representação adjunta torcida e $N : \mathcal{C}_n \to \mathcal{C}_n$ a aplicação norma. São verdadeiras as seguintes afirmações:*

i) $\ker \rho = \mathbb{R}^*$.

ii) Se $a \in Y$, então $N(a) \in \mathbb{R}^*$.

iii) A aplicação norma restrita $N_{|Y} : Y \to \mathbb{R}$ é um homomorfismo.

iv) A aplicação adjunta torcida preserva o produto interno em W.

Demonstração:

i) Se $a \in \ker \rho$, então $\rho_a = \mathrm{id}_W$, ou seja, $aw\widehat{a}^{-1} = w$, $\forall w \in W$. Suponhamos, por absurdo, que $a = \sum \alpha_I e_I \notin \mathbb{R}$, onde $\{e_I \mid I \subset \{1, \ldots, n\}\}$ é uma base de $\mathcal{C}_n$. Claramente, $a \neq 0$, caso contrário, tomando $w = 1$ teríamos $1 = 0$, contrariando a observação 1.1.2. Note que, $aw\widehat{a}^{-1} = w \Leftrightarrow aw = w\widehat{a} \Leftrightarrow e_I e_i = e_i \widehat{e_I}$, onde e_i é um elemento da base de V, sendo $1 \leq i \leq n$. Temos três possibilidades:

(Caso 1) Se $\sharp I = 0$, então $e_I = 1$ e não há o que fazer.

(Caso 2) Se $\sharp I = n$, então $e_I e_i = (-1)^{n-1} e_i e_I$, mas $e_i \widehat{e_I} = (-1)^n e_i e_I$. Logo, $e_I e_i \neq e_i \widehat{e_I}$.

(Caso 3) Se $1 \leq \sharp I = k < n$, então existe $i \in I$ tal que $e_I e_i = (-1)^{k-1} e_i e_I$, mas $e_i \widehat{e_I} = (-1)^k e_i e_I$. Logo, $e_I e_i \neq e_i \widehat{e_I}$.

Portanto, como $a \neq 0$ e pelos casos acima, segue que $a \in \mathbb{R}^*$, isto é, $\ker \rho = \mathbb{R}^*$.

ii) Se $a \in Y$, então $aw\widehat{a}^{-1} \in W$, $\forall w \in W$. Temos que, $w^* = w$, em particular $(aw\widehat{a}^{-1})^* = aw\widehat{a}^{-1}$. Daí segue que $(\overline{a})^{-1} w a^* = aw\widehat{a}^{-1} \Rightarrow (\overline{a}a) w (\widehat{\overline{a}a})^{-1} = w$. Pelo item i) segue que $\overline{a}a \in \ker \rho = \mathbb{R}^*$. Logo, $\overline{a}a = a\overline{a} \in \mathbb{R}^*$, ou seja, $N(a) \in \mathbb{R}^*$.

iii) Se $a, b \in Y$, então $N(ab) = ab\overline{ab} = ab\overline{b}\overline{a} \overset{ii)}{=} a\overline{a}b\overline{b} = N(a)N(b)$.

iv) Se $a \in Y$ e $w, w' \in W$, então $\langle \rho_a(w), \rho_a(w') \rangle = aw\widehat{a}^{-1}\overline{aw'\widehat{a}^{-1}} + aw'\widehat{a}^{-1}\overline{aw\widehat{a}^{-1}} = \frac{1}{N(a)}\left(aw\overline{w'}\,\overline{a} + aw'\overline{w}\,\overline{a}\right) = \frac{1}{N(a)}(a\langle w, w' \rangle \overline{a}) = \langle w, w' \rangle$, pois $a\overline{a} = N(a)$.

■

Com o objetivo de provar que $Y = \mathit{\Gamma}_n$, vamos enunciar um resultado conhecido como teorema de Cartan-Dieudonné, cuja demonstração será omitida, porém pode ser encontrada em **[2]**, pg. 23. Após, apresentaremos algumas consequências do grupo Y em relação à representação adjunta torcida. Particularmente se $u \in W$ é tal que $u \neq 0$, denominamos a aplicação $s_u : W \to W$ definida por $s_u(w) = w - \frac{2\langle w,u\rangle}{\|u\|^2}u$, de *reflexão sobre o hiperplano ortogonal a* u (ou simplesmente *reflexão*). Usaremos um fato aqui, que será mostrado no capítulo 3, que é de s_u ser uma involução e uma reflexão.

Teorema 2.2.13 (Cartan-Dieudonné)**.** *Seja V um espaço vetorial de dimensão finita n, munido de uma forma bilinear simétrica B. Se $f : V \to V$ é uma transformação ortogonal, então existem, no máximo, n reflexões da forma s_{v_i} tais que $f = s_{v_1} \circ \ldots \circ s_{v_k}$, onde $1 \leq k \leq n$, sendo $s_{v_i}(v) = v - \frac{2B(v,v_i)}{Q(v_i)}v_i$ e $Q(v_i) = B(v_i, v_i) \neq 0$.*

Proposição 2.2.14. *Se $\rho : Y \to GL(W)$ é a representação adjunta torcida, então são verdadeiras as afirmações:*

i) $\rho_a \in SO(n, \mathbb{R})$.

ii) *Toda rotação em $SO(n, \mathbb{R})$ é da forma ρ_a e $Y = \mathit{\Gamma}_n$.*

Demonstração:

i) Se $u \in W$ é tal que $u \neq 0$, isto é, $\|u\| \neq 0$, então considere a reflexão s_u. Mostremos que $\rho_u = s_u \circ s_1$. Com efeito: dado $w \in W$, temos que $s_u(s_1(w)) = s_u(-\overline{w}) = -\overline{w} - \frac{2\langle -\overline{w},u\rangle}{\|u\|^2}u = -\overline{w} + (\overline{w}\ \overline{u} + uw)(\overline{u})^{-1} = uw\widehat{u}^{-1}$, pois $\overline{u} = \widehat{u}$. Logo, $\rho_u = s_u \circ s_1$, mostrando que $\rho_u \in SO(n, \mathbb{R})$. Mais ainda, sendo cada reflexão uma involução, segue que $s_1 \circ s_u = s_1^{-1} \circ s_u^{-1} = (s_u \circ s_1)^{-1} = \rho_u^{-1} = \rho_{u^{-1}}$.

ii) Se $f \in SO(n, \mathbb{R})$ é uma rotação, então, pelo teorema de Cartan-Dieudonné, existe um número par de reflexões $s_{w_1}, \ldots, s_{w_k}$ tais que $f = s_{w_1} \circ \ldots \circ s_{w_k}$, com $\|w_i\| \neq 0$. Como s_w é uma involução e ρ um homomorfismo, segue que $f = (s_{w_1} \circ s_1) \circ (s_1 \circ s_{w_2}) \circ \ldots \circ (s_1 \circ s_{w_k}) = \rho_{w_1} \circ \ldots \circ \rho_{w_k} = \rho_{w_1 \ldots w_k} = \rho_a$, com $a \in Y$. Logo,

$\rho_{a(w_1\dots w_k)^{-1}} = \mathrm{id}_W$ e de acordo com o item i) da proposição 2.2.12, implica que $a(w_1 \dots w_k)^{-1} = \lambda \in \mathbb{R}^*$. Logo, $a = \lambda w_1 \dots w_k = u_1 \dots u_k$, para $u_1 = \lambda w_1 \neq 0$ e $u_i = w_i \neq 0$, para $2 \leq i \leq k$. Portanto, $\|u_j\| \neq 0$, $1 \leq j \leq k$, mostrando que $a = u_1 \dots u_k \in \mathit{\Gamma}_n$, ou seja, $Y \subset \mathit{\Gamma}_n$.

Reciprocamente, se $a \in \mathit{\Gamma}_n$, então existem $u_1 \dots u_k \in W$ tais que $a = u_1 \dots u_k$ com $\|u_i\| \neq 0$. Para cada $w \in W$, vale que $w\overline{u_i} + u_i\overline{w} = 2\langle w, u_i\rangle$ e multiplicando a direita essa igualdade por u_i, segue que $u_i\overline{w}u_i = 2\langle w, u_i\rangle u_i - \|u_i\|^2 w \in W$. Substituindo w por $\overline{w}$ e usando o fato de que $w^* = w$, obtemos $u_i w u_i^* \in W$. Logo, repetindo esse processo, iniciando com u_k até u_1, obtemos: $u_1 \dots u_k w u_k^* \dots u_1^* = awa^* = aw\frac{1}{N(a)}\widehat{a}^{-1} \in W \Rightarrow aw\widehat{a}^{-1} \in W$, isto é, $a \in Y$.

■

Decorre da proposição 2.2.14 que podemos definir $\|a\|^2 = N(a)$, $\forall \in \mathit{\Gamma}_n$, pois se $a = w_1 \dots w_k \in \mathit{\Gamma}_n$, então $N(a) = N(w_1) \dots N(w_k) = \|w_1\|^2 \dots \|w_k\|^2 \geq 0$. Logo, os ítens ii) e iii) de 2.2.12 podem ser reescritos por $a\overline{a} = \overline{a}a = \|a\|^2$ e $\|ab\| = \|a\|\|b\|$, $\forall a, b \in \mathit{\Gamma}_n$. Ainda, se $a \in \mathit{\Gamma}_n$, então $a^{-1} = \frac{1}{\|a\|^2}\overline{a}$.

A proposição abaixo esclarece o item ii) de 2.2.5 e apresenta algumas propriedades do grupo de Clifford.

Proposição 2.2.15. *São verdadeiras as afirmações abaixo:*

i) *Se $a, b \in \{w \in W \mid \|w\| < 1\}$ são tais que $a, b \neq 0$ e $ab \neq 1$, então $k := 1 + a\widehat{b} \neq 0$ e é o produto de dois elementos não-nulos de W, isto é, $k \in \mathit{\Gamma}_n$. Mais ainda, se $q := \frac{1}{\|k\|}k$, então $q \in \mathit{\Gamma}_n$, $\|q\| = 1$ e a aplicação $w \mapsto qwq^* \in SO(n, \mathbb{R})$ é uma rotação em W.*

ii) *$\mathit{\Gamma}_2 = \mathbb{H}^*$.*

iii) *Se $a \in \mathit{\Gamma}_n$, então $\widehat{a}, a^*, \overline{a} \in \mathit{\Gamma}_n$.*

iv) Se $a, b \in \Gamma_n$, então $ab^{-1} \in W$ se, e somente se, $a^*b \in W$.

Demonstração:

i) Sejam $a, b \in \{w \in W \mid \|w\| < 1\}$ tais que $a, b \neq 0$ e $ab \neq 1$. Claramente, $a, b \in \mathit{\Gamma}_n$ e $1 + a\widehat{b} \neq 0$, caso contrário, teríamos $a = -\widehat{b}^{-1}$ implicando que $\|a\| = \frac{1}{\|b\|} > 1$.

Temos que, $1 + a\widehat{b} = a(a^{-1} + \widehat{b}) \neq 0$ é o produto de dois elementos não-nulos de W, isto é, $1 + a\widehat{b} \in \mathit{\Gamma}_n$. Fazendo $k := 1 + a\widehat{b} \in W$ e $q := \frac{1}{\|k\|}k$, então $q \in \mathit{\Gamma}_n$ e $\|q\|^2 = \left\|\frac{1}{\|k\|}k\right\|^2 = \frac{1}{\|k\|}k\frac{1}{\|k\|}\overline{k} = \frac{\|k\|^2}{\|k\|^2} = 1 \Rightarrow \|q\| = 1$. Logo, a aplicação $w \to qw\widehat{q}^{-1} = qw\frac{1}{\|q\|^2}q^* = qwq^* = \rho_q$ é uma rotação em W, ou seja, $\rho_q \in SO(n, \mathbb{R})$.

ii) Basta usar a segunda caracterização do grupo de Clifford, ou seja, se $a \in \mathbb{H}^*$, então $aw\widehat{a}^{-1} = \frac{1}{\|a\|^2}awa^* \in W = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j$, para todo $w \in W$.

iii) Basta usar a primeira caracterização do grupo de Clifford, isto é, dado $a \in \mathit{\Gamma}_n$, existem $w_1, \ldots, w_k \in W$, com $w_i \neq 0$, tais que $a = w_1 \ldots w_k$. Segue o resultado do fato de que $a^* = w_k \ldots w_1$, $\widehat{a} = \widehat{w_1} \ldots \widehat{w_k}$, pois $\|\widehat{w_i}\| = \|w_i\|$, e $\overline{a} = \widehat{a}^*$.

iv) Se $b \in \mathit{\Gamma}_n$, então $bw\widehat{b}^{-1} = \frac{1}{\|b\|^2}bwb^* \in W \Rightarrow bwb^* \in W$. Como $b^* \in \mathit{\Gamma}_n$, analogamente, segue que $b^*wb \in W$. Logo, $ab^{-1} \in W \Leftrightarrow (ab^{-1})^* = (b^*)^{-1}a^* \in W \Leftrightarrow b^*((b^*)^{-1}a^*)b \in W \Leftrightarrow a^*b \in W$.

∎

Capítulo 3

Transformações de Möbius e Matrizes de Vahlen

Neste capítulo, definiremos as transformações de Möbius em várias dimensões. Para isso, nos referimos a [**1**], [**2**] e [**22**]. Alhfors, em [**1**], observa que a maneira mais natural para tratar das transformações de Möbius em várias dimensões é através dos números de Clifford do espaço paravetorial W, vistos no capítulo 2. Definiremos as aplicações inversão e reflexão de acordo com Beardon, em [**2**], porém com o foco de Alhfors, ou seja, usando números de Clifford. Após, definiremos as transformações de Möbius como sendo composições finitas dessas duas aplicações, formando o grupo geral de Möbius. Definiremos também as matrizes de Vahlen, que são matrizes invertíveis com entradas na álgebra de Clifford $\mathcal{C}_n$ satisfazendo certas condições, as quais formam um grupo. Em seguida, faremos alguns comentários do trabalho feito por Waterman, em [**22**], que mostra uma relação intrínseca entre as matrizes de Vahlen e as transformações de Möbius. Por fim, definiremos as translações de Möbius, que são transformações de Möbius que preservam o disco unitário de W e veremos uma decomposição para o grupo das transformações de Möbius que preservam o disco unitário de W.

3.1 Transformação de Möbius

Vamos introduzir duas aplicações (inversão e reflexão), as quais caracterizam as transformações de Möbius. No que segue, consideramos o espaço paravetorial W da álgebra de Clifford $\mathcal{C}_n$. Seja ∞ um ponto tal que $\infty \notin W$. Denotamos por $\widehat{W}$ o conjunto $W \cup \{\infty\}$ e denominamos ∞ de *ponto ideal.*

Dados $a \in W$ e $r > 0$, uma *hiperesfera* de centro em a e raio r é o conjunto $S(a,r) := \{w \in W \mid \|w-a\| = r\}$.

Definição 3.1.1. A *inversão* em relação à $S(a,r)$ é a aplicação $\phi : \widehat{W} \to \widehat{W}$ definida por:

$$\phi(w) = \begin{cases} a + \frac{r^2}{\|w-a\|^2}(w-a) & , \text{ se } \ w \in W \setminus \{a\} \\ a & , \text{ se } w = \infty \\ \infty & , \text{ se } w = a \end{cases}$$

Para o caso $n = 2$, temos a seguinte interpretação geométrica da definição 3.1.1.

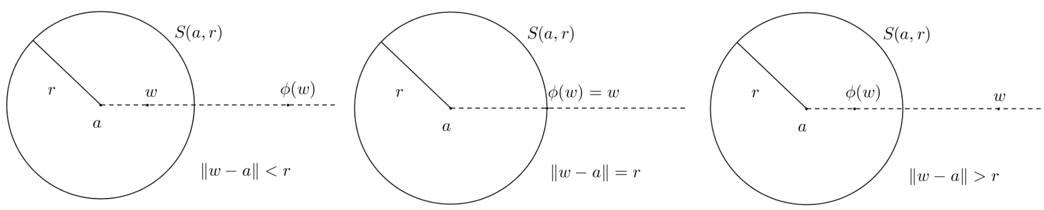

Figura 3.1.1. Inversão em relação à $S(a,r)$ para $n = 2$

De acordo com a figura acima, é fácil ver que vale a seguinte:

Proposição 3.1.2. *Se $\phi : \widehat{W} \to \widehat{W}$ é uma inversão em relação à $S(a,r)$, então são verdadeiras as seguintes afirmações:*

i) ϕ é uma involução.

ii) $\phi(w) = w$ se, e somente se, $w \in S(a,r)$.

Demonstração:

i) Claramente, $\phi^2(a) = \phi(\phi(a)) = \phi(\infty) = a$ e $\phi^2(\infty) = \phi(\phi(\infty)) = \phi(a) = \infty$ **(1)**.

Se $w \in W \setminus \{a\}$, então $\phi^2(w) = \phi(\phi(w)) = a + \frac{r^2}{\|\phi(w)-a\|^2}(\phi(w) - a)$ **(2)**.

De $\phi(w) - a = \frac{r^2}{\|w-a\|^2}(w-a)$, obtemos $\|\phi(w) - a\| = \frac{r^2}{\|w-a\|}$. Logo, subtituindo essas igualdades em (2), concluímos que:

$$\phi^2(w) = a + \frac{\|w-a\|^2}{r^2}\left(\frac{r^2}{\|w-a\|^2}(w-a)\right) = a + (w-a) = w.$$

ii) ($\Longleftarrow$) Imediato.

