Relatório Científico

Relatório final de bolsa de Iniciação Científica

Título: Rotações, Quatérnions e Álgebras de Clifford

Aluno: Felipe V. Calderan

Orientador: Thiago Castilho de Mello

Período: 01/08/2018 à 31/07/2019

UNIFESP
UNIVERSIDADE FEDERAL DE SÃO PAULO
1933

Departamento de Ciência e Tecnologia
Universidade Federal de São Paulo
02 de Julho de 2019

Sumário

1 Resumo do estudado no período

Durante o período da Iniciação Científica, os seguintes conteúdos foram abordados:

- 01/08/18 até 31/10/18: Anéis (Cap. I de [1])
- 31/10/18 até 18/03/19: Grupos (Cap. V de [1])
- 18/03/19 até 12/04/19: Álgebra Linear (Cap. I à IX de [2])
- 12/04/19 até 28/05/19: Rotações no Espaço e Quatérnions (Cap. I e II de [3])
- 28/05/19 até 31/07/19: Álgebras de Clifford (Cap. III de [3])

Os encontros de orientador e orientando ocorreram semanalmente com duração de uma hora cada. Em período letivo esses encontros foram presenciais, enquanto em período de férias foram via Skype.

Além dos itens estudados, vale mencionar que atuei no *V Congresso Acadêmico Unifesp* como discente na modalidade *Iniciação Científica* no projeto *Números Quatérnions e Rotações no Espaço.*

Ressalto também que foi preciso estudar a teoria básica de álgebra linear, pois no momento que foi precisa no projeto, eu ainda não havia cursado a disciplina.

2 Anéis

2.1 Definições e Exemplos

Definição 2.1. *Um anel A é um conjunto não vazio munido de duas operações binárias $+$ e $\cdot$ (usualmente chamadas de adição e multiplicação), é denotado por $(A, +, \cdot)$ e satisfaz as seguintes propriedades:*

A.1) Adição é associativa: $\forall x, y, z \in A,\ (x + y) + z = x + (y + z)$.

A.2) Adição tem um elemento neutro: $\exists 0 \in A : \forall x \in A, 0 + x = x = x + 0$.

A.3) Na adição, existe um inverso por elemento: $\forall x \in A, \exists z \in A : x + z = 0 = z + x$.

A.4) Adição é comutativa: $\forall x, y \in A,\ x + y = y + x$

M.1) Multiplicação é associativa: $\forall x, y, z \in A,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

AM) Adição é distributiva relativamente à multiplicação: $\forall x, y, z \in A,\ x \cdot (y + z) = x \cdot y + x \cdot z$.

Anéis com identidade satisfazem:

M.2) Multiplicação tem um elemento neutro: $\exists 1 \in A : \forall x \in A, 1 \cdot x = x = x \cdot 1$.

E anéis comutativos satisfazem:

M.3) Multiplicação é comutativa: $\forall x, y \in A,\ x \cdot y = y \cdot x$.

Observação 2.1. *A condição A.2) garante a existência de um único elemento neutro.*

Tome dois elementos neutros para adição: 0 e $0'$. Então: $0 = 0 + 0' = 0'$.

Observação 2.2. *A condição A.3) garante a existência de um único inverso para um elemento x com respeito à adição.*

Tome y e y' inversos de x. Então: $y = y + 0 = y + (x + y') = (y + x) + y' = 0 + y' = y'$.

Esse único inverso será denotado por $-x$.

Observação 2.3. *O elemento neutro da adição* 0 *possui a seguinte propriedade:* $0 \cdot x = 0, \forall x$.

De fato: $0 \cdot x = (0 + 0)x = 0 \cdot x + 0 \cdot x$.

Definição 2.2. *Um anel comutativo com unidade $(D, +, \cdot)$ é chamado domínio de integridade, ou simplesmente domínio, se o produto de quaisquer dois elementos não nulos de D, é não nulo, ou seja: $\forall x, y \in D \setminus \{0\},\ x \cdot y \neq 0$.*

Um anel comutativo com unidade $(K, +, \cdot)$ é chamado corpo se todo elemento diferente de 0 de K possui um inverso com respeito à multiplicação: $\forall x \in K \setminus \{0\},\ \exists y \in K$ tal que $x \cdot y = 1$.

Exemplo 2.1.

a) Domínios: $(\mathbb{Z}, +, \cdot)$, $\mathbb{Z}[i] = (\{a + bi \mid a, b \in \mathbb{Z}\}, +, \cdot)$ (Com as operações usuais de soma e multiplicação de complexos)

b) Corpos: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

Definição 2.3. *Seja $(A, +, .)$ um anel comutativo com unidade. Dizemos que $I \subseteq A$ é um ideal de A se:*

I) $x + y \in I,\ \forall x, y \in I$.

II) $ax \in I,\ \forall a \in A$.

Definição 2.4. *Domínio Euclidiano $(D, +, \cdot, \varphi)$ é um domínio com uma função φ definida por: $\varphi : D \setminus \{0\} \longrightarrow \mathbb{N}$, tal que:*

I) $\forall a, b \in D,\ b \neq 0,\ \exists t, r \in D : a = bt + r$ com $\varphi(r) < \varphi(b)$ ou $r = 0$.

II) $\varphi(a) \leq \varphi(ab), \forall a, b \in D \setminus \{0\}$.

Exemplo 2.2. *Um domínio euclidiano notável é o anel dos inteiros munido de valor absoluto, ou seja: $(\mathbb{Z}, +, \cdot, ||)$. A demonstração do porquê esse anel satisfazer I e II pode ser encontrada em [1] na parte Domínios Euclidianos.*

Definição 2.5. *Seja um anel $(A, +, \cdot)$ e I_A um de seus ideais. Um anel quociente é definido por A/I_A.*

Exemplo 2.3. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

2.2 Homomorfismos de Anéis

Definição 2.6. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \odot)$. Uma função $f : A \longrightarrow B$ é um homomorfismo se respeita as estruturas de anéis, ou seja:*

I) $f(x + y) = f(x) \oplus f(y),\ x, y \in A$.

II) $f(x \cdot y) = f(x) \odot f(y),\ x, y \in A$.

III) $f(1_A) = 1_B$ (Para anéis com unidade)

Exemplo 2.4. *Homomorfismo Identidade:*

$Id : (A, +, \cdot) \longrightarrow (A, +, \cdot)$, tal que $Id(a) = a$.

Verifiquemos a satisfação da estrutura de anéis:

I) Por um lado temos: $Id(x + y) = x + y$. Pelo outro: $Id(x) + Id(y) = x + y$. Então obtemos que $Id(x + y) = Id(x) + Id(y)$.

II) Análogo a I, substituindo a operação de adição, pelo produto.

III) Temos imediatamente que: $Id(1) = 1$.

Definição 2.7. *O núcleo de um homomorfismo é:* $ker(f) := \{a \in A \mid f(a) = 0\} \subseteq A$.

Observação 2.4. f *é injetiva se e somente se* $ker(f) = \{0\}$.

Demonstração 2.1.

($\Leftarrow$): Suponha que $ker(f) \neq 0$. *Então* $\exists\, x \neq 0 : f(x) = 0 = f(0)$. *Logo,* f *não é injetiva.*

($\Rightarrow$): Suponha que $ker(f) = \{0\}$. *Seja* $f(x) = f(y)$, *então* $f(y) - f(x) = f(y - x) = 0$. *Por suposição, temos que* $y - x = 0$, *então* $x = y$. □

Definição 2.8. *A imagem de um homomorfismo é dada por:* $Im(f) := \{f(a) \mid a \in A\} \subseteq B$. *Vale ressaltar que* $(Im(f), +, \cdot)$ *é um anel chamado* Imagem de f. *A demonstração é simples e segue de argumentos usuais da teoria.*

Definição 2.9. *Um* isomorfismo de anéis *é um homomorfismo bijetivo. Se existe um isomorfismo entre dois anéis, dizemos que são* isomorfos.