($\Longrightarrow$) Seja $w \in \widehat{W}$ tal que $\phi(w) = w$. Pela definição de inversão, é claro que $w \neq a$ e $w \neq \infty$. Desenvolvendo, segue que:

$$a + \frac{r^2}{\|w-a\|^2}(w-a) = w \Leftrightarrow \left(1 - \frac{r^2}{\|w-a\|^2}\right)(a-w) = 0 \Rightarrow 1 - \frac{r^2}{\|w-a\|^2} = 0.$$

Logo, $\frac{r^2}{\|w-a\|^2} = 1 \Rightarrow \|w-a\|^2 = r^2 \Rightarrow \|w-a\| = r$, isto é, $w \in S(a,r)$. ■

Sejam $a \in W\setminus\{0\}$ e $t \in \mathbb{R}$. Um *hiperplano* em $\widehat{W}$, denotado por $P(a,t)$, é o conjunto $\{w \in W \mid \langle w, a\rangle = t\} \cup \{\infty\}$. Caso $t = 0$, chamamos o hiperplano $P(a,0)$ de *hiperplano ortogonal* a a, denotado por $a^{\perp}$.

Definição 3.1.3. Uma *reflexão* em relação à $P(a,t)$ é uma aplicação $\varphi : \widehat{W} \to \widehat{W}$ tal que $\varphi(\infty) = \infty$ e $\varphi(w) = w + \lambda a$, onde $\lambda \in \mathbb{R}$ é tal que $\frac{1}{2}(w + \varphi(w)) \in P(a,t)$.

O fato do ponto médio de w e $\varphi(w)$ pertencer ao hiperplano, torna possível escrever $\varphi(w)$ exclusivamente em termos de a e t. De fato, temos que:

$$\begin{aligned}
\frac{1}{2}(\varphi(w) + w) \in P(a,t) \quad &\Leftrightarrow \quad \left\langle \frac{1}{2}(\varphi(w) + w), a \right\rangle = t \\
&\Leftrightarrow \quad 2\langle w, a\rangle + \lambda\langle a, a\rangle = 2t \\
&\overset{a\neq 0}{\Leftrightarrow} \quad \lambda = \frac{2t - 2\langle w, a\rangle}{\langle a, a\rangle} \\
&\Leftrightarrow \quad \lambda = -2\left(\frac{\langle w, a\rangle - t}{\|a\|^2}\right).
\end{aligned}$$

Logo, $\varphi(w) = w - 2\left(\frac{\langle w,a\rangle - t}{\|a\|^2}\right) a$ e $\varphi(\infty) = \infty$. Portanto, podemmos dizer que φ é a reflexão em relação à $P(a,t)$.

As figuras abaixo ilustram as definições dadas acima:

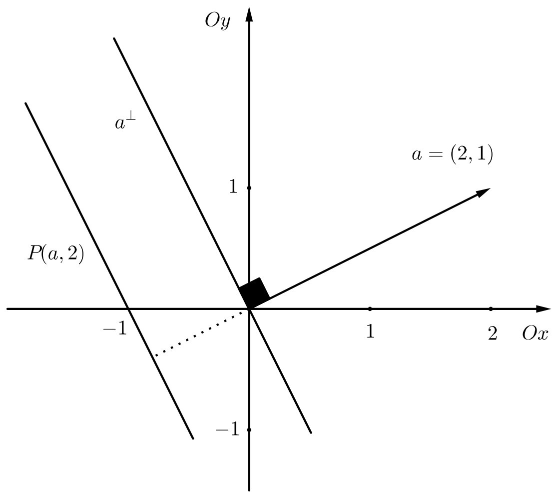

Figura 3.1.3. Para o caso $n = 2$, temos os hiperplanos $P((2,1),0)$ e $P((2,1),2)$.

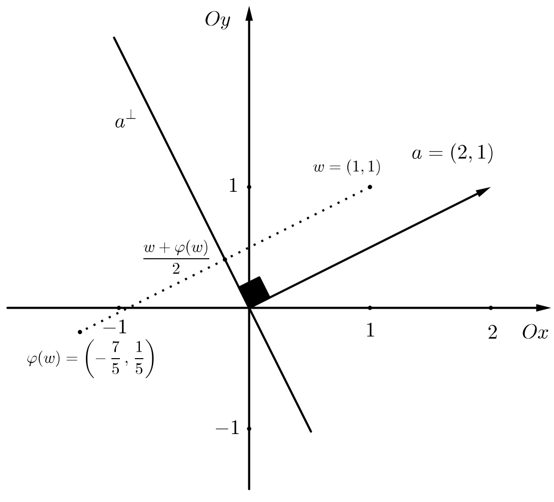

Figura 3.1.4. Reflexão de w em relação à $P((2,1),0)$.

A figura 3.1.4 motiva a seguinte:

Proposição 3.1.4. *Se $\varphi : \widehat{W} \to \widehat{W}$ é a reflexão em relação à $P(a,t)$, então são verdadeiras as seguintes afirmações:*

i) *φ é uma involução.*

ii) *$\varphi(w) = w$ se, e somente se, $w \in P(a,t)$.*

iii) *Se $t = 0$, então φ é uma reflexão.*

Demonstração:

i) Claramente, $\varphi^2(\infty) = \varphi(\varphi(\infty)) = \varphi(\infty) = \infty$ **(1)**.

Se $w \in W$, então $\varphi^2(w) = \varphi(\varphi(w)) = \varphi(w) - 2\left(\frac{\langle\varphi(w),a\rangle - t}{\|a\|^2}\right)a$. Note que, $\langle\varphi(w),a\rangle = \langle w,a\rangle - 2\left(\frac{\langle w,a\rangle - t}{\|a\|^2}\right)\underbrace{\langle a,a\rangle}_{=\|a\|^2} = \langle w,a\rangle - 2\langle w,a\rangle + 2t = 2t - \langle w,a\rangle$. Logo, $\langle\varphi(w),a\rangle - t = t - \langle w,a\rangle$ e substituindo, temos que $\varphi^2(w) = w - 2\frac{(\langle w,a\rangle - t)}{\|a\|^2}a - 2\frac{(t - \langle w,a\rangle)}{\|a\|^2}a = w$ **(2)**.

Logo, de (1) e (2), segue o desejado.

ii) $(\Longrightarrow)$ Seja $w_0 \in P(a,t)$. Se $w_o \in W$, então $\langle w_0, a\rangle = t$. Logo, $\varphi(w_0) = w_0$. Se $w_0 = \infty$, $\varphi(w_0) = \varphi(\infty) = \infty = w_0$.

$(\Longleftarrow)$ Por definição, $\varphi(\infty) = \infty$ e $\infty \in P(a,t)$. Se $w \neq \infty$, então $w - 2\frac{\langle w,a\rangle - t}{\|a\|^2}a = w \Rightarrow \frac{\langle w,a\rangle - t}{\|a\|^2}a = 0$. Como $a \neq 0$, obtemos que $\langle w,a\rangle = t$ e, portanto, $w \in P(a,t)$.

iii) Suponhamos que $\varphi : \widehat{W} \to \widehat{W}$ seja uma reflexão em relação à $P(a,0)$, isto é, $\varphi(w) = w - \frac{2\langle w,a\rangle}{\|a\|^2}a$, para todo $w \in W$. Devemos mostrar que $\varphi \in O(n,\mathbb{R})$. É fácil ver que φ é uma transformação linear que preserva o produto interno e é bijetora por i). Suponhamos que $\{1,e\}$ seja uma base de W. Assim, dado $a = x + ye \in W$, $x, y \in \mathbb{R}$, temos que $\varphi(1) = \left(1 - \frac{2x^2}{\|a\|^2}\right) - \frac{2xy}{\|a\|^2}e$ e $\varphi(e) = -\frac{2yx}{\|a\|^2} + \left(1 - \frac{2y^2}{\|a\|^2}e\right)$. Logo, o determinante de φ em relação à base $\{1,e\}$ é igual a -1. Por indução sobre a dimensão de W segue o caso geral.

■

No que segue, ϕ denota a inversão em relação à $S(a,r)$ e φ a reflexão em relação à $P(a,t)$.

Definição 3.1.5. Uma *transformação de Möbius* em $\widehat{W}$ é uma aplicação obtida pela composição de um número finito de reflexões e/ou inversões.

Proposição 3.1.6. *O conjunto* $\{f : \widehat{W} \to \widehat{W} \mid f$ *é uma transformação de Möbius*$\}$ *é um grupo com respeito a composição de funções.*

Demonstração: Claramente, o conjunto de todas as transformações de Möbius é fechada para a composição de funções. Das proposições 3.1.2 e 3.1.4 segue que a inversa de uma transformação de Möbius também goza da mesma propriedade. Por fim, as aplicações identidade, reflexão e inversão são também transformações de Möbius. ∎

Definição 3.1.7. O grupo das transformações de Möbius em $\widehat{W}$, denotado por $\mathcal{GM}(\widehat{W})$, é chamado de *grupo geral de Möbius* em $\widehat{W}$.

Exemplo 3.1.8. *As seguintes aplicações são transformações de Möbius:*

i) A aplicação $w \mapsto w + a$, $a \in W$ *está em* $\mathcal{GM}(\widehat{W})$, *pois é a composição da reflexão em* $P(a, 0)$ *com a reflexão em* $P\left(a, \frac{\|a\|^2}{2}\right)$. *Denominamos tal aplicação de translação.*

ii) A aplicação $w \mapsto kw$, $k > 0$ *está em* $\mathcal{GM}(\widehat{W})$, *pois é a composição da inversão em* $S(0, 1)$, *com a inversão em* $S(0, \sqrt{k})$. *Denominamos tal aplicação de dilatação.*

iii) Do capítulo 2, se $a \in \Gamma_n$ *é tal que* $\|a\| = 1$, *então toda rotação da forma* awa^* *é o produto de reflexões em hiperplanos ortogonais, ou seja, é uma transformação de Möbius.*

iv) A aplicação $w \mapsto w$ *é a transformação de Möbius identidade.*

v) A aplicação $w \mapsto \frac{1}{\|w\|^2} w = (\overline{w})^{-1}$ *é a inversão em relação à* $S(0, 1)$.

vi) A aplicação $w \mapsto -\overline{w}$ *é a reflexão em relação à* $P(1, 0)$.

vii) A aplicação $w \mapsto -w^{-1}$ é uma transformação de Möbius, pois é a composição das transformações de Möbius dos itens v) e vi).

3.2 Matrizes de Vahlen

Em [**1**], [**22**], temos uma generalização das propriedades existentes entre as matrizes associadas às transformações de Möbius no caso complexo $\widehat{\mathbb{C}}$. Tais matrizes são chamadas matrizes de Vahlen, que são matrizes quadradas invertíveis de ordem 2 e com entradas invertíveis ou nulas na álgebra de Clifford $\mathcal{C}_n$ sujeitas a algumas condições.

No que segue, Γ_n é o grupo de Clifford da álgebra de Clifford $\mathcal{C}_n$ e $\mathbb{M}(2, \mathcal{C}_n)$ denota o grupo das matrizes de ordem 2 com entradas em $\mathcal{C}_n$.

Definição 3.2.1. Dizemos que uma matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{M}(2, \mathcal{C}_n)$ é *de Vahlen* se satisfaz as seguintes condições:

i) $a, b, c, d \in \Gamma_n \cup \{0\}$.

ii) $ab^*,\ cd^*,\ c^*a,\ d^*b \in W$.

iii) $ad^* - bc^* = \Delta \in \mathbb{R}^*$.

Da condição iii), segue que toda matriz de Vahlen é invertível, o que é visto na seguinte:

Proposição 3.2.2. *O subconjunto das matrizes de Vahlen, munido a multiplicação usual de matrizes em $\mathbb{M}(2, \mathcal{C}_n)$ forma um grupo.*

Demonstração: Claramente, a matriz identidade é de Vahlen. Dadas duas matrizes de Vahlen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$, considere a operação multiplicação usual $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax+by & az+bw \\ cx+dy & cz+dw \end{smallmatrix}\right)$. Para mostrarmos que o subconjunto é fechado em nessa operação, consideramos primeiro a entrada $ax + by$ e analisamos quatro casos.

(Caso 1) Se $a, b, y, w \neq 0$, então $ax + by = a(xy^{-1} + a^{-1}b)y$.

Por hipótese, $y^*x, ab^* \in W$, implicando que $(y^*x)^* = x^*y \in W$ e $(ab^*)^* = ba^* = (b^*)^*a^* \in W$. Pelo item iv) de 2.2.15, segue que $xy^{-1}, b^*(a^*)^{-1} = b^*(a^{-1})^* = (a^{-1}b)^* \in W$, donde segue que $a^{-1}b \in W$. Logo, sendo W um espaço vetorial, segue que $xy^{-1} + a^{-1}b \in W$.

Se $xy^{-1} + a^{-1}b = 0$, não há o que fazer. Caso contrário, se $xy^{-1} + a^{-1}b \neq 0$, então $xy^{-1} + a^{-1}b \in W \subset \Gamma_n$. Logo, sendo Γ_n um grupo, segue que $ax + by \in \Gamma_n \cup \{0\}$.

(Caso 2) Se $a = 0$, então obtemos a matriz $\left(\begin{smallmatrix} by & bw \\ cx+dy & cz+dw \end{smallmatrix}\right)$. Claramente $by, bw \in \Gamma_n \cup \{0\}$. Repetimos o procedimento feito no caso 1 para $cx + dy$ e $cz + dw$. Analogamente, para as possibilidades: $b = 0$, $y = 0$ ou $w = 0$.

(Caso 3) Se quaisquer dois elementos dentre a, b, y, w forem nulos, então obtemos uma das seguintes matrizes: as quatro entradas são pertencem a Γ_n; duas entradas nulas e duas entradas as quais se aplicam o caso 1; uma entrada nula, duas entradas em Γ_n e uma entrada em que se aplica o caso 1; três entradas em Γ_n e uma entrada em que se aplica o caso 1.

(Caso 4) Se quaisquer três elementos dentre a, b, y, w forem nulos, então obtemos matrizes com duas entradas nulas, uma em Γ_n e a outra se aplica o caso 1, ou uma matriz com as quatro entradas em Γ_n.

Logo, seguindo o mesmo procedimento para as demais entradas, segue que, a multiplicação de matrizes de Vahlen é uma matriz de Vahlen. Agora, vamos verificar que o conjunto das matrizes de Vahlen é um grupo.

Claramente, a multiplicação é associativa. Se $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ é uma matriz de Vahlen, então $N = \left(\begin{smallmatrix} d^* & -b^* \\ -c^* & a^* \end{smallmatrix}\right)$ satisfaz a definição 3.2.1. De fato: os itens i) e ii) são claros. Se $\Delta_M = ad^* - bc^* \in \mathbb{R}^*$ e $\Delta_N = d^*a - b^*c \in \mathcal{C}_n$, então se $d \neq 0$, da relação $\Delta \|d\|^2 = d^*(ad^* - bc^*)\widehat{d} = \|d\|^2 d^*a - b^*dc^*\widehat{d} = (d^*a - b^*c)\|d\|^2$ tiramos que $\Delta_M = \Delta_N$, pois

$cd^* \in W$. Se $d = 0$, então obtemos $b \neq 0$ e $c \neq 0$, caso contrário $\Delta_M = 0$. Logo, $\Delta_M = -bc^*$, implicando que $-b = \Delta_M(c^*)^{-1}$, ou seja, $-b^*c = \Delta_M = \Delta_N$, mostrando que N satisfaz iii).

Portanto, $MN = \Delta_M I$, $NM = \Delta_N I$ e definindo $\Delta := \Delta_M = \Delta_N \in \mathbb{R}^*$, segue que $M^{-1} = \frac{1}{\Delta}N$.

■

Definição 3.2.3. O grupo das matrizes de Vahlen, denotado por $\mathcal{V}(\mathcal{C}_n)$, é chamado *grupo de Vahlen.*

Exemplo 3.2.4. *Considerando $\mathcal{C}_1 \cong \mathbb{C}$ temos que, $W = \mathbb{C}$, $\Gamma_1 = \mathbb{C}^*$ e $a^* = a \in \mathbb{C}$. Dados $a, b, c, d \in \mathbb{C}$, a matriz da forma $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfazendo $ad^* - b^*c = ad - bc \neq 0$ é uma matriz de Vahlen. Logo, $\mathcal{V}(\mathbb{C}) = GL(2, \mathbb{C}) = \{M \in \mathbb{M}(2, \mathbb{C}) \mid \det M \neq 0\}$.*

Consideremos o conjunto das matrizes da forma $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, onde $a, b, c, d \in \mathcal{C}_n$, tais que a matriz M induz uma bijeção em $\widehat{W}$ definida por $(aw+b)(cw+d)^{-1}$. Claramente, a matriz identidade induz uma bijeção em $\widehat{W}$, pois $w = (1w + 0)(0w + 1)^{-1}$.

Note que, se a matriz M em questão é de Vahlen, então a aplicação induzida por esta matriz é uma transformação de Möbius. De fato: temos que $cd^* = (c^*)^*d^* \in W \Leftrightarrow c^*(d^*)^{-1} = (d^{-1}c)^* \in W \Rightarrow \{[(d^{-1}c)^*]^*\}^{-1} = c^{-1}d \in W$. E de $c^*a = c^*(a^{-1})^{-1} \in W \Leftrightarrow ca^{-1} \in W \Rightarrow (ca^{-1})^{-1} = ac^{-1} \in W$.

Considere as transformações de Möbius

$$f_1(w) = w + c^{-1}d \text{ (translação)}, \quad f_2(w) = -w^{-1}, \quad f_3(w) = \frac{\widehat{c}}{\|c\|}w(\frac{\widehat{c}}{\|c\|})^* \text{ (rotação)}$$

$$f_4(w) = \frac{|\Delta|}{\|c\|^2}w \text{ (dilatação)}, \quad f_5(w) = \frac{\Delta}{|\Delta|}w, \quad f_6(w) = ac^{-1} + w \text{ (translação)}.$$

Dado $w \in \widehat{W}$ temos que $(f_6 \circ f_5 \circ \ldots \circ f_1)(w)$ é igual a

$$ac^{-1} + \frac{\Delta}{|\Delta|}\left\{\frac{|\Delta|}{\|c\|^2}\left[\frac{\widehat{c}}{\|c\|}(-(w + c^{-1}d)^{-1})\right]\left(\frac{\widehat{c}}{\|c\|}\right)^*\right\} = ac^{-1} - \Delta(c^*)^{-1}(w + c^{-1}d)^{-1}c^{-1}.$$

Mas $(aw+b)(cw+d)^{-1} = [ac^{-1}(cw+d)+b-ac^{-1}d](cw+d)^{-1} = ac^{-1}+(b-ac^{-1}d)(cw+d)^{-1}$ e sendo $\Delta = ad^* - bc^* \Rightarrow b = -\Delta(c^*)^{-1} + ad^*(c^*)^{-1} = -\Delta(c^*)^{-1} + a(c^{-1}d)^*$. Como $c^{-1}d \in W \Rightarrow (c^{-1}d)^* = c^{-1}d$. Logo, $(aw+b)(cw+d)^{-1}ac^{-1} - \Delta)(c^*)^{-1}(w+c^{-1}d)^{-1}c^{-1}$.

A recíproca se encontra em **[22]**, ou seja, supondo a existência de uma bijeção em $\widehat{W}$, prova-se que a matriz é de Vahlen.

O que foi mencionado acima pode ser encontrado em **[1]** e **[22]**, e é enunciado no seguinte:

Teorema 3.2.5. *Dada uma matriz* $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{M}(2, \mathcal{C}_n)$*, são verdadeiras as seguintes afirmações:*

i) *$M \in \mathcal{V}(\mathcal{C}_n)$ é uma matriz de Vahlen se, e somente se, a aplicação $f : \widehat{W} \to \widehat{W}$ definida por $f(w) = (aw+b)(cw+d)^{-1}$ é uma transformação de Möbius.*

ii) *A multiplicação de matrizes de Vahlen induz a composição de transformações de Möbius.*

iii) *O núcleo da aplicação $\mathcal{V}(\mathcal{C}_n) \mapsto \mathcal{GM}(\widehat{W})$ definida por $M \mapsto f_M(w) = (aw+b)(cw+d)^{-1}$ é o conjunto $\{\lambda I \mid \lambda \in \mathbb{R}^*\}$, onde I denota a matriz identidade.*

iv) *Matrizes de Vahlen múltiplas por um número real não-nulo, induzem a mesma transformação de Möbius.*

Demonstração: Para os ítens ii), iii) e iv) ver [**22**], pg. 91. ∎

Exemplo 3.2.6. *De acordo com* 3.2.4*, a aplicação $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ definida por $f(z) = \frac{az+b}{cz+d}$ é uma transformação de Möbius desde que $ad - bc \neq 0$, onde $a, b, c, d \in \mathbb{C}$.*

Exemplo 3.2.7. *As seguintes matrizes são de Vahlen e induzem as respectivas transformações de Möbius:*

i) $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ *induz a aplicação* $\mathrm{id}(w) = w = (1w+0)(0w+1)^{-1}$, *denominada identidade.*

ii) $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ *induz uma translação* $w + a = (1w+a)(0w+1)^{-1}$.

iii) $\left(\begin{smallmatrix} \sqrt{k} & a \\ 0 & \frac{1}{\sqrt{k}} \end{smallmatrix}\right)$ *induz a dilatação* $kw = (\sqrt{k}w + 0)\left(\frac{1}{\sqrt{k}}w + 0\right)^{-1}$, *onde* $k > 0$.

iv) Se $a \in \Gamma_n$ *é tal que* $\|a\| = 1$, *então* $\left(\begin{smallmatrix} a & 1 \\ 0 & \widehat{a} \end{smallmatrix}\right)$ *induz a rotação* $awa^* = (aw+0)(\widehat{a}w+1)^{-1}$.

v) $\left(\begin{smallmatrix} 1 & a \\ \widehat{a} & 1 \end{smallmatrix}\right)$ *induz a transformação de Möbius* $(1w+a)(\widehat{a}w+1)^{-1}$.

Denotando o disco unitário do espaço paravetorial W por B_n, ou seja, $B_n := \{w \in W \,|\, \|w\| < 1\}$, segue que se $a \in B_n$ e $f : \widehat{W} \to \widehat{W}$ é a transformação de Möbius do item v) do exemplo 3.2.7, então $f(B_n) = B_n$. Com efeito: se $w \in B_n$, então

$$\begin{aligned} \|f(w)\|^2 &= f(w)\overline{f(w)} = (w+a)[(1+\overline{w}a^*)(1+\widehat{a}w)]^{-1}(\overline{w}+\overline{a}) \\ &= \frac{\|w\|^2 + 2\langle a, w\rangle + \|a\|^2}{1 + 2\langle a, w\rangle + \|a\|^2\|w\|^2}. \end{aligned}$$

Fazendo $\|w\|^2 = x < 1$ e $\|a\|^2 = y < 1$ e $2\langle a, w\rangle = z$ e supondo, por absurdo, que $x + z + y \geq 1 + z + xy \Leftrightarrow xy - x - y + 1 \leq 0 \Leftrightarrow (x-1)(y-1) \leq 0$, implicando que $x \leq 1$ e $y \geq 1$, ou $x \geq 1$ e $y \leq 1$. Logo, $\|f(w)\|^2 < 1$, implicando que $\|f(w)\| < 1$.

Definição 3.2.8. Seja $a \in B_n$. A *translação de Möbius* induzida por a, denotada por τ_a, é a transformação de Möbius $\tau_a : \widehat{W} \to \widehat{W}$ dada por $\tau_a(w) = (w+a)(1+\widehat{a}w)^{-1}$. O conjunto de todas as translações de Möbius é denotado por $\mathcal{T}_{\mathcal{M}}$.

Se $G(B_n)$ denota o conjunto das transformações de Möbius que preservam o disco unitário do espaço paravetorial W, então $G(B_n)$ é um grupo com a operação composição. Claramente, $\mathrm{id}_W \in G(B_n)$. Se $f, g \in G(B_n)$, então $f(g(B_n)) = f(B_n) = B_n$ e $f(w) = w' \Leftrightarrow f^{-1}(w') = w$, mostrando que $f \circ g, f^{-1} \in G(B_n)$.

Lema 3.2.9. *Se* f *é uma transformação de Möbius do espaço paravetorial* W *tal que* $f(B_n) = B_n$ *e* $f(0) = 0$, *então* f *é uma transformação ortogonal.*

Demonstração: Ver [**2**], pg. 38. ∎

De acordo com o teorema 3.2.5, como a composição de transformações de Möbius induz a multiplicação de matrizes de Vahlen, concluímos que $\tau_a^{-1} = \tau_{-a}$, pois $\begin{pmatrix} 1 & a \\ \hat{a} & 1 \end{pmatrix}\begin{pmatrix} 1 & -a \\ -\hat{a} & 1 \end{pmatrix} = (1 + \|a\|^2)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, a qual induz a transformação de Möbius identidade, sendo $a \in B_n$.

Proposição 3.2.10. *Dado $f \in G(B_n)$, existem $\tau_a \in \mathcal{T}_{\mathcal{M}}$ e $\theta \in O(n, \mathbb{R})$ tais que $f = \tau_a \circ \theta$.*

Demonstração: Seja f uma tranformação de Möbius tal que $f(B_n) = B_n$ e defina $a = f(0) \in B_n$. Assim, $\tau_{-a} \circ f$ é uma transformação de Möbius que preserva B_n e leva 0 em 0. Logo, pelo lema 3.2.9, temos que $\tau_{-a} \circ f$ é uma transformação ortogonal. Sendo $f = \tau_a \circ (\tau_{-a} \circ f) = \tau_a \circ \theta$, segue que $G(B_n) = \mathcal{T}_{\mathcal{M}} \circ O(n, \mathbb{R})$, uma vez que se $\theta \in O(n, \mathbb{R})$, então θ é produto de no máximo $(n + 1)$-reflexões e satisfaz $\|\theta(w)\| = \|w\| < 1$, para todo $w \in B_n$. ∎

Capítulo 4

Teoria dos Laços

Neste capítulo, estudaremos alguns tópicos da Teoria dos Laços, tais como: B-laços, subgrupo torcido, grupo involutivo, transversal e aplicação precessão. Os dois principais exemplos tratados aqui são os laços obtidos via seção e o laço de Möbius.

4.1 B-laços

Daremos uma breve introdução dos conceitos básicos da teoria dos laços. Para um aprofundamento melhor, indicamos **[10]**. Daremos exemplos dos conceitos apresentados, sempre que necessário.

Definição 4.1.1. Seja $\mathcal{L}$ um conjunto não-vazio, munido de uma operação binária $\cdot : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$ e suponha que $\mathcal{L}$ tenha um único elemento neutro, denotado por $1_{\mathcal{L}}$. O par $(\mathcal{L}, \cdot)$ é chamado de:

i) laço à esquerda se dados $a, b \in \mathcal{L}$, existir um único $x \in \mathcal{L}$ que satisfaz $a \cdot x = b$.

ii) laço à direita se dados $a, b \in \mathcal{L}$, existir um único $y \in \mathcal{L}$ que satisfaz $y \cdot a = b$.

Nessas condições, $(\mathcal{L}, \cdot)$ é um *laço* se satisfaz i) e ii).

Observação 4.1.2. *Quando não houver confusão, denotaremos um laço* $(\mathcal{L}, \cdot)$ *simplesmente por* $\mathcal{L}$ *e um produto* $a \cdot b \in \mathcal{L}$ *simplesmente por* ab.

Exemplo 4.1.3. *Todo grupo é um laço.*

No final dessa seção mostraremos um outro exemplo de laço à esquerda. Veja que, $(\mathbb{Z}, -)$ e $(\mathbb{Z}_4, \cdot)$ não são laços, pois o primeiro não possui elemento neutro, já no segundo, a equação $\overline{2} \cdot x = \overline{1}$ não possui solução, sendo $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Seja $\mathcal{L}$ um laço. Um elemento $a \in \mathcal{L}$ é dito ser:

i) *invertível à esquerda* se existir $b \in \mathcal{L}$ tal que $ba = 1_{\mathcal{L}}$. Neste caso, dizemos que b é um *inverso à esquerda* de $a \in \mathcal{L}$.

ii) *invertível à direita* se existir $c \in \mathcal{L}$ tal que $ac = 1_{\mathcal{L}}$. Neste caso, dizemos que c é um *inverso à direita* de $a \in \mathcal{L}$.

Observação 4.1.4. *Todo elemento de um laço possui único inverso à esquerda e único inverso à direita, devido as condições da definição* 4.1.1.

Definição 4.1.5. Seja $\mathcal{L}$ um laço. Um elemento $a \in \mathcal{L}$ é *invertível* se existir $a' \in \mathcal{L}$ satisfazendo os itens i) e ii) acima. Nesse caso, dizemos que a' é um *inverso* de $a \in \mathcal{L}$.

Observação 4.1.6. *Se $a \in \mathcal{L}$ é invertível, então seu inverso é único. Com efeito: se $a' \in \mathcal{L}$ é um inverso de a, então $aa' = a'a = 1$. Sendo $\mathcal{L}$ um laço, temos que as equações $ax = 1$ e $ya = 1$ possuem solução única. Logo, $x = a' = y$, permitindo usar a notação a^{-1} para o inverso de a.*

Definição 4.1.7. Um laço $\mathcal{L}$ é chamado de:

i) *Bol-laço à esquerda* se satisfaz $a(b(ac)) = (a(ba))c$, $\forall a, b, c \in \mathcal{L}$.

ii) *K-laço* (ou *Bruck-laço*) se for um Bol-laço à esquerda, todo elemento em $\mathcal{L}$ é invertível e $(ab)^{-1} = a^{-1}b^{-1}$, $\forall a, b \in \mathcal{L}$.

Mais ainda, um K-laço possui a *propriedade da raiz quadrada* se para todo $a \in \mathcal{L}$, existir $b \in \mathcal{L}$ tal que $b^2 = a$. Neste caso, se $b \in \mathcal{L}$ for único, dizemos que $\mathcal{L}$ possui a *propriedade da raiz quadrada única* e denotamos b por $a^{\frac{1}{2}}$.

Definição 4.1.8. Um *B-laço* é um K-laço com a propriedade da raiz quadrada única.

Exemplo 4.1.9. *Todo grupo comutativo é um K-laço. Em particular,* $\mathbb{R}_+^*$ *com a multiplicação usual de números reais é um B-laço.*

Observação 4.1.10. *A propriedade da raiz quadrada única pode ser aplicada para qualquer conjunto não-vazio munido de uma operação binária.*

Com o objetivo de apresentar um exemplo de laço à esquerda, enunciamos a seguinte:

Definição 4.1.11. Sejam $(G, \cdot)$ um grupo, $H \subset G$ um subgrupo, G/H conjunto das classes laterais à esquerda de H em G e $\pi : G \to G/H$ a projeção canônica. Uma *seção* da projeção canônica é uma aplicação $\sigma : G/H \to G$ tal que $\pi \circ \sigma = \mathrm{id}_{G/H}$ e $\sigma(H) = 1_G$.

Veremos mais adiante que sempre existe seção. O seguinte exemplo ilustra a definição acima.

Exemplo 4.1.12. *Considere o grupo* $G = S_3 = \{\mathrm{id} = \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \alpha_1 = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \alpha_2 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \alpha_3 = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \alpha_4 = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \alpha_5 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)\}$ *e tome* $H = \{\mathrm{id}, \alpha_5\} \subset G$*. Claramente,* H *é um subgrupo, mas não é subgrupo normal de* G*. Temos que* $G/H = \{H, \alpha_1 \circ H, \alpha_2 \circ H\}$*, pois* $H = \alpha_5 \circ H$*,* $\alpha_1 \circ H = \alpha_3 \circ H$ *e* $\alpha_2 \circ H = \alpha_4 \circ H$*. Logo, definindo a aplicação* $\sigma : G/H \to G$ *por* $\sigma(H) = \mathrm{id}$ *e* $\sigma(\alpha_i \circ H) = \alpha_i$*, para* $i = 1, 2$*, segue que* σ *é uma seção de* $\pi : G \to G/H$*.*

Vamos introduzir uma operação em G/H, via seção, de tal forma que G/H adquira uma estrutura de laço à esquerda. Para isso, sejam G um grupo multiplicativo, $H \subset G$ um subgrupo que não é normal e suponhamos que $\sigma : G/H \to G$ seja uma seção da projeção canônica. Considere a operação $\oplus_\sigma : G/H \times G/H \to G/H$ definida por:

$$aH \oplus_\sigma bH := \sigma(aH)\sigma(bH)H.$$

A operação $\oplus_\sigma$ é bem definida, pois se $aH, bH, cH, dH \in G/H$ são tais que $aH = cH$ e $bH = dH$, então $\sigma(aH) = \sigma(cH)$ e $\sigma(bH) = \sigma(dH)$. Logo, $\sigma(aH)\sigma(bH) = \sigma(cH)\sigma(dH) \Rightarrow \sigma(aH)\sigma(bH)H = \sigma(cH)\sigma(dH)H$, mostrando que $aH \oplus_\sigma bH = cH \oplus_\sigma dH$.

Como $\sigma(aH)H = \pi(\sigma(aH)) = \underbrace{(\pi \circ \sigma)}_{=\text{id}}(aH) = aH$, segue que $\sigma(aH) = ah$, para algum $h \in H$. Logo, podemos escrever $aH \oplus_\sigma bH = \sigma(aH)bH$.

Para cada $aH \in G/H$ temos que, $H \oplus_\sigma (aH) = (aH) \oplus_\sigma H = aH$, mostrando que H é o elemento neutro de $(G/H, \oplus_\sigma)$.

Agora, dada a equação $aH \oplus_\sigma xH = bH$, temos que $\sigma(aH)xH = bH$. Segue que $xH = \sigma(aH)^{-1}bH$. Caso $yH \in G/H$ seja outra solução da equação, multiplicando a igualdade $aH \oplus_\sigma xH = aH \oplus_\sigma yH$ por $\sigma(aH)^{-1}$, obtemos que $yH = xH$. Logo, denotamos por $\ominus_\sigma aH$ o elemento $\sigma(aH)^{-1}H$. Podemos resumir o que foi feito no seguinte:

Lema 4.1.13. *Se G é um grupo, $H \subset G$ é um subgrupo e $\sigma : G/H \to G$ é uma seção de $\pi : G \to G/H$ então a operação binária $\oplus_\sigma : G/H \times G/H \to G/H$ definida por $(aH) \oplus_\sigma (bH) := \sigma(aH)bH$ é tal que $(G/H, \oplus_\sigma)$ é um laço à esquerda.*

Demonstração: Segue das considerações acima. ■

Observação 4.1.14. *Se H é subgrupo normal, então a operação $\oplus_\sigma$ coincide com a operação do grupo quociente G/H, isto é, a operação $\oplus_\sigma$ independe da seção, pois $\sigma(aH)\sigma(bH)H = ah_1bh_2H = ab(b^{-1}h_1b)h_2H = abH$, para certos $h_1, h_2 \in H$.*

4.2 Subgrupo torcido

Nesta seção, veremos uma condição suficiente para termos um laço à esquerda. Após, definiremos subgrupo torcido, donde segue um resultado o qual afirma que é possível tornar um subgrupo torcido um B-laço, desde que este possua a propriedade da raiz quadrada única.