2.3 Teorema dos Isomorfismos

Teorema 2.1. *Seja* $f : (A, +, \cdot) \longrightarrow (B, \oplus, \odot)$ *um homomorfismo de anéis. Então, a seguinte aplicação é um isomorfismo de anéis:*

$$\bar{f} : (A/ker(f), \underset{ker(f)}{\oplus}, \underset{ker(f)}{\odot}) \longrightarrow (Im(f), \oplus, \odot)$$

$$\bar{a} \longmapsto f(a)$$

Demonstração 2.2. *Primeiramente, verifiquemos que* $\bar{f}$ *está bem definida:*

De fato, $\bar{a}_1 = \bar{a}_2 \Rightarrow a_1 - a_2 \in ker(f) \Rightarrow f(a_1 - a_2) = 0$. *Como* f *é um homomorfismo, temos que:* $f(a_1 - a_2) = f(a_1) - f(a_2) \Leftrightarrow f(a_1) = f(a_2)$.

Agora, $\bar{f}$ *é sobrejetiva e é um homomorfismo, pois:*

$\bar{f}(\bar{a}_1 \underset{ker(f)}{\oplus} \bar{a}_2) = \bar{f}(\overline{a_1 + a_2}) = f(a_1 + a_2) = f(a_1) \oplus f(a_2) = \bar{f}(\bar{a}_1) \oplus \bar{f}(\bar{a}_2)$.

De maneira similar podemos mostrar que $\bar{f}(\bar{a}_1 \odot_{ker(f)} \bar{a}_2) = \bar{f}(\bar{a}_1) \odot \bar{f}(\bar{a}_2)$.

Finalmente, temos que:

$ker(\bar{f}) = \{\bar{a} \in (A/ker(f) \mid f(a) = 0\} = \{\bar{a} \in (A/ker(f)) \mid a \in ker(f)\} = \{\bar{0}\}$

Assim concluímos que $\bar{f}$ *é injetiva.* □

3 Grupos

3.1 Definições e Exemplos

Definição 3.1. *Um grupo G é munido de uma operação binária $\cdot$, é denotado por $(G, \cdot)$ e satisfaz as seguintes propriedades:*

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

II) Possui um elemento neutro: $\exists e \in G : \forall a \in G, e \cdot a = a = a \cdot e$.

III) Todo elemento possui um inverso: $\forall a \in G, \exists b \in G : a \cdot b = e = b \cdot a$.

Se além das 3 anteriores, um grupo satisfaz a seguinte propriedade:

IV) A operação é comutativa: $\forall a, b \in G,\ a \cdot b = b \cdot a$.

Ele é chamado de *grupo abeliano.*

Observação 3.1. *O elemento neutro é único.*

Tome $e, e' \in G$ elementos neutros de G, então: $e = e \cdot e' = e'$.

Observação 3.2. *O elemento inverso é único.*

Tome $a \in G$ e $b, b' \in G$ inversos de a. Então: $b = b \cdot e = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = e \cdot b' = b'$.

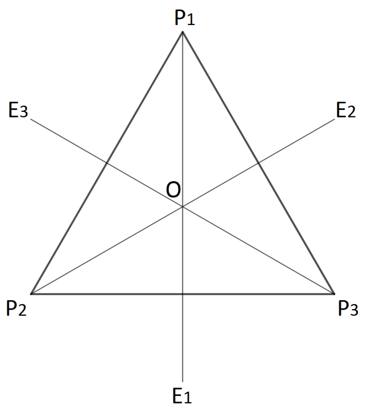
Denotaremos o inverso de a por a^{-1}.

Exemplo 3.1. $(\mathbb{Z}/n\mathbb{Z}, \underset{n}{\oplus})$ *é um grupo abeliano finito com n elementos.*

3.2 Grupo das simetrias espaciais de um triângulo equilátero

Grupos de permutações possuem grande importância em Teoria de Grupos. Apesar de existir vários exemplos clássicos desses, nesse relatório será abordado mais detalhadamente somente o grupo $S_\triangle$, ou grupo das simetrias espaciais de um triângulo equilátero.

Seja $P_1P_2P_3$ um triângulo equilátero. Coloque o centro de gravidade na origem O do espaço e chame de $E_1E_2E_3$ as retas do espaço passando pelas medianas do triângulo.



As transformações espaciais que preservam o triângulo são:

- $id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}$: as rotações planas centradas em O, no sentido anti-horário, de ângulos 0, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$, respectivamente.
- R_1, R_2, R_3: as rotações espaciais de ângulo π com eixos E_1, E_2, E_3, respectivamente.

Assim, temos que $S_\triangle := \{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$ com composição de funções é um grupo.

Note que **não** é abeliano, pois um contra-exemplo é: $R_1 \circ R_2 = R_{\frac{2\pi}{3}} \neq R_2 \circ R_1 = R_{\frac{4\pi}{3}}$.

3.3 Subgrupos

Definição 3.2. *Seja H um subconjunto não vazio do grupo G. Então $H < G$ (H é subgrupo de G) se e somente se as seguintes condições são satisfeitas:*

I) $h_1 \cdot h_2 \in H, \forall h_1, h_2 \in H.$

II) $h^{-1} \in H, \forall h \in H.$

Exemplo 3.2. $\{id, R_1\}$ *é subgrupo de* $S_{\triangle}$. *Verifiquemos a satisfação das condições:*

I) $id \cdot id = id; \;\; id \cdot R_1 = R_1; \;\; R_1 \cdot id = R_1; \;\; R_1 \cdot R_1 = id.$

Então, como todos os resultados pertencem à $\{id, R_1\}$, I é satisfeita.

II) $id^{-1} = id; \;\; R_1^{-1} = R_1$

Como os inversos pertencem à $\{id, R_1\}$, II é satisfeita.

Definição 3.3.

a) Se $g \in G$, então o subgrupo gerado por g é $\langle g \rangle = \{g^t \mid t \in \mathbb{Z}\}$

b) Se S é um subconjunto não vazio de G, então:

$\langle S \rangle = \{a_1 a_2 \cdots a_n \mid n \in \mathbb{N}, a_i \in S \text{ ou } a_i \in S^{-1}\} < G$ *(subgrupo gerado por S).*

c) Se um grupo é gerado por um único elemento, ele é um grupo cíclico.

Definição 3.4. *O centro de um grupo G é dado por: $Z(G) = \{x \in G \mid xg = gx, \forall g \in G\}$.*

Note que $Z(G) < G$ e G é abeliano $\Leftrightarrow Z(G) = G$.

Exemplo 3.3. *Tome o grupo $(\mathbb{Z}/n\mathbb{Z}, \underset{n}{\oplus})$. Imediatamente temos que $Z(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. Com isso, confirmamos que $(\mathbb{Z}/n\mathbb{Z}, \underset{n}{\oplus})$ é abeliano.*

Definição 3.5. *O subgrupo dos comutadores de G é dado por: $G' = \big\langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \big\rangle$.*

Vale ressaltar que G é abeliano $\Leftrightarrow G' = \{e\}$.