O seguinte lema fornece uma condição suficiente para que tenhamos um laço à esquerda.

Lema 4.2.1. *Seja $\mathcal{L}$ um conjunto não-vazio, munido de uma operação binária $\cdot$ e com elemento neutro $1_{\mathcal{L}}$. Se para todo $a \in \mathcal{L}$, existe $a' \in \mathcal{L}$ tal que $a' \cdot (a \cdot b) = b$, para cada $b \in \mathcal{L}$, então $(\mathcal{L}, \cdot)$ é um laço à esquerda.*

Demonstração: Primeiramente, mostremos que todo elemento de $\mathcal{L}$ é invertível.

Dado $a \in \mathcal{L}$, por hipótese, existe $a' \in \mathcal{L}$ tal que $a' \cdot (a \cdot b) = b$, $\forall b \in \mathcal{L}$. Em particular, tomando $b = 1_{\mathcal{L}}$, segue que $a' \cdot a = 1_{\mathcal{L}}$. Ainda, tome $b = a'$, donde segue que $a' \cdot (a \cdot a') = a'$.

Aplicando a hipótese para $a' \in \mathcal{L}$, existe $a'' \in \mathcal{L}$ tal que $a'' \cdot (a' \cdot c) = c$, $\forall c \in \mathcal{L}$. Em particular, para $c = a \cdot a'$, segue que $a'' \cdot (a' \cdot (a \cdot a')) = a \cdot a'$. Mas $a' \cdot (a \cdot a') = a'$ e então, $a'' \cdot a' = a \cdot a'$. Tomando $c = 1_{\mathcal{L}}$, segue que $a'' \cdot a' = 1_{\mathcal{L}}$, implicando que $a \cdot a' = 1_{\mathcal{L}}$.

Por fim, se a_0 é outro inverso de a, então $a' = a' \cdot 1_{\mathcal{L}} = a' \cdot (a \cdot a_0) \stackrel{b=a_0}{=} a_0$.

Agora, mostremos que $(\mathcal{L}, \cdot)$ é um laço à esquerda. Como $a' = a^{-1}$, segue que, para todos $a, b \in \mathcal{L}$, vale a identidade $a^{-1} \cdot (a \cdot b) = b$. Logo, a equação $a \cdot x = b$ possui solução única, a saber $x = a^{-1} \cdot b$

■

Definição 4.2.2. Seja $(G, \cdot)$ um grupo com elemento neutro 1_G. Um subconjunto não-vazio $X \subset G$ é um *subgrupo torcido* se $1_G \in X$ e para todos $x, y \in X$, implicar que $x^{-1},\ x \cdot y \cdot x \in X$.

Exemplo 4.2.3. *Se G é um grupo e $H \subset G$ um subgrupo, então H é um subgrupo torcido de G.*

Observação 4.2.4. *Nem todo subgrupo torcido é um subgrupo. De fato: considere* $(G, \cdot)$ *um grupo não-abeliano e fixe um automorfismo não-trivial* $f : G \to G$*. Defina* $K(f) := \{g \in G \mid f(g) = g^{-1}\}$*. Claramente,* $K(f)$ *é um subgrupo torcido que não é um subgrupo de* G*, pois se* $x, y \in K(f)$ *e* $x \cdot y \neq y \cdot x$ *então* $f(x \cdot y) = f(x) \cdot f(y) = x^{-1} \cdot y^{-1}$ *e* $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$*, ou seja,* $x \cdot y \notin K(f)$*.*

Teorema 4.2.5. *Seja* $(G, \cdot)$ *um grupo e* $X \subset G$ *um subgrupo torcido com a propriedade da raiz quadrada única. Se* X *for munido da operação binária* $\odot : X \times X \to X$ *definida por* $a \odot b = a^{\frac{1}{2}} \cdot b \cdot a^{\frac{1}{2}}$*, então* $a \odot a = a \cdot a$*,* $\forall a \in X$ *e* $(X, \odot)$ *é um B-laço.*

Demonstração: Note que, se $a \in X$, então $(a^{\frac{1}{2}})^{-1} = (a^{-1})^{\frac{1}{2}}$. Com efeito: se $x = (a^{-1})^{\frac{1}{2}}$, então $x^2 = a^{-1} \Leftrightarrow (x^2)^{-1} = a \Leftrightarrow (x^{-1})^2 = a \Leftrightarrow x^{-1} = a^{\frac{1}{2}} \Leftrightarrow x = (a^{\frac{1}{2}})^{-1}$. Logo, podemos denotar $a^{-\frac{1}{2}}$ por $(a^{\frac{1}{2}})^{-1} = (a^{-1})^{\frac{1}{2}} \in X$.

Temos que $a \odot a$ em X, coincide com $a \cdot a$ em G. Como $(a \cdot a^{\frac{1}{2}} \cdot a^{-1})^2 = a$, segue que $a \cdot a^{\frac{1}{2}} = a^{\frac{1}{2}} \cdot a$. Assim, temos que $a \odot a = a^{\frac{1}{2}} \cdot a \cdot a^{\frac{1}{2}} = a \cdot a^{\frac{1}{2}} \cdot a^{\frac{1}{2}} = a \cdot a$. Logo, segue que $(X, \odot)$ possui a propriedade da raiz quadrada única, restando mostrar que é um K-laço.

Como X é um subgrupo torcido, para cada $a \in X$, temos que $1_G, a^{-1} \in X$. Note que, $1_G \odot a = a \odot 1_G = a$ e $a^{-1} \odot a = a \odot a^{-1} = 1_G$. Dados $a, b \in X \subset G$ é imediato que $a^{-1} \odot (a \odot b) = b$. Pelo lema 4.2.1, segue que $(X, \odot)$ é um laço à esquerda.

Agora, mostrando que $a \odot (b \odot (a \odot c)) = (a \odot (b \odot a)) \odot c$, $\forall a, b, c \in X$ **(1)**, segue que $(X, \odot)$ é um laço à direita, implicando que $(X, \odot)$ é um Bol-laço. Se $a, b \in X$, então defina $u := a^{\frac{1}{2}} \cdot b^{\frac{1}{2}} \cdot a^{\frac{1}{2}} \in X$. Para todo $c \in X$, temos que $a \odot (b \odot (a \odot c)) = a^{\frac{1}{2}} \cdot b^{\frac{1}{2}} \cdot a^{\frac{1}{2}} \cdot c \cdot a^{\frac{1}{2}} \cdot b^{\frac{1}{2}} \cdot a^{\frac{1}{2}} = u \cdot c \cdot u = (u^2)^{\frac{1}{2}} \cdot c \cdot (u^2)^{\frac{1}{2}} = u^2 \odot c$. Tomando $c = 1_G$, obtemos que $a \odot (b \odot a) = u^2$, implicando em (1).

Se $y = a^{-1} \odot ((a \odot b) \odot a^{-1}) \in X$, então $y \odot a = (a^{-1} \odot ((a \odot b) \odot a^{-1})) \odot a \overset{(1)}{=} a^{-1} \odot ((a \odot b) \odot \underbrace{(a^{-1} \odot a)}_{=1_G}) = a^{-1} \odot (a \odot b) = b$. Logo, a equação $y \odot a = b$ possui solução. Se $y_0 \in X$ é outra solução, então:

$$\begin{aligned} a \odot y_0 &= a \odot (y_0 \odot (a \odot a^{-1})) \overset{(1)}{=} (a \odot (y_0 \odot a)) \odot a^{-1} \\ &= (a \odot (y \odot a)) \odot a^{-1} \overset{(1)}{=} a \odot (y \odot (a \odot a^{-1})) = a \odot y. \end{aligned}$$

Sendo $(X, \odot)$ um laço à esquerda, concluímos que $y_0 = y$. Logo, $(X, \odot)$ é um laço e por (1), é também um Bol-laço. Por fim, veja que $(a^{-1} \odot b^{-1}) = a^{-\frac{1}{2}} \cdot b^{-1} \cdot a^{-\frac{1}{2}} = (a^{\frac{1}{2}} \cdot b \cdot a^{\frac{1}{2}})^{-1} = (a \odot b)^{-1}$, ou seja, X é um K-laço, encerrando a nossa demonstração.

∎

Corolário 4.2.6. *Um subgrupo torcido X de um grupo $(G, \cdot)$, com a propriedade da raiz quadrada única, é um B-laço com respeito a operação $a \diamond b := (a \cdot b^2 \cdot a)^{\frac{1}{2}}$.*

Demonstração: A operação $\diamond : X \times X \to X$ está bem definida, pois sendo X um subgrupo torcido, para cada $a, b \in X$, temos que $b^2 = b \cdot 1_G \cdot b \in X$ e $a \cdot b^2 \cdot a \in X$. Como X possui a propriedade da raiz quadrada única temos que $a \diamond b \in X$.

Definamos a aplicação $f : (X, \diamond) \to (X, \odot)$ por $f(x) = x \odot x$ e afirmamos que f é um isomorfismo. Pela hipótese, podemos escrever $x = f(x)^{\frac{1}{2}}$. Assim, dados $x, y \in X$, temos que:

i) se $f(x) = f(y)$, então $x = f(x)^{\frac{1}{2}} = f(y)^{\frac{1}{2}} = y$, ou seja, f é injetora.

ii) $x = (x^{\frac{1}{2}})^2 = f(x^{\frac{1}{2}})$, isto é, f é sobrejetora.

iii) $f(x \diamond y) = f((x \cdot y^2 \cdot x)^{\frac{1}{2}}) = x \cdot y^2 \cdot x = (x^2)^{\frac{1}{2}} \cdot y^2 \cdot (x^2)^{\frac{1}{2}} = x^2 \odot y^2 = f(x) \odot f(y)$.

Portanto, as propriedades de $(X, \odot)$ são transferidas para $(X, \diamond)$ via o isomorfismo f, ou seja, $(X, \diamond)$ é um B-laço.

∎

4.3 Grupos involutivos

Nesta seção, definimos grupo involutivo, ou seja, um grupo munido de uma involução, que também é um automorfismo. A partir desse conceito definiremos mais três conjuntos e estudamos suas propriedades. Introduziremos a noção de transversal e aplicação polar e veremos uma proposição que relaciona grupo involutivo, transversal, aplicação polar e subgrupo torcido. Encerraremos vendo que a noção de transversal é equivalente a noção de seção da projeção canônica.

O par (G, τ) é denominado um *grupo involutivo* se G é um grupo e τ é uma involução e um automorfismo.

Observação 4.3.1. *Se (G, τ) é um grupo involutivo, então $g^\bullet := [\tau(g)]^{-1} = \tau(g^{-1})$, para todo $g \in G$.*

Proposição 4.3.2. *Se (G, τ) é um grupo involutivo, então a aplicação $g \mapsto g^\bullet$ é uma involução e um anti-automorfismo.*

Demonstração: Imediato. ■

Agora, fixado um grupo involutivo (G, τ), consideremos os seguintes conjuntos:

$$G^\tau := \{g \in G \mid \tau(g) = g\} = \{g \in G \mid g^\bullet = g^{-1}\},$$

$$P_G := \{g \cdot g^\bullet \mid g \in G\} \text{ e } G_\tau := \{g \in G \mid g^\bullet = g\}.$$

Temos que $P_G \subset G_\tau$, pois se $x \in P_G$, então $x = g \cdot g^\bullet$, para algum $g \in G$. Pela proposição 4.3.2, segue que $x^\bullet = (g \cdot g^\bullet)^\bullet = (g^\bullet)^\bullet \cdot g^\bullet = g \cdot g^\bullet = x$. Mais ainda, G^τ é um subgrupo de G e $G^\tau \cap G_\tau = \{g \in G \mid g^2 = 1_G\}$.

Lema 4.3.3. *Se (G, τ) é um grupo involutivo, então P_G é um subgrupo torcido tal que a aplicação $T : G \times P_G \to P_G$ definida por $T(g, h) := g \cdot h \cdot g^\bullet$, é uma ação de G em P_G. Mais ainda, se para cada $g \in G$ definirmos $T_g(h) := T(g, h)$, então $T_g(P_G) \subset P_G$.*

Demonstração: Claramente, $1_G \in P_G$, pois $1_G^\bullet = 1_G$. Dados $g, h \in P_G$, existem $x, y \in G$ tais que $g = x \cdot x^\bullet$, $h = y \cdot y^\bullet$. Logo, temos que:

$$g^{-1} = (x^{-1})^\bullet \cdot [(x^{-1})^\bullet]^\bullet \in P_G \text{ e } g \cdot h \cdot g = (x \cdot x^\bullet \cdot y) \cdot (x \cdot x^\bullet \cdot y)^\bullet \in P_G.$$

Mostrando que P_G é um subgrupo torcido.

Temos que, a aplicação $T : G \times P_G \to G$ definida por $T(g, h) = g \cdot h \cdot g^\bullet$ é uma ação de G em P_G. De fato: se $h = x \cdot x^\bullet \in P_G$, com $x \in G$, então $g \cdot h \cdot g^\bullet = g \cdot x \cdot x^\bullet \cdot g^\bullet = (g \cdot x) \cdot (g \cdot x)^\bullet \in P_G$. Logo, $T : G \times P_G \to P_G$. Dados $g_1, g_2 \in G$ e $h \in P_G$, temos que $T(1_G, h) = h$ e $T(g_1, T(g_2, h)) = g_1 \cdot T(g_2, h) \cdot g_1^\bullet = g_1 \cdot (g_2 \cdot h \cdot g_2^\bullet) \cdot g_1^\bullet = (g_1 \cdot g_2) \cdot h \cdot (g_1 \cdot g_2)^\bullet = T(g_1 \cdot g_2, h)$.

Para cada $g \in G$ fixado, fazendo $T_g(h) := T(g, h)$, segue que $T_g(P_G) \subset P_G$. Logo, P_G é um subgrupo torcido invariante pelas aplicações $T_g : P_G \to P_G$, sendo $T_g(h) = T(g, h)$. Em particular, o subgrupo $G^\tau \subset G$ satisfaz $g^\bullet = g^{-1}$, $\forall g \in G^\tau$. E de forma análoga, obtemos o mesmo para a aplicação $T : G^\tau \times P_G \to P_G$ dada por $T_g(h) = g \cdot h \cdot g^{-1}$.

■

Definição 4.3.4. Sejam $(G, \cdot)$ um grupo, $H \subset G$ um subgrupo. Um subconjunto $L \subset G$ é uma *transversal* de G/H se $1_G \in L$ e $\sharp(L \cap g \cdot H) = 1$, para cada $g \in G$.

Observação 4.3.5. *Pelo axioma da escolha, existe transversal. De fato, seja G um grupo e $H \subset G$ um subgrupo. Defina a seguinte relação de equivalência em G: dados $x, y \in G$, $x \equiv y \pmod H$ se, e somente se, $x - y \in H$. Daí segue que G/H é uma partição de G. Logo, pelo axioma da escolha, tome $1_G \in H$ e, para cada $g \in G$, um único $x_g \in gH$, onde $gH \neq H$. Portanto, $L = \{1_G\} \cup \{x_g \mid g \in G\}$ é uma transversal de G/H.*

Exemplo 4.3.6. *De acordo com as notações do exemplo* 4.1.12*, se $G = S_3$, $H = \{\mathrm{id}, \alpha_5\}$ e $L = \{\mathrm{id}, \alpha_1, \alpha_2\}$, então L é uma transversal de H, pois* $\mathrm{id} \in L$ *e $\sharp(L \cap \alpha_i \circ H) = 1$, para $i = 0, 1, 2$, onde $\alpha_0 :=$* id.

Apresentamos uma equivalência da definição 4.3.4, dada acima.

Proposição 4.3.7. *Seja H um subgrupo do grupo $(G, \cdot)$ e $1_G \in L \subset G$. Então, L é uma transversal de G/H se, e somente se, a aplicação $f : L \times H \to G$ definida por $f(\ell, g) = \ell \cdot h$, é bijetora.*

Demonstração: ($\Longrightarrow$) Se $\sharp(L \cap g \cdot H) = 1$, então para cada $g \in G$, existe $h_g \in H$ tal que $g \cdot h_g \in L$. Como $H \subset G$ é subgrupo, para cada $g \in G$, temos que $g = (g \cdot h_g) \cdot h_g^{-1} = f(g \cdot h_g, h_g)$, mostrando que f é sobrejetora. Note que, se $\ell \in L$, então $L \cap \ell \cdot H = \{\ell\}$. Assim, se $\ell, \ell' \in L$ e $h, h' \in H$ são tais que $f(\ell, h) = f(\ell', h')$, então $\ell = \ell' \cdot (h' \cdot h^{-1})$. Logo, segue que $\{\ell\} = L \cap \ell \cdot H \ni \ell = \ell' \cdot (h' \cdot h^{-1}) \in L \cap \ell' \cdot H = \{\ell'\}$, ou seja $\ell = \ell'$ e $h = h'$, mostrando que f é injetora.