Exemplo 3.4. *Como o grupo $(\mathbb{Z}/n\mathbb{Z}, \underset{n}{\oplus})$ é abeliano, seu subgrupo dos comutadores é $\{e\}$.*

3.4 Classes Laterais e Teorema de Lagrange

Definição 3.6. *Seja G um grupo e $H < G$. Sobre G, defina as seguintes relações de equivalência:*

- $y \underset{E}{\sim} x \Leftrightarrow \exists h \in H : y = xh.$
- $y \underset{D}{\sim} x \Leftrightarrow \exists h \in H : y = hx.$

Assim, temos que $xH = \{y \in G \mid y \underset{E}{\sim} x\}$ *é a* classe lateral à esquerda.

Analogamente, $Hx = \{y \in G \mid y \underset{D}{\sim} x\}$ *é a* classe lateral à direita.

Definição 3.7. *Seja G um grupo e $H < G$.*

A cardinalidade do conjunto das classes laterais (seja à esquerda, ou à direita) é o índice *de H em G. Esse índice é denotado por $(G : H)$.*

Proposição 3.1. *Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H.*

Demonstração 3.1. *A função abaixo é claramente uma bijeção:*

$$H \longrightarrow xH$$

$$h \longmapsto xh$$

$\square$

Teorema 3.1 (Teorema de Lagrange)**.** *Seja G um grupo finito e $H < G$. Então $|G| = |H|(G : H)$. Note que a ordem e o índice de H dividem a ordem de G.*

Demonstração 3.2. *Considerando a relação de equivalência à esquerda $\underset{E}{\sim}$ em G, obtemos uma partição de G em classes de equivalência. A proposição anterior mostra que em cada uma dessas classes temos $|H|$ elementos. Como, por definição, o número de classes é $(G : H)$, temos a igualdade $|G| = |H|(G : H)$.* $\square$

3.5 Subgrupos Normais e Grupos Quocientes

Seja G um grupo e seja H um subgrupo de G. Queremos ver se a operação de G induz de maneira natural uma operação sobre o conjunto das classes laterais à esquerda de H em G, ou seja, se a operação $(xH, yH) \longrightarrow xyH$ é bem definida, no sentido de não depender da escolha dos representantes x e y.

Dados $x, y \in G$ e $h, k \in H$ arbitrários, então x e xh são representantes da mesma classe xH e, y e yk são representantes da mesma classe yH. Assim, a operação induzida sobre as classes laterais à esquerda é bem definida se e somente se $xyH = xhykH, \forall x, y \in G, \forall h, k \in H$. Logo, se e somente se $y^{-1}x^{-1}xyH = y^{-1}x^{-1}xhykH$, ou seja, $H = y^{-1}hyH, \forall h, k \in H$. Finalmente, se e somente se $ghg^{-1} \in H, \forall g \in G, \forall h \in H$.

Proposição 3.2. *Seja H um subgrupo de um grupo G. As afirmações seguintes são equivalentes:*

I) a operação induzida sobre as classes laterais à esquerda de H em G é bem definida.

II) $gHg^{-1} \subseteq H, \forall g \in G$.

III) $gHg^{-1} = H, \forall g \in G$.

IV) $gH = Hg, \forall g \in G$.

Demonstração 3.3. *I $\Leftrightarrow$ II já foi feito. III $\Leftrightarrow$ IV é óbvio. III $\Rightarrow$ II é óbvio.*

II $\Rightarrow$ III: Suponhamos que $gHg^{-1} \subseteq H, \forall g \in G$. Queremos mostrar que $H \subseteq gHg^{-1}, \forall g \in G$. Sejam então $h \in H$ e $g \in G$. Temos: $h = g(g^{-1}hg)g^{-1} \in g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$. $\square$

Definição 3.8. *Um subgrupo H é um subgrupo normal de G ($H \lhd G$) se ele satisfaz as afirmações equivalentes da proposição anterior. Neste caso, as classes laterais à esquerda de H são iguais às da direita. Vamos chamá-las de classes laterais de H.*

Exemplo 3.5. *Vamos mostrar que $Z(G) \lhd G$.*

Primeiramente, mostremos que é um subgrupo:

I) Sejam $a, b \in Z(G)$. Sabemos que $\forall g : ag = ga$ e $bg = gb$, logo $gab = agb = abg$ e, portanto, $ab \in Z(G)$.

II) Tome $h \in Z(G)$. Sabendo que $\forall g \in G : gh = hg$, portanto:

$$h^{-1}(gh)h^{-1} = h^{-1}(hg)h^{-1} \Leftrightarrow h^{-1}g(hh^{-1}) = (h^{-1}h)gh^{-1} \Leftrightarrow$$

$$\Leftrightarrow h^{-1}(ge) = (eg)h^{-1} \Leftrightarrow h^{-1}g = gh^{-1}$$

Logo, $h^{-1} \in Z(G)$.

Agora, para mostrar que é normal, basta escolher $h \in Z(G)$ e notar que:

$$\forall g \in G,\ ghg^{-1} = gg^{-1}h = h \in Z(G)$$

Definição 3.9. *Seja G um grupo e $H \lhd G$. O conjunto de suas classes laterais, com a operação induzida de G é um grupo chamado de grupo quociente de G por H e é denotado por G/H.*

Exemplo 3.6. *G/G' é um grupo quociente abeliano.*

3.6 Homomorfismos de Grupos

Definição 3.10. *Sejam $(G, \cdot)$ e $(\mathcal{G}, \times)$ dois grupos. a função $f : G \longrightarrow \mathcal{G}$ é um homomorfismo se ela satisfaz:*

$$f(a \cdot b) = f(a) \times f(b),\ \forall a, b \in G$$

Exemplo 3.7. *Vamos mostrar que $I_g : G \longrightarrow G,\ I_g(x) = gxg^{-1}$ é um homomorfismo.*

Por um lado temos que $I_g(a \cdot b) = gabg^{-1}$.

Pelo outro temos: $I_g(a) \cdot I_g(b) = gag^{-1}gbg^{-1} = gaebg^{-1} = gabg^{-1}$.

Assim, temos que $I_g(a \cdot b) = I_g(a) \cdot I_g(b)$.

Definição 3.11. *O núcleo de um homomorfismo é: $ker(f) := \{x \in G \mid f(x) = e_{\mathcal{G}}\}$.*

Proposição 3.3. *$ker(f) \lhd G$*

Demonstração 3.4. *Primeiramente mostraremos que $ker(f) < G$. Dados $x, y \in ker(f)$, temos:*

$f(x \cdot y) = f(x) \times f(y) = e_{\mathcal{G}} \times e_{\mathcal{G}} = e_{\mathcal{G}}$

$f(x^{-1}) = f(x)^{-1} = e_{\mathcal{G}}^{-1} = e_{\mathcal{G}}$.

Portanto, $ker(f) < G$. Para provar que $ker(f) \lhd G$ devemos mostrar que $gxg^{-1} \in ker(f), \forall g \in G$ e $\forall x \in ker(f)$.

De fato, temos: $f(gxg^{-1}) = f(g) \times f(x) \times f(g^{-1}) = f(g) \times e_{\mathcal{G}} \times f(g)^{-1} = f(g) \times f(g)^{-1} = e_{\mathcal{G}}$ $\square$

Definição 3.12. *A imagem é dada por:* $Im(f) = \{y \in \mathcal{G} \mid y = f(g) \text{ para algum } g \in G\}$. *Além disso, é um subgrupo de* $\mathcal{G}$. *A demonstração é simples e segue de argumentos usuais da teoria.*

Definição 3.13. *Um isomorfismo de grupos é um homomorfismo bijetivo. Se existe um isomorfismo entre dois grupos, dizemos que são isomorfos.*

3.7 Teorema dos Isomorfismos

Teorema 3.2. *Seja* $f : (G, \cdot) \longrightarrow (\mathcal{G}, \times)$ *um homomorfismo de grupos. Então,*

$$\bar{f} : \frac{G}{ker(f)} \longrightarrow f(G)$$

$$gker(f) \longmapsto f(g)$$

é um isomorfismo.