($\Longleftarrow$) Reciprocamente, suponhamos que f seja bijetora. Da sobrejetividade temos que, para cada $g \in G$, existem $\ell \in L$ e $h \in H$ tais que $f(\ell, h) = g$, isto é, $\ell \cdot h = g$, implicando que $\ell = g \cdot h^{-1}$. Assim, temos que $L \ni \ell = g \cdot h^{-1} \in g \cdot H$, ou seja, $\sharp(L \cap g \cdot H) \geq 1$. Se $\ell_1, \ell_2 \in L \cap g \cdot H$, então existem $h_1, h_2 \in H$ tais que $\ell_1 = g \cdot h_1, \ell_2 = g \cdot h_2$. Segue que $g = \ell_1 \cdot h_1^{-1} = \ell_2 \cdot h_2^{-1}$, implicando que $f(\ell_1, h_1^{-1}) = f(\ell_2, h_2^{-1})$. Como f é injetora, concluímos que $\ell_1 = \ell_2$, daí $\sharp(L \cap h \cdot H) \leq 1$, para cada $g \in G$. Logo, como $1_G \in L$ e $\sharp(L \cap g \cdot H) = 1$, $\forall g \in G$, segue que L é uma transerval de G/H. ■

A proposição 4.3.7, diz que dada uma transversal L de G/H, podemos decompor de forma única cada elemento de G, como um produto de elementos de L e H, nesta ordem, isto é, para cada $g \in G$, existem únicos $\ell \in L$, $h \in H$ tais que $g = \ell \cdot h$, ou seja, $G = L \cdot H$.

Definição 4.3.8. Seja (G, τ) um grupo involutivo e $L \subset G$ um subconjunto não-vazio. Uma *aplicação polar* é uma aplicação $p : L \times G^\tau \to G$ definida por $p(\ell, k) = \ell \cdot k$ tal que $L \subset G_\tau$.

Proposição 4.3.9. *Seja (G, τ) um grupo involutivo e $1_G \in L \subset G_\tau$. Então, L é uma transversal de G/G^τ se, e somente se, a aplicação polar é bijetora.*

Demonstração Basta fazer $H = G^\tau$ na proposição 4.3.7. ■

Quando a aplicação polar $p : L \times G^\tau G$ for uma bijeção, o par (L, G^τ) é denominado uma *decomposição polar* de (G, τ), com $G = L \cdot G^\tau$.

Proposição 4.3.10. *Seja (G, τ) um grupo involutivo. São equivalentes as seguintes afirmações:*

i) P_G é um subgrupo torcido com a propriedade da única raiz quadrada.

ii) Para cada $g \in G$, existem únicos $x \in P_G$ e $k \in G^\tau$ tais que $g = x \cdot k$, onde $x = (g \cdot g^\bullet)^{1/2}$, ou seja, (P_G, G^τ) é uma decomposição polar de G.

iii) P_G é transversal em G/G^τ.

Demonstração: $i) \Longrightarrow ii)$ Dado $g \in G$, por hipótese, existe um único $x \in P_G \subset G_\tau$ tal que $x^2 = g \cdot g^\bullet \in P_G$, onde $x = (g \cdot g^\bullet)^{1/2}$. Fazendo $k = x^{-1} \cdot g \in G$, segue que $k \in G^\tau$ se, e somente se, $k^\bullet = k^{-1}$. De fato, basta ver que $k \cdot k^\bullet = (x^{-1} \cdot g) \cdot (x^{-1} \cdot g)^\bullet = x^{-1} \cdot g \cdot g^\bullet \cdot (x^{-1})^\bullet = x^{-1} \cdot x^2 \cdot x^{-1} = 1_G$.

Logo, se $x' \in P_G$ e $k' \in G^\tau$ são tais que $g = x' \cdot k'$, então $g \cdot g^\bullet = x^2 = (x')^2$, implicando que $x = x'$, o que garante que $k = k'$, mostrando a unicidade.

Portanto a aplicação polar é bijetora e (P_G, G^τ) é uma decomposição polar de G.

$ii) \Longrightarrow iii)$ Como $P_G \subset G_\tau$, então a aplicação $p : P_G \times G^\tau \to G$ dada por $p(x, k) = x \cdot k$ é uma aplicação polar. Como, por hipótese, a aplicação polar é bijetora, pela proposição 4.3.9, segue que P_G é uma transversal de G/G^τ.

$iii) \Longrightarrow i)$ Se P_G é transversal de G/G^τ, então, pela proposição 4.3.7, a aplicação polar é bijetora, ou seja, para cada $g \in G$, existem únicos $x \in P_G$, $k \in G^\tau$ tais que $g = x \cdot k$.

Temos que $g \cdot g^\bullet = (x \cdot k)(x \cdot k)^\bullet = x \cdot k \cdot k^\bullet \cdot x^\bullet = x \cdot k \cdot k^{-1} \cdot x = x^2$, e sendo $g \cdot g^\bullet \in P_G$, segue que P_G possui a propriedade da raiz quadrada.

Mostremos a unicidade dessa propriedade. Se $y \in P_G$ é tal que $y^2 = g \cdot g^\bullet$, com $g \in G$, então $y^{-1} \cdot g \in G^\tau$, pois

$$\begin{aligned} y^{-1} \cdot g &= y^{-1} \cdot g \cdot g^\bullet \cdot (g^\bullet)^{-1} = y^{-1} \cdot (g \cdot g^\bullet) \cdot (\tau(g)^{-1})^{-1} = y^{-1} \cdot y^2 \cdot \tau(g) \\ &= y \cdot \tau(g) = y^\bullet \cdot \tau(g) = \tau(y^{-1}) \cdot \tau(g) = \tau(y^{-1} \cdot g) = (g^{-1} \cdot y)^\bullet \end{aligned}$$

Logo, temos que $g = y \cdot (y^{-1} \cdot g) \in P_G \cdot G^\tau$ é uma decomposição para $g \in G$. Como a aplicação polar p é bijetora e sabendo $g = x \cdot k$, concluímos que $y = x$ e $y^{-1} \cdot g = k$. Pelo lema 4.3.3, segue que P_G é um subgrupo torcido.

■

Observação 4.3.11. *O conceito de transversal e seção são equivalentes. Se $L \subset G$ é uma transversal de G/H, então defina a aplicação $\sigma_L : G/H \to G$ por $\sigma(H) = 1_G$ e $\sigma_L(gH) = x_g$, onde $x_g \in gH \cap L$ é único. Logo, é fácil ver que σ_L é uma seção de $\pi : G \to G/H$. Reciprocamente, se $\sigma : G/H \to G$ é uma seção da projeção canônica, então $1_G \in \sigma(G/H)$ e como $\sigma(gH)H = gH$, segue que $\sharp(\sigma(G/H) \cap gH) \geq 1$. Se $x, y \in \sigma(G/H) \cap gH$, então $x = gh_1 = \sigma(gH) = gh_2 = y$, para cada $g \in G$, ou seja, $\sharp(\sigma(G/H) \cap gH) \leq 1$. Logo, $\sigma(G/H)$ é uma transversal de G/H.*

Observação 4.3.12. *Pelas observações* 4.3.5 *e* 4.3.11*, segue que sempre existe seção.*

4.4 Laços em transversais

Nesta seção, dada uma transversal $L \subset G$ de G/H, onde $H \subset G$ é subgrupo, introduziremos a operação transversal em L e a aplicação transversal de $L \times L$ em H. Dessa forma, L munido da operação transversal adquire uma estrutura de laço à esquerda, tornando possível definir a aplicação precessão em L. Veremos também que, se P_G é uma transversal de G^τ, então P_G é um B-laço com a operação transversal e a aplicação precessão é dada em termos da conjugação da aplicação transversal.

Seja $(G, \cdot)$ um grupo, $H \subset G$ um subgrupo e L uma transversal de G/H. Sabemos que para todo $g \in G$, existem únicos $\ell \in L$ e $h \in H$ tais que $g = \ell \cdot h$. Em particular, para $\ell_1, \ell_2 \in L \subset G$, existem únicos $\ell = \ell(\ell_1, \ell_2) \in L$ e $h = h(\ell_1, \ell_2) \in H$ tais que $\ell_1 \cdot \ell_2 = \ell \cdot h$. Assim, garantimos a existência de uma operação binária $\centerdot$ em L definida por $\ell_1 \centerdot \ell_2 = \ell$, e de uma aplicação $\mathbf{h} : L \times L \to H$ definida por $\mathbf{h}(\ell_1, \ell_2) = h$. Denominamos a operação $\centerdot$ em L de *operação transversal* e a aplicação $\mathbf{h}$ de *aplicação transversal*.

Proposição 4.4.1. *Seja $(G, \cdot)$ um grupo, $H \subset G$ um subgrupo e L uma transversal de G/H. Se $\centerdot : L \times L \to L$ é a operação transversal, então $(L, \centerdot)$ é um laço à esquerda.*

Demonstração: Se $L = \{1_G\}$ não há o que fazer. Suponhamos que $L \neq \{1_G\}$ e tomemos $\ell \in L$ tal que $\ell \neq 1_G$. Como $\ell = \ell \cdot 1_G = (\ell \centerdot 1_G) \cdot \mathbf{h}(\ell, 1_G)$, segue que $\ell \centerdot 1_G = \ell$. Escrevendo $\ell = 1_G \cdot \ell$, obtemos que $1_G \centerdot \ell = \ell$, mostrando que 1_G é o elemento neutro de $(L, \centerdot)$.

Dados $a, b \in L$, existem únicos $x_0 \in L$ e $h \in H$ tais que $a^{-1} \cdot b = x_0 \cdot h \in G = L \cdot H$, ou melhor, $a \cdot x_0 = b \cdot h^{-1}$. Como H é subgrupo, temos que $h^{-1} \in H$, mas $a \cdot x_0 = (a \centerdot x_0) \cdot \mathbf{h}(a, x_0)$, e devido a unicidade da decomposição, segue que a equação $a \centerdot x_0 = b$, possui solução única. Logo, $(L, \centerdot)$ é um laço à esquerda. ■

Fixado um laço à esquerda $(\mathcal{L}, \cdot)$ e dados $a, b \in \mathcal{L}$ temos que, para cada $c \in \mathcal{L}$, existe um único $x \in \mathcal{L}$ tal que $(a \cdot b) \cdot x = a \cdot (b \cdot c)$, onde x depende dos três elementos $a, b, c \in \mathcal{L}$. Uma vez fixados a e b, a determinação deste único elemento x é obtida de acordo com a escolha de $c \in \mathcal{L}$, afinal em $\mathcal{L}$ toda equação da forma $u \cdot x = v$, para quaisquer $u, v \in \mathcal{L}$, tem solução única. Formalmente, fixados $a, b \in \mathcal{L}$, existe e é única a função $\gamma_{a,b} : \mathcal{L} \to \mathcal{L}$ que satisfaz a igualdade $(a \cdot b) \cdot \gamma_{a,b}(c) = a \cdot (b \cdot c)$, para todo $c \in \mathcal{L}$. A aplicação definida acima é denominada de *aplicação precessão.* É imediato que a aplicação precessão é bijetora e $\gamma_{a,b}(1_{\mathcal{L}}) = 1_{\mathcal{L}}$.

Exemplo 4.4.2. *Em um grupo a aplicação precessão é a aplicação identidade.*

Exemplo 4.4.3. *Considere o laço à esquerda $(G/H, \oplus_\sigma)$. Se $a, b, c \in G$ e $h(ab) := [\sigma(\sigma(aH)bH)]^{-1}\sigma(aH)\sigma(bH)$, então $h(ab) \in H$ e $\gamma_{aH,bH}(cH) = h(ab)ch(ab)^{-1}H$. De fato: como $\sigma(aH) = ah$, para algum $h \in H$, temos que:*

$$h(ab) = (ah_1bh_2)^{-1}ah_1bh_3 = h_2^{-1}b^{-1}h_1^{-1}a^{-1}ah_1bh_3 = h_2^{-1}h_3 \in H, \text{ com } h_1, h_2, h_3 \in H.$$

Por verificação, segue que:

$$\begin{aligned} ((aH) \oplus_\sigma (bH)) \oplus_\sigma (h(ab)ch(ab)^{-1}H) &= (\sigma(aH)bH) \oplus_\sigma (h(ab)ch(ab)^{-1}H) \\ &= (\sigma(\sigma(aH)bH))h(ab)ch(ab)^{-1}H \\ &= \sigma(aH)\sigma(bH)cH \\ &= (aH) \oplus_\sigma (\sigma(bH)cH) \\ &= (aH) \oplus_\sigma ((bH) \oplus_\sigma (cH)). \end{aligned}$$

O seguinte teorema afirma que, dado um grupo involutivo (G, τ) temos que, P_G sob a hipótese de ser transversal ganha uma estrutura de B-laço em relação a operação transversal, onde sua aplicação precessão é caracterizada pela aplicação transversal.

Teorema 4.4.4. *Seja (G, τ) um grupo involutivo. Se P_G é uma transversal de G/G^τ e sendo $\centerdot : P_G \times P_G \to P_G$ a operação transversal e $\mathbf{h} : P_G \times P_G \to G^\tau$ a aplicação transversal, então as seguintes afirmações são verdadeiras:*

i) Para todo $a, b \in P_G$, temos que $a \cdot b = (a \centerdot b) \cdot \mathbf{h}(a, b) \in P_G \cdot G^\tau$, sendo $a \centerdot b = (a \cdot b^2 \cdot a)^{\frac{1}{2}}$.

ii) $(P_G, \centerdot)$ é um B-laço.

iii) Dados $a, b \in P_G$, temos que a aplicação precessão é dada por $\gamma_{a,b}(c) = \mathbf{h}(a,b) \cdot c \cdot \mathbf{h}(a,b)^{-1}$, $\forall c \in P_G$.

Demonstração: Suponhamos que P_G seja uma transversal de G/G^τ. Pelo item ii) da proposição 4.3.10, dado $g \in G$, existem únicos $x \in P_G$, $k \in G^\tau$ tais que $g = x \cdot k$, onde $x = (g \cdot g^\bullet)^{\frac{1}{2}}$.

i) Se $a, b \in P_G$, então existem únicos $x \in P_G$, $k \in G^\tau$ tais que $a \cdot b = x \cdot k$, onde $x = ((a \cdot b) \cdot (a \cdot b)^\bullet)^{\frac{1}{2}} = (a \cdot b \cdot b^\bullet \cdot a^\bullet)^{\frac{1}{2}}$. Como $P_G \subset G_\tau$, temos que $a^\bullet = a$ e $b^\bullet = b$. Logo, $x = (a \cdot b \cdot b \cdot a)^{\frac{1}{2}} = (a \cdot b^2 \cdot a)^{\frac{1}{2}}$. Mas $a \cdot b = (a \centerdot b) \cdot \mathbf{h}(a,b)$ e pela decomposição polar, temos que $x = a \centerdot b$, ou seja, $a \centerdot b = (a \cdot b^2 \cdot a)^{\frac{1}{2}}$.

ii) Pelo item i) da proposição 4.3.10, P_G é um subgrupo torcido com a propriedade da raiz quadrada única. Logo, do corolário 4.2.6, segue que $(P_G, \centerdot)$ é um B-laço.

iii) Como G é grupo, dados $a, b, c \in P_G \subset G$, temos que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Desenvolvendo cada lado da igualdade, obtemos que:

$$a \cdot (b \cdot c) = a \cdot ((b \centerdot c) \cdot \mathbf{h}(b,c)) = \underbrace{(a \centerdot (b \centerdot c))}_{\in P_G} \cdot \underbrace{\mathbf{h}(a, (b \centerdot c) \cdot \mathbf{h}(b,c)) \cdot \mathbf{h}(b,c)}_{\in G^\tau}.$$

$$\begin{aligned}(a \cdot b) \cdot c &= ((a \centerdot b) \cdot \mathbf{h}(a,b)) \cdot c = (a \centerdot b) \cdot (\mathbf{h}(a,b) \cdot c \cdot \mathbf{h}(a,b)^{-1}) \cdot \mathbf{h}(a,b) \\ &\overset{\substack{\text{lema} \\ 4.3.3}}{=} \underbrace{((a \centerdot b) \centerdot (\mathbf{h}(a,b) \cdot c \cdot \mathbf{h}(a,b)^{-1}))}_{\in P_G} \cdot \underbrace{\mathbf{h}(a \centerdot b, \mathbf{h}(a,b) \cdot c \cdot \mathbf{h}(a,b)^{-1}) \cdot \mathbf{h}(a,b)}_{\in G^\tau}\end{aligned}$$

Logo, $a \centerdot (b \centerdot c) = (a \centerdot b) \centerdot (\mathbf{h}(a,b) \cdot c \cdot \mathbf{h}(a,b)^{-1})$, mostrando que $\gamma_{a,b}(c) = \mathbf{h}(a,b) \cdot c \cdot \mathbf{h}(a,b)^{-1}$.

■

4.5 O Laço de Möbius

Nesta seção, veremos um teorema que liga alguns dos conceitos vistos nos capítulos anteriores com o capítulo atual. Na verdade, dado certo grupo involutivo (G, τ), iremos caracterizar G^τ e P_G, onde provaremos que o segundo conjunto possui a propriedade da raiz quadrada única.

Considere $\mathcal{C}_n$ a álgebra de Clifford associada a $(\mathbb{R}^n, -\langle .,. \rangle)$, B_n o disco unitário no espaço paravetorial $W = \mathbb{R} \oplus \mathbb{R}^n$ e os grupos ortogonal $O(n, \mathbb{R})$ e especial ortogonal $SO(n, \mathbb{R})$ em relação à W.

Do capítulo 3, temos que $G(B_n)$, ou seja, o conjunto das transformações de Möbius que preservam B_n, é um grupo. Note que, $j \in G(B_n)$ definida por $j(w) = -w$ é uma involução, tornando possível definir a aplicação $\sigma : G(B_n) \to G(B_n)$ da seguinte forma $\sigma(f) := j \circ f \circ j$. Afirmamos que σ é uma involução e um automorfismo. De fato: se $f \in G(B_n)$, então $\sigma^2(f) = \sigma(\sigma(f)) = j \circ \sigma(f) \circ j = \underbrace{j \circ j}_{=\mathrm{id}} \circ f \circ \underbrace{j \circ j}_{=\mathrm{id}} = f$, ou seja, f é uma involução. Pelo lema 2.1.7, segue que σ é bijetora.