As funções

$$\{subgrupos\ de\ G \supseteq ker(f)\} \longleftrightarrow \{subgrupos\ de f(G)\}$$

$$H \longrightarrow f(H)$$

$$f^{-1}(\mathcal{H}) \longleftarrow \mathcal{H}$$

são bijeções inversas uma da outra. Além disso, estas bijeções levam subgrupos normais em subgrupos normais, isto é:

I) $H \lhd G \Rightarrow f(H) \lhd f(G)$. *II)* $\mathcal{H} \lhd f(G) \Rightarrow f^{-1}(\mathcal{H}) \lhd G$.

Demonstração 3.5. *A demonstração do teorema não será abordada nesse relatório por conta de sua extensão, mas pode ser encontrada em [1] na parte Homomorfismos de Grupos.* $\square$

4 Rotações

4.1 Rotações no Plano

Seja a base canônica $\{e_1, e_2\}$ do plano. Para rotacionar um vetor por um ângulo θ no plano em torno da origem, usaremos uma função R_θ tal que:

$R_\theta(e_1) = (cos\theta)e_1 + (sen\theta)e_2$

$R_\theta(e_2) = -(sen\theta)e_1 + (cos\theta)e_2$

É fácil verificar que R_θ é uma transformação linear, assim podemos utilizar a seguinte representação por matriz:

$$R_\theta = \begin{bmatrix} cos\theta & -sen\theta \\ sen\theta & cos\theta \end{bmatrix}$$

Definição 4.1. *São chamados $SO(n)$ os grupos das matrizes ortogonais (ou seja, matrizes cuja inversa é igual à sua transposta) $n \times n$ de determinante unitário.*

A matriz R_θ é ortogonal e possui determinante unitário, então podemos classificá-la como membro do grupo $SO(2)$.

De fato, todas as rotações no plano pertencem ao $SO(2)$, vide [3].

Agora, veremos como é possível codificar rotações no plano através dos *Números Complexos.*

Definição 4.2. *O conjunto dos números complexos, usualmente denotado por $\mathbb{C}$, é dado por $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}$ **e** $i^2 = -1\}$*

Observação 4.1. *Um número complexo pode ser visto como o vetor no plano $z = (a, b)$. Este plano é gerado pela base canônica $1 = (1, 0)$ e $i = (0, 1)$.*

Definição 4.3. *A norma de um número complexo z é dada por $|z| = \sqrt{a^2 + b^2}$. Esse valor é o comprimento do vetor $z = (a, b)$ no plano.*

Definição 4.4. *O argumento de um número complexo é o ângulo θ formado entre o vetor z e o eixo 1, onde $\theta = tan^{-1}(\frac{a}{b})$.*

Definição 4.5. *A soma de dois números complexos z e w é: $z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$.*

Definição 4.6. *A multiplicação de dois números complexos z e w é: $z \cdot w = (a+bi)\cdot(c+di) = (ac - bd) + (ad + bc)i$.*

Proposição 4.1. *Os números complexos com essas operações formam um corpo.*

Demonstração 4.1. *Previamente no relatório, foi abordado que $\mathbb{C}$ forma um corpo. Além disso, é fácil verificar que $\mathbb{C}$ é um anel comutativo com unidade. Um $z \in \mathbb{C}$ não nulo possui inverso dado por $z^{-1} = \frac{\bar{z}}{|z|^2}$, onde $\bar{z} = a - bi$ é o conjugado de $z = a + bi$.* □

Definição 4.7. *Os números complexos possuem um subconjunto notável chamado números complexos unimodulares.*

Esse subconjunto é dado por: $U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$, também denotado por $\mathbb{S}^1$, pois é geometricamente equivalente à circunferência no plano de raio 1.

Logo, temos que se $z \in \mathbb{S}^1$, então $z = cos\theta + isen\theta$.

Proposição 4.2. *$\mathbb{S}^1$ é um subgrupo de $(\mathbb{C}^*, \cdot)$.*

Demonstração 4.2. *Seja $z \in \mathbb{S}^1$.*

Note que $z \in \mathbb{S}^1 \Leftrightarrow |z| = 1$. Assim, como $z.z^{-1} = 1$, temos: $1 = |z||z^{-1}| = 1.|z^{-1}| = |z^{-1}|$.

Além disso, se $w \in \mathbb{S}^1$, então $|zw^{-1}| = |z||w^{-1}| = |z||w| = 1$

Portanto, $zw^{-1} \in \mathbb{S}^1$, mostrando que $\mathbb{S}^1 < (\mathbb{C}^*, \cdot)$. □

Definição 4.8. *Podemos definir a seguinte aplicação linear:*

$$\begin{array}{cccc} \varphi : & \mathbb{C} & \longrightarrow & M_2(\mathbb{R}) \\ & a + bi & \longmapsto & \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \end{array}$$

Restringindo a aplicação acima aos complexos unimodulares, temos:

$$\begin{array}{cccc} \phi: & \mathbb{S}^1 & \longrightarrow & M_2(\mathbb{R}) \\ & cos\theta + isen\theta & \longmapsto & \begin{bmatrix} cos\theta & -sen\theta \\ sen\theta & cos\theta \end{bmatrix} \end{array}$$

Teorema 4.1. *A aplicação ϕ corresponde a um isomorfismo entre os grupos $\mathbb{S}^1$ e $SO(2)$.*

Demonstração 4.3. *Sejam $z, w \in \mathbb{S}^1$. Primeiramente, precisamos mostrar que ϕ é um homomorfismo de grupos. Para isso, é necessário mostrar que $\phi(z \cdot w) = \phi(z) \cdot \phi(w)$:*

Por um lado temos que:

$$\phi(z \cdot w) = \phi((a + bi) \cdot (c + di)) = \phi((ac - bd) + (ad + bc)i) = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix}$$

Pelo outro:

$$\phi(z) \cdot \phi(w) = \phi(a + bi) \cdot \phi(c + di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{bmatrix}$$

Portanto $\phi(z \cdot w) = \phi(z) \cdot \phi(w)$.

Agora precisamos verificar que esse homomorfismo é bijetivo.

Vamos mostrar primeiro a injetividade.

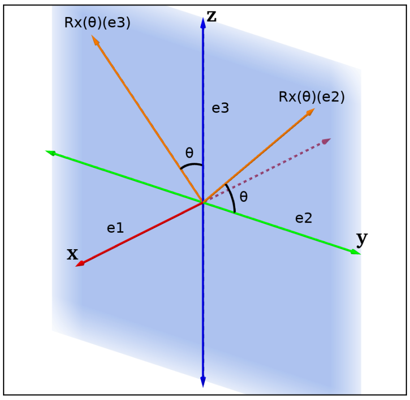
Sejam $z = a+bi, z' = a'+b'i \in \mathbb{C}$. Agora suponha que $\phi(z) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} a' & -b' \\ b' & a' \end{bmatrix} = \phi(z')$.

Como as matrizes serão iguais se e somente se cada elemento for igual, temos que $a = a'$ e $b = b'$, implicando que $z = z'$ e que ϕ é injetiva.