Se $f, g \in G(B_n)$, então $\sigma(f \circ g) = j \circ f \circ g \circ j = j \circ f \circ j \circ j \circ g \circ j = \sigma(f) \circ \sigma(g)$. Logo, $(G(B_n), \sigma)$ é um grupo involutivo.

Nesse caso, veremos que os conjuntos G^τ e P_G ganham uma caracterização especial. E mais, iremos garantir que P_G possui a propriedade da raiz quadrada única.

Teorema 4.5.1. *Seja $(G(B_n), \sigma)$ um grupo involutivo. Então:*

i) $G(B_n)^\sigma = O(n, \mathbb{R})$ *é o grupo ortogonal.*

ii) $P_{G(B_n)} = \mathcal{T}_{\mathcal{M}}$ *é um subgrupo torcido com a propriedade da raiz quadrada única, onde* $\mathcal{T}_{\mathcal{M}} = \{\tau_a \mid a \in B_n\}$ *é o conjunto de todas as translações de Möbius.*

iii) $(\mathcal{T}_{\mathcal{M}}, O(n, \mathbb{R}))$ *é a decomposição polar de* $G(B_n)$.

Demonstração: Temos que, $G(B_n)^\sigma = \{f \in G(B_n) \mid f^\bullet = f^{-1}\}$, $G(B_n)_\sigma = \{f \in G(B_n) \mid f^\bullet = f\}$ e $P_{G(B_n)} = \{f \circ f^\bullet \mid f \in G(B_n)\}$ é um subgrupo torcido.

i) Se $\theta \in O(n, \mathbb{R}) \subset G(B_n)$ é uma transformação ortogonal, então, em particular, $\theta^{-1} : W \to W$ é uma transformação linear. Dado $w \in W$, segue que:

$$\begin{aligned} \theta^\bullet(w) &= [\sigma(\theta^{-1})](w) = (j \circ \theta^{-1} \circ j)(w) = j(\theta^{-1}(j(w))) \\ &= j(\theta^{-1}(-w)) = j(-\theta^{-1}(w)) = -(-\theta^{-1}(w)) = \theta^{-1}(w). \end{aligned}$$

Logo, $\theta^\bullet = \theta^{-1}$, mostrando que $\theta \in G(B_n)^\sigma$.

Agora, se $f \in G(B_n)^\sigma$, então $f^\bullet = f^{-1}$ se, e só se, $\sigma(f) = f$. Em particular, $\sigma(f(0)) = f(0) \Rightarrow f(0) = 0$. Pelo lema 3.2.9, segue que $f \in O(n, \mathbb{R})$ é uma transformação ortogonal. Logo, $G(B_n)^\sigma = O(n, \mathbb{R})$.

ii) Se $a \in B_n$, então a translação de Möbius $\tau_a \in \mathcal{T}_\mathcal{M}$ é tal que $\tau_a \in G(B_n)_\sigma$. **(1)**

De fato: temos que $\tau_a^{-1} = \tau_{-a}$ e se $w \in W$, então $j^{-1}(w) = -w$. Logo,

$$\begin{aligned} \tau_a^\bullet(w) &= [\sigma(\tau_a)]^{-1}(w) = (j \circ \tau_a \circ j)^{-1}(w) = (j^{-1} \circ \tau_a^{-1} \circ j^{-1})(w) \\ &= (j^{-1}(\tau_{-a}(-w))) = j^{-1}((-w-a)(1+\widehat{(-a)}(-w))^{-1}) \\ &= -(-w-a)(1+\widehat{a}w)^{-1} = (w+a)(1+\widehat{a}w)^{-1} = \tau_a(w). \end{aligned}$$

De acordo com o teorema 3.2.5, a translação de Möbius τ_a induz a matriz de Vahlen $\left(\begin{smallmatrix} 1 & a \\ \widehat{a} & 1 \end{smallmatrix}\right)$. E se $a \neq 0$, então $\widehat{a} = \overline{a}$ e $a\overline{a} = \|a\|^2$, pois $a \in W \subset \Gamma_n$.

Sejam $\lambda \in \mathbb{R}$ e $a \in B_n$ tais que $0 < \lambda < 1$ e $a \neq 0$. Daí segue que $\tau_{\lambda a} \in \mathcal{T}_\mathcal{M}$, induzindo a seguinte matriz de Vahlen dada por $\begin{pmatrix} 1 & \lambda a \\ \widehat{\lambda a} & 1 \end{pmatrix} = \begin{pmatrix} 1 & \lambda a \\ \lambda\overline{a} & 1 \end{pmatrix}$. Pelo teorema 3.2.5, vamos obter a composição $\tau_{\lambda a} \circ \tau_{\lambda a}$ através da multiplicação das matrizes de Vahlen correspondentes, isto é:

$$\begin{pmatrix} 1 & \lambda a \\ \lambda\overline{a} & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda a \\ \lambda\overline{a} & 1 \end{pmatrix} = \begin{pmatrix} 1+\lambda^2 a\overline{a} & 2\lambda a \\ 2\lambda\overline{a} & 1+\lambda^2\overline{a}a \end{pmatrix} = \begin{pmatrix} 1+\lambda^2\|a\|^2 & 2\lambda a \\ 2\lambda\overline{a} & 1+\lambda^2\|a\|^2 \end{pmatrix}$$

$$= (1+\lambda^2\|a\|^2)\begin{pmatrix} 1 & \frac{2\lambda}{1+\lambda^2\|a\|^2}a \\ \frac{2\lambda}{1+\lambda^2\|a\|^2}\overline{a} & 1 \end{pmatrix}.$$

Se $\frac{2\lambda}{1+\lambda^2\|a\|^2} = 1$, então $\lambda = \frac{1-\sqrt{1-\|a\|^2}}{\|a\|^2} < 1$. Caso $a = 0$, então $\tau_a = \mathrm{id}$ e não há o que fazer. Logo, para cada $\tau_a \in \mathcal{T}_{\mathcal{M}}$, existe $\lambda \in \mathbb{R}$, $0 < \lambda < 1$, tal que $\tau_a = \tau_{\lambda a} \circ \tau_{\lambda a} \overset{(1)}{=} \tau_{\lambda a} \circ \tau_{\lambda a}{}^\bullet \in P_{G(B_n)}$, mostrando que $\mathcal{T}_{\mathcal{M}} \subset P_{G(B_n)}$.

Reciprocamente, se $f \circ f^\bullet \in P_{G(B_n)}$, onde $f \in G(B_n)$, então, pela proposição 3.2.10, existem $\tau_a \in \mathcal{T}_{\mathcal{M}}$ e $\theta \in O(n,\mathbb{R})$ tais que $f = \tau_a \circ \theta$. Sendo $\theta^\bullet = \theta^{-1}$ e $\tau_a{}^\bullet = \tau_a$, segue que $f \circ f^\bullet = \tau_{\frac{2}{1+\|a\|^2}a} \in \mathcal{T}_{\mathcal{M}}$. Logo, $P_{G(B_n)} = \mathcal{T}_{\mathcal{M}}$, restando mostrar que $P_{G(B_n)}$ possui a propriedade da raiz quadrada única.

Sejam $a, b \in B_n$ não-nulos tais que $a \neq b$ e suponhamos, por absurdo, que $\tau_a^2 = \tau_b^2$. Em particular, $\tau_a^2(0) = \frac{2}{1+\|a\|^2}a = \frac{2}{1+\|b\|^2}b = \tau_b^2(0)$. Da igualdade $\|\tau_a^2(0)\|^2 = \|\tau_b^2(0)\|^2$, obtemos que: $\frac{2\|a\|}{1+\|a\|^2} = \frac{2\|b\|}{1+\|b\|^2}$. Desenvolvendo, obtemos $(\|a\| - \|b\|)(1 - \|a\|\|b\|) = 0 \Rightarrow \|a\| = \|b\|$ ou $\|a\|\|b\| = 1$.

Se $\|a\| = \|b\|$, então de $\tau^2(0) = \tau^2(0)$, obtemos que $a = b$. Se $\|a\|\|b\| = 1$, então $\|b\| = \frac{1}{\|a\|} > 1$, pois $0 < \|a\| < 1$.

Logo, pela contra-positiva, se $\tau_a^2 = \tau_b^2$, então $a = b$.

iii) Por ii) e pelo item i) do teorema 4.3.10 temos que, $\mathcal{T}_{\mathcal{M}}$ é uma transversal de $G(B_n)/O(n,\mathbb{R})$, donde segue que $(\mathcal{T}_{\mathcal{M}}, O(n,\mathbb{R}))$ é a decomposição polar de $G(B_n)$.

■

Observação 4.5.2. *Com o teorema* 4.5.1*, garantimos a unicidade da decomposição vista na proposição* 3.2.10.

Sejam $a, b \in B_n$ tais que $a, b \neq 0$ e $ab \neq 1$. Pelo item iii) do teorema 4.5.1, existem únicos $\tau_c \in \mathcal{T}_{\mathcal{M}}$ e $\theta \in O(n, \mathbb{R})$ tais que $\tau_a \circ \tau_b = \tau_c \circ \theta$. Por outro lado, podemos obter uma caracterização para τ_c e θ através da multiplicação das respectivas matrizes de Vahlen $\left(\begin{smallmatrix} 1 & a \\ \widehat{a} & 1 \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} 1 & b \\ \widehat{b} & 1 \end{smallmatrix}\right)$. De acordo com a proposição 2.2.15 item i), temos que $1 + a\widehat{b}$ é invertível. Daí segue que:

$$\begin{aligned}
\begin{pmatrix} 1 & a \\ \widehat{a} & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ \widehat{b} & 1 \end{pmatrix} &= \begin{pmatrix} 1 + a\widehat{b} & a + b \\ \widehat{a + b} & 1 + \widehat{a}b \end{pmatrix} \\
&= \begin{pmatrix} 1 & (a+b)(1+\widehat{a}b)^{-1} \\ \widehat{(a+b)(1+\widehat{a}b)^{-1}} & 1 \end{pmatrix}\begin{pmatrix} 1 + a\widehat{b} & 0 \\ 0 & 1 + \widehat{a}b \end{pmatrix}.
\end{aligned}$$

Usando o teorema 3.2.5 na última igualdade acima segue que, a primeira matriz de Vahlen corresponde a translação de Möbius $\tau_{(a+b)(1+\widehat{a}b)^{-1}}$ e a segunda matriz de Vahlen corresponde a transformação de Möbius $\theta : \widehat{W} \to \widehat{W}$ dada por $\theta(w) = (1 + a\widehat{b})w\left(\widehat{1 + a\widehat{b}}\right)^{-1}$ que é uma transformação ortogonal.

Como $\mathcal{T}_{\mathcal{M}}$ é uma transversal de $G(B_n)/O(n, \mathbb{R})$, pelo teorema 4.4.4, podemos considerar a operação transversal $\centerdot : \mathcal{T}_{\mathcal{M}} \times \mathcal{T}_{\mathcal{M}} \to \mathcal{T}_{\mathcal{M}}$, onde $(\mathcal{T}_{\mathcal{M}}, \centerdot)$ é um B-laço. Para $a \in B_n$, temos $\widehat{a} = \overline{a}$, mostrando que $\tau_c = \tau_a \centerdot \tau_b = \tau_{(a+b)(1+\overline{a}b)^{-1}}$.

Agora, definimos a aplicação $g : \mathcal{T}_{\mathcal{M}} \to B_n$ por $g(\tau_a) = a$. Claramente, g é bijetora. Dessa forma, podemos definir a operação binária $\oplus$ em B_n por $a \oplus b := g(\tau_a \centerdot \tau_b)$. Como $\tau_a \centerdot \tau_b = \tau_{(a+b)(1+\overline{a}b)^{-1}}$, segue que $a \oplus b := (a + b)(1 + \overline{a}b)^{-1}$.

Proposição 4.5.3. *$(B_n, \oplus)$ é um B-laço.*

Demonstração: B_n é um laço, pois de $a \oplus b = g(\tau_a \centerdot \tau_b)$ e $\tau_0 = \mathrm{id}$, segue que $0 \oplus a = a \oplus 0 = a$. Como as equações $\tau_a \centerdot \tau_x = \tau_b$ e $\tau_y \centerdot \tau_a = \tau_b$ possuem solução única em $(\mathcal{T}_{\mathcal{M}}, \centerdot)$ temos que, $a \oplus x = b$ e $y \oplus a = b$ possuem solução única em $(B_n, \oplus)$. Ainda, B_n é um Bol-laço à esquerda, pois $\tau_a \centerdot \tau_b = \tau_{a \oplus b}$ e sendo $\mathcal{T}_{\mathcal{M}}$ um Bol-laço, segue que

$$a \oplus (b \oplus (a \oplus c)) = g(\tau_{a \oplus (b \oplus (a \oplus c))}) = g(\tau_a \centerdot (\tau_b \centerdot (\tau_a \centerdot \tau_c))) = g((\tau_a \centerdot (\tau_b \centerdot \tau_a)) \centerdot \tau_c) = (a \oplus (b \oplus a)) \oplus c.$$

Sendo $a^{-1} = -a$ e $g(\tau_a^{-1}) = g(\tau_{-a}) = -a$, temos que:

$$-(a \oplus b) = g((\tau_a \centerdot \tau_b)^{-1}) \overset{(*)}{=} g(\tau_a^{-1} \centerdot \tau_b^{-1}) = g(\tau_{-a} \centerdot \tau_{-b}) = (-a) \oplus (-b)$$

onde em $(*)$ usamos o fato de $\mathcal{T}_{\mathcal{M}}$ ser um K-laço. Logo, B_n é um K-laço possuindo a propriedade da raiz quadrada única. ∎

Definição 4.5.4. Chamamos o B-laço $(B_n, \oplus)$ de *laço de Möbius.*

Teorema 4.5.5. *O laço de Möbius $(B_n, \oplus)$ satisfaz as seguintes propriedades:*

i) A operação $\oplus : B_n \times B_n \to B_n$ é dada em termos da álgebra de Clifford $\mathcal{C}_n$.

ii) Dados $a, b \in B_n$, temos que $\gamma_{a,b}(c) = qcq^*$, para todo $c \in B_n$, onde $q = \frac{1+a\bar{b}}{\|1+a\bar{b}\|}$ e sendo $\gamma_{a,b} \in SO(n, \mathbb{R})$

Demonstração: O item i) é imediato.

ii) Dados $a, b \in B_n$, existem únicos $\tau_{a\oplus b} \in \mathcal{T}_{\mathcal{M}}$ e $\theta \in O(n, \mathbb{R})$ tais que $\tau_a \circ \tau_b = \tau_{a\oplus b} \circ \theta$, onde $\theta(w) = (1 + a\widehat{b})w\widehat{(1 + a\widehat{b})}^{-1}$, $\forall w \in \widehat{W}$. Para todo $c \in B_n$, temos $a \oplus (b \oplus c) = (a \oplus b) \oplus \gamma_{a,b}(c)$. Daí segue que $\tau_a \centerdot (\tau_b \centerdot \tau_c) = (\tau_a \centerdot \tau_b) \centerdot \tau_{\gamma_{a,b}(c)}$, sendo $\tau_{\gamma_{a,b}(c)} = \gamma_{\tau_a,\tau_b}(\tau_c)$. Mas por 4.4.4., temos que $\gamma_{\tau_a,\tau_b}(\tau_c) = \theta \circ \tau_c \circ \theta^{-1}$. Logo, para algum $x \in B_n$, vale a igualdade $\gamma_{\tau_a,\tau_b}(\tau_c) = \tau_x$.

Note que, ao multiplicar a matriz de Vahlen $\begin{pmatrix} 1+a\widehat{b} & 0 \\ 0 & 1+\widehat{a}b \end{pmatrix}$ pelo número real $\frac{1}{\|1+a\widehat{b}\|}$ e fazendo $q = \frac{1}{\|1+a\widehat{b}\|}(1 + a\widehat{b})$, obtemos uma nova matriz de Vahlen dada por $\begin{pmatrix} q & 0 \\ 0 & \widehat{q} \end{pmatrix}$. Pelo item iv) do teorema 3.4.5, essa matriz induz a mesma transformação de Möbius θ. Ainda, note que, o elemento q satisfaz o item i) da proposição 2.2.15. Logo, a aplicação $qw\widehat{q}^{-1} = qwq^* \in W$ é uma rotação **(1)**. Por outro lado, como $\begin{pmatrix} q & 0 \\ 0 & \widehat{q} \end{pmatrix}^{-1} = \begin{pmatrix} \overline{q} & 0 \\ 0 & q^* \end{pmatrix}$, e sendo $q\overline{q} = \overline{q}q = 1$, temos que

$$\begin{pmatrix} q & 0 \\ 0 & \widehat{q} \end{pmatrix} \begin{pmatrix} 1 & c \\ \widehat{c} & 1 \end{pmatrix} \begin{pmatrix} q & 0 \\ 0 & \widehat{q} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & qcq^* \\ \widehat{qcq^*} & 1 \end{pmatrix},$$

que é a matriz de Vahlen da translação de Möbius τ_{qcq^*}, afinal $\|qcq^*\| = \|c\| < 1$. Portanto, $x = qcq^*$ e como $\widehat{a} = \overline{a}$, $\forall a \in \varGamma_n$, segue que $\gamma_{a,b}(c) = qcq^* = \frac{(1+a\bar{b})}{\|1+a\bar{b}\|}c\frac{(1+\bar{a}b)^{-1}}{\|1+a\bar{b}\|}$, e por (1), garantimos que $\gamma_{a,b} \in SO(n, \mathbb{R})$.