Para a sobrejetividade, basta ver que se $A \in SO(2)$, então $\exists \theta \in \mathbb{R} : A = R_\theta$. Essa matriz, por vez, corresponde a $\phi(cos\theta + isen\theta)$. $\square$

4.2 Rotações no Espaço

Seja a base canônica $\{e_1, e_2, e_3\}$ do espaço. Consideremos a rotação desses vetores em torno do eixo O_x por um ângulo θ.



Vamos determinar a matriz de rotação R_x:

$R_x(\theta)(e_1) = e_1 + 0e_2 + 0e_3$

$R_x(\theta)(e_2) = 0e_1 + (cos(\theta))e_2 + (sen(\theta))e_3$

$R_x(\theta)(e_3) = 0e_1 + (sen(\theta))(-e_2) + (cos(\theta))e_3$

Dessa forma obtemos a matriz:

$$R_x(\theta) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & cos(\theta) & -sen(\theta) \\ 0 & sen(\theta) & cos(\theta) \end{bmatrix}$$

Fazendo o mesmo procedimento para O_y e O_z, temos:

$$R_y(\theta) = \begin{bmatrix} cos(\theta) & 0 & sen(\theta) \\ 0 & 1 & 0 \\ -sen(\theta) & 0 & cos(\theta) \end{bmatrix} \qquad R_z(\theta) = \begin{bmatrix} cos(\theta) & -sen(\theta) & 0 \\ sen(\theta) & cos(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Definição 4.9. *É fácil verificar que essas matrizes são elementos do $SO(3)$, assim como a matriz de rotação no plano era elemento de $SO(2)$.*

Definição 4.10. *Para realizarmos uma rotação em torno de um eixo qualquer, que não seja necessariamente um dos eixos coordenados, consideraremos um vetor unitário $\overrightarrow{n} \in \mathbb{R}^3$ chamado eixo de rotação. Esse eixo pode ser escrito em coordenadas esféricas como:*

$$\overrightarrow{n} = \begin{bmatrix} sen(\theta)cos(\varphi) \\ sen(\theta)sen(\varphi) \\ cos(\theta) \end{bmatrix}$$

Observação 4.2. *O vetor $\overrightarrow{n}$ também pode ser escrito como $R_z(\varphi) \circ R_y(\theta)(e_3)$*

Demonstração 4.4.

$$R_z(\varphi) \circ R_y(\theta)(e_3) = \begin{bmatrix} cos(\varphi) & -sen(\varphi) & 0 \\ sen(\varphi) & cos(\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} cos(\theta) & 0 & sen(\theta) \\ 0 & 1 & 0 \\ -sen(\theta) & 0 & cos(\theta) \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right) =$$

$$= \begin{bmatrix} cos(\varphi) & -sen(\varphi) & 0 \\ sen(\varphi) & cos(\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} sen(\theta) \\ 0 \\ cos(\theta) \end{bmatrix} = \begin{bmatrix} sen(\theta)cos(\varphi) \\ sen(\theta)sen(\varphi) \\ cos(\theta) \end{bmatrix} = \overrightarrow{n}$$

□

Assim obtemos um procedimento padrão para escrevermos uma rotação ao redor do eixo $\overrightarrow{n}$ com um ângulo ψ, fazendo uso apenas das matrizes R_x, R_y e R_z:

- Fazer $\overrightarrow{n}$ coincidir com e_3, desfazendo as rotações que determinam $\overrightarrow{n}$.
- Rotacionar ao redor de O_z pelo ângulo ψ.
- Devolver $\overrightarrow{n}$ através das rotações que o determinam.

Em outras palavras:

$$R_{\overrightarrow{n},\psi} = R_z(\varphi) \circ R_y(\theta) \circ R_z(\psi) \circ R_y(-\theta) \circ R_z(-\varphi)$$

Assim, é claro que toda rotação no espaço é elemento de $SO(3)$. Por isso, $SO(3)$ é também conhecido como grupo das rotações espaciais.

5 Números Quatérnions

5.1 Estrutura Algébrica

Definição 5.1. *Os conjunto dos quatérnions, denotado por $\mathbb{H}$ é dado por:*

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$$

Ou seja, é um espaço vetorial cuja base é $\{1, i, j, k\}$, munido de um produto, e que satisfaz a regra acima, obedecendo a distributividade em relação à adição.

Observação 5.1. *Por satisfazer $i^2 = j^2 = k^2 = ijk = -1$, percebemos que $\mathbb{H}$ é uma álgebra não comutativa. A seguinte tabela resume as relações de multiplicações:*

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Definição 5.2. *O conjugado de $q = a + bi + ck + dk \in \mathbb{H}$ é dado por: $\bar{q} = a - bi - cj - dk$. Temos algumas propriedades notáveis com relação ao conjugado:*

I) $\overline{p+q} = \bar{p} + \bar{q}$ *II)* $\overline{pq} = \bar{q}\bar{p}$ *III)* $\bar{\bar{q}} = q$

As demonstrações para essas 3 propriedades são triviais.

Definição 5.3. *A norma de $q = a + bi + ck + dk \in \mathbb{H}$ é dada por: $\|q\| = \sqrt{a^2 + b^2 + c^2 + d^2}$ e possui as seguintes propriedades:*

I) $\|q\|^2 = q\bar{q} = \bar{q}q$ *II)* $\|pq\|^2 = \|p\|^2\|q\|^2$, $p \in \mathbb{H}$ *III)* $q^{-1} = \frac{1}{\|q\|^2}\bar{q}$, $q \neq 0$

Demonstração 5.1. *Sejam $p, q \in \mathbb{H}$.*

I) A demonstração é trivial

II) $\|pq\|^2 = (pq)(\overline{pq}) = pq\bar{q}\bar{p} = p\|q\|^2\bar{p} = p\bar{p}\|q\|^2 = \|p\|^2\|q\|^2$

III) $q \cdot \dfrac{1}{\|q\|^2}\bar{q} = \dfrac{q\bar{q}}{\|q\|^2} = \dfrac{\|q\|^2}{\|q\|^2} = 1$ □

Observação 5.2. *Com as propriedades acima, podemos ver que $\mathbb{H}$ é um anel que satisfaz todas as propriedades de corpo, exceto a comutatividade da multiplicação. Um anel com tais propriedades é chamado de* anel com divisão.

Observação 5.3. *Os quatérnions unitários podem ser interpretados geometricamente como a esfera tridimensional no $\mathbb{R}^4$*

5.2 Conjugação

Definição 5.4. *Seja $q \in \mathbb{H}^*$ (quatérnions não nulos). Definimos a conjugação por q como a aplicação:*

$$\begin{array}{rccc} Ad_q : & \mathbb{H} & \longrightarrow & \mathbb{H} \\ & r & \longmapsto & qrq^{-1} \end{array}$$

Proposição 5.1. *Sejam $p, q \in \mathbb{H}^*$. Então:*

I) $Ad_q(\lambda r + s) = \lambda Ad_q(r) + Ad_q(s)$, $\forall t, s \in \mathbb{H}, \forall \lambda \in \mathbb{R}$.

II) $Ad_q(rs) = Ad_q(r)Ad_q(s, \forall r, s \in \mathbb{H}$.

III) $Ad_p \circ Ad_q = Ad_{pq}$.

IV) $Id_{\mathbb{H}} = Ad_1$.