$\blacksquare$

Exemplo 4.5.6. *Considerando a álgebra de Clifford* $\mathcal{C}\ell_1 \cong \mathbb{C}$*, segue que o disco unitário complexo é um B-laço. De fato: dados* $z, w \in B_1 = \{z \in \mathbb{C} \,||z| < 1\}$*, pelo teorema* 4.5.5*, vale que* $z \oplus w = \frac{z+w}{1+\bar{z}w}$ *e* $q = \frac{1+z\overline{w}}{|1+z\overline{w}|}$*, sendo* $\gamma_{z,w}(c) = qc(\widehat{q})^{-1} = qcq^* = \frac{1+z\overline{w}}{|1+z\overline{w}|}c\frac{|1+z\overline{w}|}{1+\bar{z}w} = \frac{1+z\overline{w}}{1+\bar{z}w}c$*. Logo, podemos escrever* $\gamma_{z,w} = \frac{z\oplus w}{w\oplus z}$.

Capítulo 5

Girogrupos

Neste capítulo, veremos que o conceito de girogrupo, que geometricamente é uma adaptação de vetores para a geomtria hiperbólica e algebricamente, generaliza o conceito de grupo, foi introduzido por Abraham A. Ungar em 1988. Na primeira seção, apresentaremos algumas de suas propriedades e exemplos, os quais se encontram em **[19]**. Na segunda e última seção, abordaremos o artigo de Lawson, mostrando que os conceitos de K-laços e girogrupos girocomutativos são equivalentes, conforme observado em **[12]**. Com isso, obtemos como consequência o nosso resultado principal, que é a generalização do caso conhecido do girogrupo de Möbius, uma vez que, do capítulo 4, $(B_n, \oplus)$ é um K-laço. O girogrupo de Möbius possui aplicações na Fisíca, no estudo das transformações de Lorentz, na teoria da relatividade especial, pois o grupo de Lorentz atua no disco de todos as possíveis velocidades simétricas via aplicações conformes. Usamos como referências para este capítulo: **[5]**, **[12]** e **[19]**.

5.1 Introdução aos Girogrupos

Nesta seção, definiremos girogrupos, sendo estes uma generalização do conceito de grupo. Apresentaremos algumas de suas propriedades e daremos alguns exemplos de girogrupos no final da seção.

Definição 5.1.1. Um conjunto não-vazio G, munido de uma operação binária $\oplus$, é um *girogrupo* se para todos $a, b \in G$, existir uma aplicação $gyr[a, b] : G \to G$ de maneira que as seguintes condições sejam satisfeitas:

i) Existe $e \in G$ tal que $e \oplus a = a$, $\forall a \in G$. Neste caso, e é um *elemento neutro à esquerda* em G.

ii) Para cada $a \in G$, existe $a' \in G$ tal que $a' \oplus a = e$. Neste caso, dizemos que a' é um *inverso à esquerda* de a.

iii) Dados $a, b, c \in G$, existe um único elemento $gyr[a, b](c) \in G$ tal que $a \oplus (b \oplus c) = (a \oplus b) \oplus gyr[a, b](c)$. Chamamos essa igualdade de *lei da giroassociatividade à esquerda.*

iv) A aplicação $gyr[a, b] : G \to G$ é um automorfismo, ou seja, $gyr[a, b](c \oplus d) = gyr[a, b](c) \oplus gyr[a, b](d)$, $\forall c, d \in G$, chamado de *giroautomorfismo* gerado por a e b, e a aplicação $gyr : G \times G \to Aut(G)$ chamada de *girador* de G, onde $Aut(G) = \{f : G \to G \mid f \text{ é um automorfismo}\}$.

v) $gyr[a \oplus b, b] = gyr[a, b]$, $\forall a, b \in G$. Chamamos esta igualdade de *propriedade do laço à esquerda.*

Dizemos que o girogrupo é *girocomutativo* se $a \oplus b = gyr[a, b](b \oplus a)$, $\forall a, b \in G$.

Da definição de girogrupo, as duas primeiras condições dizem respeito sobre a estrutura de G, enquanto as duas últimas condições falam da aplicação $gyr[a, b]$. Enfim, a terceira condição é a ponte que liga a estrutura de G com $gyr[a, b]$.

Vejamos algumas propriedades imediatas da definição de girogrupo.

Proposição 5.1.2. *Se $(G, \oplus)$ é um girogrupo, então valem as seguintes propriedades:*

i) Dados $a, b, c \in G$, se $a \oplus b = a \oplus c$ então $b = c$.

ii) *Se* $e \in G$ *é um elemento neutro à esquerda em* G*, então* $gyr[e, a] = \mathrm{id}$.

iii) *Se* a' *um elemento inverso à esquerda de* $a \in G$*, então* $gyr[a', a] = \mathrm{id}$.

iv) $gyr[a, a] = \mathrm{id}$*,* $\forall a \in G$.

v) *Se* $e \in G$ *é um elemento neutro à esquerda em* G*, então* $a \oplus e = a$*,* $\forall a \in G$*, ou seja,* e *é um elemento neutro à direita em* G.

vi) *Existe um único elemento que é neutro à esquerda e neutro à direita em* G*, denotado por* $0 \in G$*, isto é,* $0 \oplus a = a \oplus 0 = a, \forall a \in G$.

vii) *Se* $a' \in G$ *é um elemento inverso à esquerda de* $a \in G$*, então* $a \oplus a' = e$*, ou seja,* a' *é um elemento inverso à direita de* $a \in G$.

viii) *Dado* $a \in G$*, existe um único elemento que é inverso de* a*, denotado por* $\ominus a$ *e* $\ominus(\ominus a) = a, \forall a \in G$.

ix) $(\ominus a) \oplus (a \oplus b) = b\ \forall a, b \in G$*. (lei do cancelamento à esquerda)*

x) $gyr[a, b](c) = (\ominus(a \oplus b)) \oplus [a \oplus (b \oplus c)]$*,* $\forall a, b, c \in G$.

xi) $gyr[a, b](0) = 0$*,* $\forall a, b \in G$.

xii) $gyr[a, b](\ominus c) = \ominus gyr[a, b](c)$*,* $\forall a, b, c \in G$.

xiii) $gyr[a, 0] = \mathrm{id}$*,* $\forall a \in G$.

Demonstração:

i) Dados $e \in G$ um elemento neutro à esquerda em G e $a' \in G$ um inverso à esquerda de $a \in G$, por hipótese, temos que $a' \oplus (a \oplus b) = a' \oplus (a \oplus c)$. Usando a lei da giroassociatividade à esquerda em cada lado da igualdade, segue que:

$$(\underbrace{a' \oplus a}_{=e}) \oplus gyr[a', a](b) = (\underbrace{a' \oplus a}_{=e}) \oplus gyr[a', a](c) \Rightarrow gyr[a', a](b) = gyr[a', a](c).$$

Como $gyr[a', a]$ é injetora, segue que $b = c$.

ii) Dados $a, b \in G$ e $e \in G$ um elemento neutro à esquerda em G, pela lei da giroassociatividade à esquerda, temos que:

$$a \oplus b = e \oplus (a \oplus b) = (e \oplus a) \oplus gyr[e, a](b) = a \oplus gyr[e, a](b)$$

Logo, do item i), segue que $b = gyr[e, a](b)$, isto é, $gyr[e, a] = \text{id}$.

iii) Seja $a' \in G$ um elemento inverso à esquerda de $a \in G$. Pela propriedade do laço à esquerda, segue que $gyr[a', a] = gyr[a' \oplus a, a] = gyr[e, a] \stackrel{ii)}{=} \text{id}$.

iv) Seja e um elemento neutro à esquerda em G. Usando a propriedade do laço à esquerda e o item ii), temos $gyr[a, a] = gyr[e \oplus a, a] = gyr[e, a] = \text{id}$, $\forall a \in G$.

v) Seja $e \in G$ um elemento inverso à esquerda em G e $a' \in G$ um elemento inverso à esquerda de $a \in G$. Usando a lei da giroassociatividade, temos que:

$$a' \oplus (a \oplus e) = (\underbrace{a' \oplus a}_{=e}) \oplus \underbrace{gyr[a', a]}_{=\text{id}}(e) = e \oplus e = e = a' \oplus a.$$

Logo, pelo item i) segue que $a \oplus e = a$, $\forall a \in G$.

vi) Se $e_0 \in G$ é tal que $e_0 \oplus a = a \oplus e_0 = a$, $\forall a \in G$, então, em particular, $e_0 = e \oplus e_0 = e$, mostrando que e é o elemento neutro de G, denotado por $0 \in G$.

vii) Seja $a' \in G$ um elemento inverso à esquerda de $a \in G$. Usando a lei da giroassociatividade e ii), segue que $a' \oplus (a \oplus a') = 0 \oplus a' = a' = a' \oplus 0$. Logo, pelo item i), obtemos que $a \oplus a' = 0$, $\forall a \in G$.

viii) Seja $a'' \in G$ tal que $a'' \oplus a = a \oplus a'' = 0$. Logo, $a'' = a'' \oplus 0 = a'' \oplus (a \oplus a') = (a'' \oplus a) \oplus gyr[a'', a](a') = 0 \oplus a' = a'$, mostrando que a é invertível. Denotamos o inverso de a por $\ominus a$.

ix) Dados $a, b \in G$, pela lei da giroassociatividade à esquerda e iii), temos que $(\ominus a) \oplus (a \oplus b) = 0 \oplus b = b$.

x) $\ominus(a \oplus b) \oplus [a \oplus (b \oplus c)] = \ominus(a \oplus b)[(a \oplus b) \oplus gyr[a,b](c)] \overset{ix)}{=} gyr[a,b](c)$, $\forall a, b, c \in G$.

xi) Tome $c = 0$ no item x).

xii) $0 = gyr[a,b](0) = gyr[a,b]((\ominus c) \oplus c) = gyr[a,b](\ominus c) \oplus gyr[a,b](c)$. Logo, do item viii) segue que $\ominus gyr[a,b](c) = gyr[a,b](\ominus c)$, $\forall a, b, c \in G$.

xiii) Fazendo $b = 0$ no item x), vem que $gyr[a,0](c) = \ominus(a \oplus 0) \oplus (a \oplus (0 \oplus c)) = (\ominus a) \oplus (a \oplus c) = ((\ominus a) \oplus a) \oplus gyr[\ominus a, a](c) = 0 \oplus c = c$, $\forall a, c \in G$, ou seja, $gyr[a, 0] = \mathrm{id}$.

$\blacksquare$

Observação 5.1.3. *Dados $a, b \in G$, definimos $\ominus a \oplus a := (\ominus a) \oplus a$, $a \ominus b := a \oplus (\ominus b)$ e $\ominus a \ominus b := (\ominus a) \oplus (\ominus b)$.*

Exemplo 5.1.4. *Listamos abaixo alguns girogrupos:*

i) Todo grupo G é um girogrupo, basta tomar $gyr[a,b] = \mathrm{id}$, $\forall a, b \in G$.

ii) Considere T_4 o grupo de todas as matrizes triangulares superiores de ordem 4 com entradas complexas, cuja diagonal principal é igual a 1, em relação a multiplicação usual. Definindo $A \odot B := A^2 B A^{-1}$ e considerando $gyr[A,B](C) = (A \odot B)^{-1} \odot [A \odot (B \odot C)]$, $\forall A, B, C \in T_4$, segue que $(T_4, \odot)$ é um girogrupo.

iii) Considere o conjunto $K_{16} := \{1, 2, \ldots, 16\}$ com a tábua da operação $\odot : K_{16} \times K_{16} \to K_{16}$ dada abaixo, possuindo apenas dois giroautomorfismos, sendo um a *identidade e o outro, denotado por* $A : K_{16} \to K_{16}$*, obedecendo:*

$$\begin{array}{cccc} 1 \to 1 & 5 \to 5 & 9 \to 10 & 13 \to 14 \\ 2 \to 2 & 6 \to 6 & 10 \to 9 & 14 \to 13 \\ 3 \to 3 & 7 \to 7 & 11 \to 12 & 15 \to 16 \\ 4 \to 4 & 8 \to 8 & 12 \to 11 & 16 \to 15 \end{array}$$

$\odot$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	3	4	2	1	7	8	6	5	12	11	9	10	16	15	13	14
4	4	3	1	2	8	7	5	6	11	12	10	9	15	16	14	13
5	5	6	7	8	4	3	2	1	16	15	13	14	10	9	12	11
6	6	5	8	7	3	4	2	1	15	16	14	13	9	10	11	12
7	7	8	6	5	1	2	3	4	14	13	16	15	11	12	10	9
8	8	7	5	6	2	1	4	3	13	14	15	16	12	11	9	10
9	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
10	10	9	12	11	14	13	16	15	2	1	4	3	6	5	8	7
11	11	12	10	9	15	16	14	13	4	3	1	2	8	7	5	6
12	12	11	9	10	16	15	13	14	3	4	2	1	7	8	6	5
13	13	14	15	16	12	11	9	10	7	8	6	5	2	1	4	3
14	14	13	16	15	11	12	10	9	8	7	5	6	2	1	4	3
15	15	16	14	13	9	10	11	12	5	6	7	8	4	3	1	2
16	16	15	13	14	10	9	12	11	6	5	8	7	3	4	2	1

$gyr[a,b]$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id
2	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id
3	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id
4	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id	id
5	id	id	id	id	id	id	id	A	A	A	A	A	A	A	A	A
6	id	id	id	id	id	id	id	A	A	A	A	A	A	A	A	A
7	id	id	id	id	id	id	id	A	A	A	A	A	A	A	A	A
8	id	id	id	id	id	id	id	A	A	A	A	A	A	A	A	A
9	id	id	id	id	A	A	A	A	id	id	id	id	A	A	A	A
10	id	id	id	id	A	A	A	A	id	id	id	id	A	A	A	A
11	id	id	id	id	A	A	A	A	id	id	id	id	A	A	A	A
12	id	id	id	id	A	A	A	A	id	id	id	id	A	A	A	A
13	id	id	id	id	A	A	A	A	A	A	A	A	id	id	id	id
14	id	id	id	id	A	A	A	A	A	A	A	A	id	id	id	id
15	id	id	id	id	A	A	A	A	A	A	A	A	id	id	id	id
16	id	id	id	id	A	A	A	A	A	A	A	A	id	id	id	id

De acordo com as tabelas, temos que $(K_{16}, \odot)$ *é um girogrupo, não-girocomutativo, pois* $9 \odot 8 = 16$*, mas* $gyr[9,8](8 \odot 9) = A(13) = 14$.

Observação 5.1.5. *Não se verifica o exemplo ii) de imediato, uma demonstração é encontrada em* [**7**].

Observação 5.1.6. *O exemplo iii) é de um girogrupo finito, o qual foi criado pelo pacote de software MAGMA e por sua biblioteca* [**3**], *utilizando o método desenvolvido em* [**7**].

5.2 Laços e Girogrupos

É notável algumas semelhanças entre as definições e propriedades de girogrupos e as de laços. Na verdade, os K-laços e os girogrupos girocomutativos gozam das mesmas propriedades. O objetivo deste capítulo é o de apresentar um teorema que liga os K-laços com os girogrupos girocomutativos, conforme Lawson observa em [**12**]. Dessa forma, poderemos ampliar nossos exemplos de girogrupos, sendo o principal exemplo dessa dissertação a generalização do girogrupo de Möbius.

Definição 5.2.1. A operação *coadição* em um girogrupo $(G, \oplus)$ é definida por:

$$a \boxplus b := a \oplus gyr[a, \ominus b](b), \ \forall a, b \in G.$$

Lema 5.2.2. *Se $(G, \oplus)$ é um girogrupo, então, para quaisquer $a, b, c \in G$, as seguintes identidades são verdadeiras:*

i) $gyr[a, b \oplus c] \circ gyr[b, c] = gyr[a \oplus b, gyr[a, b](c)] \circ gyr[a, b]$.

ii) $\mathrm{id} = gyr[a \oplus b, \ominus gyr[a, b](b)] \circ gyr[a, b]$.

iii) $\mathrm{id} = gyr[a, \ominus gyr[a, b](b)] \circ gyr[a, b]$.

iv) $\mathrm{id} = gyr[\ominus a, a \oplus b] \circ gyr[a, b]$.

v) $\mathrm{id} = gyr[b, a \oplus b] \circ gyr[a, b]$.

Demonstração: Sejam $a, b, c, d \in G$.

i) $a\oplus(b\oplus(c\oplus d)) = a\oplus((b\oplus c)\oplus gyr[b,c](d)) = (a\oplus(b\oplus c))\oplus gyr[a,b\oplus c](gyr[b,c](d))$.