V) $(Ad_q)^{-1} = Ad_{q^{-1}}$

Demonstração 5.2. *Sejam $r, s \in \mathbb{H}$ e $\lambda \in \mathbb{R}$, então:*

I)$Ad_q(\lambda r + s) = q(\lambda r + s)q^{-1} = q\lambda rq^{-1} + qsq^{-1} = \lambda qrq^{-1} + qsq^{-1} = \lambda Ad_q(r) + Ad_q(s)$.

II) $Ad_q(rs) = qrsq^{-1} = qrq^{-1}qsq^{-1} = Ad_q(r)Ad_q(s)$.

III) $Ad_p \circ Ad_q(r) = Ad_p(qrq^{-1}) = p(qrq^{-1})p^{-1} = (pq)rq^{-1}p^{-1} = (pq)r(pq)^{-1} = Ad_{pq}(r)$.

IV) Para qualquer $r \in \mathbb{H}$ temos $Ad_1(r) = 1r1^{-1} = 1r1 = r \Rightarrow Ad_1 = Id_{\mathbb{H}}$.

V) $Ad_q \circ Ad_{q^{-1}} = Ad_{qq^{-1}} = Ad_1 = Id_{\mathbb{H}}$ e $Ad_q^{-1} \circ Ad_q = Ad_{q^{-1}q} = Ad_1 = Id_{\mathbb{H}}$

Assim temos que $Ad_{q^{-1}} = (Ad_q)^{-1}$. □

Definição 5.5. *O grupo das transformações lineares inversíveis de um espaço vetorial $\mathbb{V}$ é denotado por $GL(\mathbb{V})$. Se $\mathbb{V}$ é um espaço vetorial de dimensão n sobre um corpo K, temos um isomorfismo de grupos entre $GL(\mathbb{V})$ e $GL_n(K)$, o grupo das matrizes $n \times n$ com coeficientes em K que são invertíveis. Esse isomorfismo é tomado fixando-se uma base de $\mathbb{V}$ e considerando a matriz de cada transformação linear.*

Os itens *I*, *II* e *V* da proposição acima dizem que $\forall q \in \mathbb{H}^*$, a aplicação Ad_q é um automorfismo da álgebra dos quatérnions. Cada Ad_q é uma aplicação linear inversível em $\mathbb{H}$, logo, é um elemento do grupo das transformações lineares inversíveis $GL(\mathbb{H})$. Assim, podemos considerar a aplicação:

$$\begin{array}{rccc} Ad : & \mathbb{H}^* & \longrightarrow & GL(\mathbb{H}) \\ & q & \longmapsto & Ad_q \end{array}$$

Definição 5.6. *Um quatérnion* $p \in \mathbb{H}$ *é dito puro se sua parte real for igual a zero, ou seja,* $p = xi + yj + zk$*.*

Proposição 5.2. *Podemos identificar* $\mathbb{R}^3$ *como o subespaço dos quatérnions puros. Para tornarmos mais precisa essa identificação, temos o seguinte resultado:*

A aplicação abaixo é injetiva.

$$\begin{array}{cccc} \iota: & \mathbb{R}^3 & \longrightarrow & \mathbb{H} \\ & (x, y, z) & \longmapsto & xi + yj + zk \end{array}$$

Demonstração 5.3. *Sejam* $(x, y, z), (x', y', z') \in \mathbb{R}^3$*. Agora suponha que* $\iota(x, y, z) = xi + yj + zk = x'i + y'j + z'k = \iota(x', y', z')$*.*

Como os quatérnions serão iguais se e somente se os coeficientes correspondentes forem iguais, temos que $x = x'$*,* $y = y'$ *e* $z = z'$*. Assim, temos que* ι *é injetiva.*

Proposição 5.3. *Seja* $q \in \mathbb{H}^*$ *e* w *um quatérnion puro. Então* $Ad_q(w)$ *também é um quatérnion puro.*

Demonstração 5.4. *Sejam* $q = a + bi + cj + dk$ *e* $w = xi + yj + zk$*. Então:*

$$qwq^{-1} = qw\frac{\bar{q}}{\|q\|^2} = \frac{1}{\|q\|^2}(a + bi + cj + dk)(xi + yj + zk)(a - bi - cj - dk) =$$

$$= \frac{1}{\|q\|^2}((-bx - cy - dz) + (ax + cz - dy)i + (ay + dx - bz)j + (az + by - cx)k)(a - bi - cj - dk) =$$

$$= \frac{1}{\|q\|^2}(((-bx - cy - dz)a + (ax + cz - dy)b + (ay + dx - bz)c + (az + by - cx)d) +$$

$$+ (\cdots)i + (\cdots)j + (\cdots)k) =$$

$$= \frac{1}{\|q\|^2}((\cdots)i + (\cdots)j + (\cdots)k)$$

Finalmente, como a parte real de $Ad_q(w)$ *é zero, então é um quatérnion puro.*

Com isso, podemos fazer a co-restrição da aplicação Ad para:

$$\begin{array}{cccc} Ad: & \mathbb{H}^* & \longrightarrow & GL_3(\mathbb{R}) \\ & q & \longmapsto & Ad_q \end{array}$$

Esse grupo de transformações lineares inversíveis em $\mathbb{R}^3$ são as transformações lineares no subespaço dos quatérnions puros.

5.3 Rotações por Quatérnions

Teorema 5.1. *Restringindo o domínio de* Ad *à* $\mathbb{S}^3$*, temos a aplicação:*

$$\begin{array}{cccc} Ad: & \mathbb{S}^3 & \longrightarrow & GL_3(\mathbb{R}) \\ & q & \longmapsto & Ad_q \end{array}$$

Então Ad é um homomorfismo de grupos cuja imagem é exatamente $SO(3)$. O núcleo desse homomorfismo é $\{-1, 1\}$, assim, pelo teorema do isomorfismo, o grupo $SO(3)$ é o quociente do grupo $\mathbb{S}^3$ por $\{-1, 1\}$.

Dessa forma, cada quatérnion unitário q dá origem a um elemento de $SO(3)$, ou seja, uma rotação no espaço $\mathbb{R}^3$, representado agora pelos quatérnions puros. Queremos agora identificar qual o eixo $\overrightarrow{n}$ e qual o ângulo ψ dessa rotação.

Primeiramente, considere $q = a + bi + cj + dk \in \mathbb{S}^3$.

Observação 5.4. *O eixo de rotação $\overrightarrow{n}$ é dado por: $\overrightarrow{n} = \frac{1}{\sqrt{1-a^2}}(bi + cj + dk)$.*

Observação 5.5. *O ângulo de rotação ψ é dado por $\psi = 2cos^{-1}a$.*

Portanto, temos que:

$$q = cos\left(\frac{\psi}{2}\right) + sen\left(\frac{\psi}{2}\right)\overrightarrow{n}$$

Há uma forma simples de verificar que esse é realmente nosso q inicial:

$$cos\left(\frac{\psi}{2}\right)^2 + sen\left(\frac{\psi}{2}\right)^2 = 1 \underset{cos\left(\frac{\psi}{2}\right)=a}{\Leftrightarrow} sen\left(\frac{\psi}{2}\right) = \sqrt{1-a^2}$$

Então:

$$q = a + \sqrt{1-a^2}\overrightarrow{n} = a + \frac{\sqrt{1-a^2}}{\sqrt{1-a^2}}(bi + cj + dk) = a + bi + cj + dk$$

.

Exemplo 5.1. *Vamos rotacionar $v = (1, 0, 0)$ por $90°$ no eixo z:*

Primeiramente, convertamos o vetor para quatérnion puro: $v = 0 + 1i + 0j + 0k = i$

Agora, o eixo $\overrightarrow{n}$ em quatérnion: $\overrightarrow{n} = 0 + 0i + 0j + 1k = k$

E então temos: $q = \left[cos\left(\frac{\pi}{4}\right) + \left(sen\left(\frac{\pi}{4}\right) \cdot k\right)\right]$

Finalmente:

$$v' = Ad_q(v) = qv\bar{q} =$$

$$= \left[cos\left(\frac{\pi}{4}\right) + \left(sen\left(\frac{\pi}{4}\right) \cdot k\right)\right] i \left[cos\left(\frac{\pi}{4}\right) - \left(sen\left(\frac{\pi}{4}\right) \cdot k\right)\right] =$$

$$\left(\frac{\sqrt{2}}{2}i + \frac{\sqrt{2}}{2}j\right)\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}k\right) = \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}j - \frac{1}{2}i = j$$

Portanto $v' = (0, 1, 0)$.

6 Álgebras de Clifford

Para essa parte do relatório, alguns teoremas serão enunciados sem demonstração por conta da complexidade e/ou extensão.

$$\begin{array}{rccc} b: & \mathbb{V}\times\mathbb{V} & \longrightarrow & \mathbb{K} \\ & (v,w) & \longmapsto & b(v,w) \end{array}$$

6.1 Formas Quadráticas

Definição 6.1. *Seja $\mathbb{V}$ um espaço vetorial sobre um corpo $\mathbb{K}$. Uma forma bilinear simétrica em $\mathbb{V}$ é uma aplicação:*

que satisfaz as seguintes propriedades:

I) $b(\lambda v_1 + v_2, w) = \lambda(v_1, w) + b(v_2, w)$, para quaisquer $v_1, v_2, w \in \mathbb{V}$ e qualquer $\lambda \in \mathbb{K}$.

II) $b(v, \lambda w_1 + w_2) = \lambda b(v, w_1) + b(v, w_2)$ para quaisquer $v, w_1, w_2 \in \mathbb{V}$ e qualquer $\lambda \in \mathbb{K}$.

III) $b(v, w) = b(w, v)$ para quaisquer $v, w \in \mathbb{V}$.

Se além das três acima, b satisfizer:

IV) $b(v, w) = 0, \forall w \in \mathbb{V} \Rightarrow v = 0$.

Dizemos que é uma forma bilinear simétrica não degenerada.

Definição 6.2. *A forma quadrática associada a uma forma bilinear simétrica b é uma aplicação $q : \mathbb{V} \longrightarrow \mathbb{K}$ dada por $q(v) = b(v, v)$.*

Proposição 6.1. *Podemos escolher uma base de $\mathbb{V}$ para a qual existam números inteiros não negativos p, q e r, satisfazendo $p + q + r = n$, onde n é a dimensão do espaço vetorial, de forma que para todo par de vetores $v, w \in \mathbb{V}$, tenhamos:*

$$b(v, w) = v^1 w^1 + \cdots + v^p w^p - v^{p+1} w^{p+1} - \cdots - v^{p+q} w^{p+q}$$

Demonstração 6.1. *Presente em [3] na parte Formas Quadráticas.* □

Definição 6.3. *Dizemos que $p + q$ é o posto da forma quadrática, r é a nulidade e $p - q$ é a assinatura da forma b. Se $r = 0$, e portanto $n = p + q$, temos que b não é degenerada. Se $n = p$, então b é positiva. Finalmente, uma base de $\mathbb{V}$ segundo a qual b pode ser escrita na forma da proposição acima é dita ser uma base ortogonal relativa a b.*

6.2 Produto Tensorial

Definição 6.4. *Dados dois espaços vetoriais $\mathbb{V}$ e $\mathbb{W}$, o produto tensorial entre os dois é um novo espaço vetorial $\mathbb{V} \otimes \mathbb{W}$ e uma aplicação bilinear $\varphi : \mathbb{V} \times \mathbb{W} \longrightarrow \mathbb{V} \otimes \mathbb{W}$ de forma que para qualquer outra aplicação bilinear $f : \mathbb{V} \times \mathbb{W} \longrightarrow \mathbb{U}$ exista uma única aplicação linear $\bar{f} : \mathbb{V} \otimes \mathbb{W} \longrightarrow \mathbb{U}$ tal que $f = \bar{f} \circ \varphi$.*

Observação 6.1. *Podemos visualizar o espaço produto tensorial $\mathbb{V} \otimes \mathbb{W}$ como sendo o espaço vetorial das combinações lineares de produtos da forma $v \otimes w$, para $v \in \mathbb{V}$ e $w \in \mathbb{W}$ satisfazendo:*

I) $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$.

II) $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$.

III) $(\lambda v) \otimes w = v \otimes (\lambda w) = \lambda(v \otimes w)$.

Observação 6.2. *A observação acima nos permite definir* φ *como:* $\varphi(v, w) = v \otimes w$.

Definição 6.5. *Dada uma aplicação bilinear* $f : \mathbb{V} \times \mathbb{W} \longrightarrow \mathbb{U}$, *podemos construir a aplicação linear a ela associada como:*

$$\bar{f}\left(\sum_i v_i \otimes w_i\right) = \sum_i f(v_i, w_i)$$

Um enunciado importante de produtos tensoriais é o seguinte teorema, que será enunciado sem ser demonstrado:

Teorema 6.1. *Sejam* $\{e_i\}_{i\in I}$ *base de* $\mathbb{V}$ *e* $\{f_j\}_{j\in J}$ *base de* $\mathbb{W}$, *então temos que o conjunto* $\{e_i \otimes f_j\}_{i\in I, j\in J}$ *é base para o produto tensorial* $\mathbb{V} \otimes \mathbb{W}$.

Observação 6.3. *Podemos escrever de maneira única um elemento do produto tensorial como uma combinação linear*

$$\sum_{i,j} \lambda_{ij} e_i \otimes f_j \ ; \ \lambda_{ij} \in \mathbb{R}$$

Teorema 6.2. *Existem os seguintes isomorfismos entre os produtos tensoriais de espaços vetoriais:*

I) $\mathbb{V} \otimes (\mathbb{W} \otimes \mathbb{U}) \cong (\mathbb{V} \otimes \mathbb{W}) \otimes \mathbb{U}$.

II) $\mathbb{V} \otimes \mathbb{R} \cong \mathbb{V}$.

III) $\mathbb{V} \otimes \mathbb{W} \cong \mathbb{W} \otimes \mathbb{V}$.

IV) $\mathbb{V} \otimes \mathbb{W}^* \cong \mathcal{L}(\mathbb{W}, \mathbb{V})$. *Esse isomorfismo só vale para* $dim(\mathbb{W}) < \infty$. *Aqui,* $\mathbb{W}^*$ *é o espaço vetorial dual a* $\mathbb{W}$ *e* $\mathcal{L}(\mathbb{W}, \mathbb{V})$ *denota o espaço das transformações lineares de* $\mathbb{W}$ *em* $\mathbb{V}$.

V) $\mathbb{V}^* \otimes \mathbb{W}^* \cong (\mathbb{V} \otimes \mathbb{W})^*$. *Esse isomorfismo só vale para* $\mathbb{V}$ *e* $\mathbb{W}$ *de dimensão finita.*

O item I do teorema garante que podemos fazer produtos tensoriais independentemente da ordem que tomarmos os produtos dois a dois.

O item III garante o isomorfismo dos espaços.