De outra forma, temos que:

$$\begin{aligned} a \oplus (b \oplus (c \oplus d)) &= (a \oplus b) \oplus gyr[a,b](c \oplus d) \\ &= (a \oplus b) \oplus (gyr[a,b](c) \oplus gyr[a,b](d)) \\ &= ((a \oplus b) \oplus gyr[a,b](c)) \oplus gyr[a \oplus b, gyr[a,b](c)](gyr[a,b](d)) \end{aligned}$$

$$= (a \oplus (b \oplus c)) \oplus gyr[a \oplus b, gyr[a,b](c)](gyr[a,b](d)).$$

Logo, do item i) de 5.1.2, segue o resultado.

ii) Tome $c = \ominus b$ em i) e use xii) de 5.1.2.

iii) Segue do item ii), que:

$$\begin{aligned} \mathrm{id} &= gyr[a \oplus b, \ominus gyr[a,b](b)] \circ gyr[a,b] \\ &\overset{1)}{=} gyr[(a \oplus b) \oplus gyr[a,b](\ominus b), \ominus gyr[a,b](b)] \circ gyr[a,b] \\ &\overset{2)}{=} gyr[a \oplus (b \ominus b), \ominus gyr[a,b](b)] \circ gyr[a,b] \\ &= gyr[a, \ominus gyr[a,b](b)] \circ gyr[a,b], \end{aligned}$$

sendo 1)-lei do laço à esquerda e o item xii) da proposição 5.1.2 e 2) a lei da giroassociatividade à esquerda.

iv) Se $b = \ominus a$ em i), então:

$$gyr[a, \ominus a \oplus c] \circ gyr[\ominus a, c] = gyr[a \ominus a, gyr[a, \ominus a](c)] \circ gyr[a, \ominus a] = \mathrm{id},$$

onde na última igualdade, segue dos ítens xiii) e iii) de 5.1.2. Substituindo a por $\ominus a$ e c por b, segue o desejado.

v) $\text{id} \overset{iv)}{=} gyr[\ominus a, a \oplus b] \circ gyr[a, b] \overset{1)}{=} gyr[\ominus a \oplus (a \oplus b), a \oplus b] \circ gyr[a, b]$

$\overset{2)}{=} gyr[b, a \oplus b] \circ gyr[a, b]$, sendo 1)-propriedade do laço à esquerda, 2)-lei do cancelamento à esquerda.

■

Lema 5.2.3. *Se $(G, \oplus)$ é um girogrupo, então são válidas as afirmações:*

i) Para todo $a, b, c \in G$, vale a identidade $a \oplus (b \oplus (a \oplus c)) = (a \oplus (b \oplus a)) \oplus c$.

ii) Dados $a, b \in G$, existem únicos $x, y \in G$ tais que $a \oplus x = b$ e $y \oplus a = b$, sendo $x = \ominus a \oplus b$ e $y = b \boxplus (\ominus a)$.

iii) $\ominus(a \oplus b) = gyr[a, b](\ominus b \ominus a)$.

iv) G é girocomutativo se, e somente se, $\ominus(a \oplus b) = \ominus a \ominus b$, $\forall a, b \in G$.

Demonstração:

i) Se $a, b, c \in G$, então

$$\begin{aligned}
a \oplus (b \oplus (a \oplus c)) &= (a \oplus b) \oplus gyr[a, b](a \oplus c) \\
&= (a \oplus b) \oplus (gyr[a, b](a) \oplus gyr[a, b](c)) \\
&\overset{1)}{=} ((a \oplus b) \oplus gyr[a, b](a)) \oplus (gyr[a \oplus b, gyr[a, b](a)] \circ gyr[a, b])(c) \\
&\overset{2)}{=} (a \oplus (b \oplus a)) \oplus (gyr[a, b \oplus a] \circ gyr[b, a])(c) \\
&\overset{3)}{=} (a \oplus (b \oplus a)) \oplus c,
\end{aligned}$$

sendo 1)-lei da giroassociatividade à esquerda, 2)-lema 5.2.2 item i) e 3)-lema 5.2.2 item v).

ii) Dados $a, b \in G$, defina $x = \ominus a \oplus b \in G$. Logo, pela lei do cancelamento à esquerda e item i) de 5.1.2, segue que x é único tal que $a \oplus x = b$. Agora, se $y = b \boxplus (\ominus a)$, então $y = b \oplus (\ominus gyr[b,a](a))$. Logo, temos que:

$$\begin{aligned} y \oplus a &= (b \ominus gyr[b,a](a)) \oplus a \\ &\overset{\substack{5.2.2\\ iii)}}{=} (b \ominus gyr[b,a](a)) \oplus gyr[b, \ominus gyr[b,a](a)](gyr[b,a](a)) \\ &= b \oplus (\ominus gyr[b,a](a) \oplus gyr[b,a](a)) \\ &= b \oplus 0 = b. \end{aligned}$$

Agora, se $y_0 \in G$ é outa solução, então $y \oplus a \overset{\text{hip}}{=} y_0 \oplus a$. Assim, temos que:

$a \oplus y_0 = a \oplus (y_0 \oplus (a \ominus a)) \overset{i)}{=} (a \oplus (y_0 \oplus a)) \ominus a \overset{\text{hip}}{=} (a \oplus (y \oplus a)) \ominus a \overset{i)}{=} a \oplus (y \oplus (a \ominus a))$ $= a \oplus y$. Mas $a \oplus y = a \oplus y_0$ possui solução única, mostrando que $y = y_0$.

iii) Pela proposição 5.1.2 item x) e usando a lei do cancelamento à esquerda, segue que:

$gyr[a,b](\ominus b \ominus a) = \ominus(a \oplus b) \oplus (a \oplus (b \oplus (\ominus b \ominus a))) = \ominus(a \oplus b) \oplus (a \ominus a) = \ominus(a \oplus b)$.

iv) Suponhamos que G seja girocomutativo, ou seja, $a \oplus b = gyr[a,b](b \oplus a)$, $\forall a, b \in G$. Temos que:

$gyr[a,b](\ominus(\ominus a \ominus b)) = \ominus gyr[a,b](\ominus a \ominus b) \overset{iii)}{=} \ominus(\ominus(b \oplus a)) = b \oplus a = gyr[a,b](a \oplus b)$.

Pela bijetividade, segue que $\ominus(\ominus a \ominus b) = a \oplus b$, ou seja, $\ominus(a \oplus b) = \ominus a \ominus b$.

Reciprocamente, se $\ominus(a \oplus b) = \ominus a \ominus b$, então:

$a \oplus b \overset{iii)}{=} \ominus gyr[a,b](\ominus b \ominus a) = \ominus gyr[a,b](\ominus(b \oplus a)) = gyr[a,b](\ominus(\ominus(b \oplus a)) =$ $gyr[a,b](b \oplus a)$, mostrando que G é girocomutativo.

■

Proposição 5.2.4. *Se $(G, \oplus)$ é um girogrupo girocomutativo, então $(G, \oplus)$ é um K-laço.*

Demonstração: Da proposição 5.1.2 item vi) e do lema 5.2.3 item ii), segue que G é um laço. Pelo lema 5.2.3 ítens i) e iv), segue que G é um K-laço.

■

Para mostrarmos a recíproca da proposição acima, apresentamos dois lemas técnicos. Antes, veja que se $(\mathcal{L}, \cdot)$ é um laço, então, dados $x, \ell \in \mathcal{L}$, temos que as aplicações $\lambda_\ell(x) = \ell \cdot x$ e $\eta_\ell(x) = x \cdot \ell$ são bijetoras.

Lema 5.2.5. *Seja $(\mathcal{L}, \cdot)$ um laço e sejam $\alpha, \beta, \gamma : \mathcal{L} \to \mathcal{L}$ aplicações bijetoras tais que $\alpha(x) \cdot \beta(y) = \gamma(x \cdot y)$, $\forall x, y \in \mathcal{L}$. Se $\beta(1_\mathcal{L}) = 1_\mathcal{L}$, então $\alpha = \gamma$ e $(\alpha(1_\mathcal{L}) \cdot \beta(x)) \cdot \beta(y) = \alpha(1_\mathcal{L}) \cdot \beta(x \cdot y)$.*

Demonstração: Fazendo $a = \alpha(1_\mathcal{L})$ e $b = \beta(1_\mathcal{L})$, temos que:

$$\gamma(x) = \gamma(x \cdot 1_\mathcal{L}) = \alpha(x) \cdot \beta(1_\mathcal{L}) = \alpha(x) \cdot b \text{ e } \gamma(x) = \gamma(1_\mathcal{L} \cdot x) = \alpha(1_\mathcal{L}) \cdot \beta(x) = a \cdot \beta(x).$$

Logo, $\alpha(x) \cdot b = \gamma(x) = a \cdot \beta(x)$. Por hipótese, $b = 1_\mathcal{L}$, implicando que $\alpha = \gamma$ e $\alpha(x) = a \cdot \beta(x)$, ou melhor, $\alpha = \lambda_a \circ \beta$.

Portanto, $(\lambda_a \circ \beta)(x) \cdot \beta(y) = (\lambda_a \circ \beta)(x \cdot y)$, ou seja, $(a \cdot \beta(x)) \cdot \beta(y) = a \cdot \beta(x \cdot y)$, onde $a = \alpha(1_\mathcal{L})$.

■

Lema 5.2.6. *Se $(\mathcal{L}, \cdot)$ é um K-laço, então a aplicação precessão é um automorfismo.*

Demonstração: Note que, $\lambda_a^{-1} = \lambda_{a^{-1}}$ e ${\eta_a}^{-1} = \eta_{a^{-1}}$, pois $aa^{-1} = a^{-1}a = 1_\mathcal{L}$. Sendo $\mathcal{L}$ um Bol-laço, para cada $x, y \in \mathcal{L}$, temos que $(\lambda_a \eta_a)(x) \cdot \lambda_a^{-1}(y) = (a(xa))(a^{-1}y) = a(xy) = \lambda_a(x \cdot y)$. Logo, como $\gamma_{a,b}(1_\mathcal{L}) = 1_\mathcal{L}$ e sendo $(\lambda_{a \cdot b} \circ \lambda_a^{-1} \circ \lambda_b^{-1})(1_\mathcal{L}) = ((a \cdot b) \cdot (a^{-1} \cdot b^{-1})) = 1_\mathcal{L}$, segue do lema 5.2.5 que $((\underbrace{(a \cdot b) \cdot (a^{-1} \cdot b^{-1})}_{=1_\mathcal{L}}) \cdot \gamma_{a,b}(x)) \cdot \gamma_{a,b}(y) = (\underbrace{(a \cdot b) \cdot (a^{-1} \cdot b^{-1})}_{=1_\mathcal{L}}) \cdot \gamma_{a,b}(x \cdot y)$, como queríamos.

■

Proposição 5.2.7. *Se $(\mathcal{L}, \cdot)$ é um K-laço, então $(\mathcal{L}, \cdot)$ é um girogrupo girocomutativo.*

Demonstração: As condições i) e ii) da definição 5.1.1, seguem pelo fato de $\mathcal{L}$ ser um laço. Definindo o girador gerado por $a, b \in \mathcal{L}$ pela aplicação precessão, isto é, $gyr[a,b] := \gamma_{a,b}$, obtemos a lei da giroassociatividade à esquerda.

De acordo com o lema 5.2.5, dado $a \in \mathcal{L}$, a aplicação $\lambda_a : \mathcal{L} \to \mathcal{L}$ definida por $\lambda_a(x) = a \cdot x$ é bijetora. Decorre do fato de $\mathcal{L}$ ser um Bol-laço à esquerda a seguinte relação $\lambda_a \circ \lambda_b = \lambda_{a \cdot b} \circ \gamma_{a,b} \Rightarrow \gamma_{a,b} = \lambda_{a\cdot b}^{-1} \circ \lambda_a \circ \lambda_b$, onde $\gamma_{a,b}$ é um automorfismo e que $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. Restando mostrar que a aplicação precessão obedece a lei do laço à esquerda.

Se $a \cdot (b \cdot (a \cdot c)) = (a \cdot (b \cdot a)) \cdot c$, então $\gamma_{a,b} = \gamma_{a \cdot b, b}$, $\forall a, b, c \in \mathcal{L}$. É suficiente mostrar que $\gamma_{a,b\cdot a}^{-1} = \gamma_{b,a}$ e $\gamma_{a,b}^{-1} = \gamma_{a^{-1}, a\cdot b}$, pois $\gamma_{a,b} = (\gamma_{a^{-1},a\cdot b})^{-1} = (\gamma_{a\cdot b, a^{-1}\cdot(a\cdot b)}^{-1})^{-1} = \gamma_{a\cdot b, b}$. De fato: como $\gamma_{a,b\cdot a} = \lambda_{a\cdot(b\cdot a)}^{-1} \circ \lambda_a \circ \lambda_{b\cdot a}$ e $\gamma_{b,a} = \lambda_{b\cdot a}^{-1} \circ \lambda_b \circ \lambda_a$ e por ser um Bol-laço, temos que vale a igualdade $\lambda_a \circ \lambda_b \circ \lambda_a = \lambda_{a\cdot(b\cdot a)}$. Logo, é imediato que $\gamma_{b,a} \circ \gamma_{a,b\cdot a} = \gamma_{b\cdot a, a} \circ \gamma_{b,a} = \mathrm{id}$.

Temos também que $\gamma_{a^{-1},a\cdot b} = \lambda_{a^{-1}\cdot(a\cdot b)}^{-1} \circ \lambda_{a^{-1}} \circ \lambda_{a\cdot b} = \lambda_b^{-1} \circ \lambda_{a^{-1}} \circ \lambda_{a\cdot b}$, onde a outra igualdade é óbvia, mostrando que $\mathcal{L}$ é um girogrupo girocomutativo. ■

Podemos enriquecer essa ligação dizendo que todo B-laço é um girogrupo girocomutativo. De fato: note que, das proposições 5.2.4 e 5.2.5 segue que G é um K-laço, se, e somente se, G é um girogrupo girocomutativo. Por fim, um B-laço se, e somente se, G é um K-laço com a propriedade da raiz quadrada única.

Dessa forma, denominamos o B-laço $(B_n, \oplus)$ de *laço de Möbius*, ou seja, um girogrupo girocomutativo com a propriedade da raiz quadrada única, sendo seu girador definido por $gyr[a,b](c) = qcq^*$, $\forall a, b, c \in B_n$, onde $q = \frac{1+a\bar{b}}{\|1+a\bar{b}\|}$. Por essa razão, o laço de Möbius também é chamado de *girogrupo de Möbius*.

O girogrupo de Möbius é um dos principais objetos de estudo em **[19]**, ou laço de Möbius conforme vimos. Ungar(**[19]**) define a adição de Möbius no disco unitário de $\mathbb{R}^n$ pela equação (1) dada na introdução. Nossa abordagem, via álgebras de Clifford, produz uma fórmula equivalente, porém mais compacta, dada por (2), que é uma forma mais geral da adição de Möbius do disco unitário complexo dada na introdução desta dissertação.

Bibliografia

[1] Ahlfors, L. - Möbius transformations and Clifford numbers, in "Differencial Geometry and Complex Analysis"(I. Chavel and H. M. Farkas, Eds.), pg 65-73, Springer-Verlag, Berlin, 1985.

[2] Beardon, A.F. - The Geometry of Discrete Groups - Springer, 1991.

[3] Cannon, J; Playoust, C. - An Introduction to MAGMA - University of Sydney, Sydney - 1993.

[4] Ferreira, M. dos S. - Transformadas contínuas de onduleta na superfícies esférica - Universidade de Aviero (tese de doutorado), 2008.

[5] Ferreira, M. e Ren, G. - Möbius gyrogroups: A Clifford algebra approach - Journal of Algebra 328 (2011) 230-253, 2010.

[6] Foguel, T.; Kinyon, M.K.; Philips, J.D. - On twisted subgroups and Bol loops of odd order - Mathematics Subject Classification. 20N05 - 1991.

[7] Foguel, T. and Ungar, A. A. - Gyrogroups and the decomposition of groups into twisted subgroups and subgroups, Pacific J. Math 197 (2001) 1-11.

[8] Gallier, J. - Clifford Algebras, Clifford Groups and a Generalization of the Quaternions: The Pin an Spin groups - University of Pennsylvania, 2012.

[9] Hoffman, K. e Kunze, R.; Álgebra Linear, Livros Técnicos e Científicos, Rio de Janeiro, 1976.

[**10**] Kiechle, H. - Theory of K-loops, Lectures Notes in Mathematics 1778, Springer, 2002.

[**11**] Lawson, Jr. H. B. and Michelsohn, M.L. - Spin Geometry - Princeton University, 1989.

[**12**] Lawson J.; Clifford algebras, Möbius transformations, Vahlen matrices, and B-loops - Commentationes Mathematicae Universitatis Carolinae, Vol. 51(2010), No. 2, 319-331.

[**13**] Lima, E. L. - Cálculo Tensorial - IMPA, 2012.

[**14**] Lounesto, P. - Clifford Algebras and Spinors, Second Edition, 2001.

[**15**] Mendes, D. - Álgebras de Clifford e a fibração de Hopf - Universidade Estadual de Campinas (dissertação de mestrado) - 2012.

[**16**] Rocha, R. da - Spinors e Twistors no modelo paravetorial do espaço-tempo: uma formulação via álgebras de Clifford - Universidade Estadual de Campinas (dissertação de mestrado), 2001.

[**17**] Sousa, M. P. de - Álgebras de Clifford: uma introdução à Geometria Spin, Universidade Federal da Paraíba (dissertação de mestrado), 2013.

[**18**] Traesel, M. A. - Estruturas não-Associativas generalizadas em S^7 e álgebras de Clifford - Sandro André: Unviersidade Federal do ABC (dissertação de mestrado), 2009.

[**19**] Ungar, A. A. - Analytic Hiperbolic Geometry: Mathematical Foundations and Applications, World Scientific, 2005.

[20] Ungar, A. A. e Kasparian, A. - Lie Gyrovector Spaces, Journal of Geometry and Symmetry in Physics 1(2004) 3-53.

[21] Vieira, N.F.L. - Transformações de Möbius em $\mathbb{R}^{0,n}$ - Universidade de Aviero (dissertação de mestrado), 2005.

[22] Waterman, P. L. - Möbius transformations in several dimensions - Adv. Math. 101(1993) 87-113.