Definição 6.6. *Dado um espaço vetorial* $\mathbb{V}$, *podemos construir a álgebra tensorial* $T(\mathbb{V})$ *que é o espaço vetorial:*

$$T(\mathbb{V}) = \bigoplus_{n\geq 0} \mathbb{V}^{\otimes n}$$

onde $\mathbb{V}^{\otimes 0} = \mathbb{R}$, $\mathbb{V}^{\otimes 1} = \mathbb{V}$ *e* $\mathbb{V}^{\otimes v} = \mathbb{V} \otimes \mathbb{V}^{\otimes n-1}$, *para* $n > 1$.

Definição 6.7. *Em* $T(\mathbb{V})$ *podemos definir um produto de maneira natural:*

$$(v_1 \otimes \cdots \otimes v_n)(w_1 \otimes \cdots \otimes w_m) = v_1 \otimes \cdots \otimes v_n \otimes w_1 \otimes \cdots \otimes w_m$$

estendendo-o linearmente. Esta é a chamada álgebra tensorial sobre $\mathbb{V}$.

Temos dois teoremas essenciais a respeito de álgebras tensoriais:

Teorema 6.3. *Dada qualquer aplicação linear $f : \mathbb{V} \longrightarrow A$, onde A é uma álgebra, existe um único homomorfismo de álgebras $\hat{f} : T(\mathbb{V}) \longrightarrow A$ comutando o diagrama abaixo:*

$$\begin{tikzcd}
 & T(\mathbb{V}) \arrow[d, "\hat{f}"] \\
\mathbb{V} \arrow[ur, "i"] \arrow[r, "f"] & A
\end{tikzcd}$$

Sendo que $i : \mathbb{V} \longrightarrow T(\mathbb{V})$ é a inclusão canônica.

Assim, podemos construir homomorfismos de álgebras entre $T(\mathbb{V})$ e uma álgebra A qualquer por aplicações lineares. Como consequência disso, juntamente com o teorema dos isomorfismos, obtemos o seguinte resultado:

Teorema 6.4. *Dada qualquer álgebra A sobre o corpo dos reais, existe um espaço vetorial $\mathbb{V}$ e um ideal $I \lhd T(\mathbb{V})$ tal que $A \cong \frac{T(\mathbb{V})}{I}$*

Com isso, sabemos que todas as álgebras são quocientes de alguma álgebra tensorial.

Observação 6.4. *Se $f : \mathbb{V} \longrightarrow A$ uma transformação linear de V em A na álgebra A, então o homomorfismo $\hat{f}$ é dado por: $\hat{f}(v_1 \otimes \cdots \otimes v_n) = f(v_1) \cdots f(v_n)$ e estendido por linearidade para todos os elementos de $T(\mathbb{V})$.*

6.3 Álgebra de Clifford

Definição 6.8. *Dado um espaço vetorial $\mathbb{V}$ e uma forma quadrática $q : \mathbb{V} \longrightarrow \mathbb{R}$, a álgebra de Clifford associada a eles é uma álgebra $C(\mathbb{V}, q)$ e uma aplicação linear $\phi : \mathbb{V} \longrightarrow C(\mathbb{V}, q)$, satisfazendo $\phi(v)^2 = -q(v)1$ de forma que para qualquer aplicação linear $f : \mathbb{V} \longrightarrow A$, onde A é uma álgebra, e que também satisfaça $f(v)^2 = -q(v)1$, existe um único homomorfismo de álgebras $\hat{f} : C(\mathbb{V}, q) \longrightarrow A$ comutando o diagrama abaixo:*

$$\begin{tikzcd}
 & C(\mathbb{V}, q) \arrow[d, "\hat{f}"] \\
\mathbb{V} \arrow[ur, "\phi"] \arrow[r, "f"] & A
\end{tikzcd}$$

Assim, estamos definindo esse objeto pela chamada propriedade universal.

Como vimos pelo teorema 4.4, toda álgebra é quociente de uma álgebra tensorial. Tomemos a álgebra $T(\mathbb{V})$ como candidata. Queremos que $v^2 = -q(v)1 = -q(v)$, então definamos o ideal bilateral $I = \langle v \otimes v + q(v)1 \mid v \in \mathbb{V} \rangle \lhd T(\mathbb{V})$. A álgebra quociente será nossa álgebra de Clifford.

Denotemos por $v_1 \bullet \cdots \bullet v_n$ a classe do monômio $v_1 \otimes \cdots \otimes v_n$ em $C(\mathbb{V}, q)$. Então, seja $\phi : \mathbb{V} \longrightarrow C(\mathbb{V}, q)$ dada pela inclusão canônica. Automaticamente, ϕ satisfará $\phi(v)^2 = -q(v)$.

Tendo o par $(C(\mathbb{V}, q), \phi)$ verifiquemos se a propriedade universal é satisfeita:

Seja $f : \mathbb{V} \longrightarrow A$ linear na álgebra A, satisfazendo $f(v)^2 = -q(v)1_A$.

Pelo teorema 4.3, existe um único homomorfismo de álgebras $\tilde{f} : T(\mathbb{V}) \longrightarrow A$ tal que: $\tilde{f}(v_1 \otimes \cdots \otimes v_n) = f(v_1)\cdots f(v_n)$. Como para qualquer $v \in \mathbb{V}$ temos que $f(v)^2 = -q(v)1_A$, então $\tilde{f}|_I \equiv 0$. Assim podemos definir $\hat{f} : C(\mathbb{V}, q) \longrightarrow A$ dado por:

$$\hat{f}(v_1 \bullet \cdots \bullet v_n) = \tilde{f}(v_1 \otimes \cdots \otimes v_n)$$

Com isso temos que $\hat{f}$ está bem definido nas classes, pois $\tilde{f}$ se anula no ideal que define a álgebra de Clifford.

Observação 6.5. *Podemos denotar $C(\mathbb{V}, q)$ por $C_{p,q,r}$.*

Definição 6.9. *Seja $\{e_i\}_{i=1}^n$ uma base ortogonal para q. Então, $C_{p,q,r}$ será gerada por monômios $e_{i_1} \bullet \cdots \bullet e_{i_k}$ de comprimentos variáveis, sendo que os elementos da base satisfazem as seguintes relações:*

I) $e_i \bullet e_i = -1$, para $1 \leq i \leq p$.

II) $e_i \bullet e_i = 1$, para $P + 1 \leq i \leq p + q$.

III) $e_i \bullet e_i = 0$, para $p + q + 1 \leq i \leq n = p + q + r$.

IV) $e_i \bullet e_j = -e_j \bullet e_i$, para $i \neq j$.

Exemplo 6.1. *Vamos mostrar que, se $dim(\mathbb{V}) = n$, então, para qualquer forma quadrática em $\mathbb{V}$, temos que $dim(C(\mathbb{V}, q)) = 2^n$.*

Seja $1 \leq m \leq n$ o comprimento do monômio gerador de $C(\mathbb{V}, q)$. Então temos $\binom{n}{m}$ modos de escolhermos um subconjunto de m elementos dentre os n elementos da base. Assim, a dimensão de $C(\mathbb{V}, q)$ deve ser a soma de todas as possíveis escolhas de m:

$$dim(C(\mathbb{V}, q)) = \sum_{m=0}^{n} \binom{n}{m} = 2^n, \text{ por indução através do Triângulo de Pascal.}$$

Definição 6.10. *Denotemos por $C(\mathbb{V}, q)^+$ o subespaço gerado pelos monômios de comprimento par e $C(\mathbb{V}, q)^-$ pelos de comprimento ímpar.*

Então temos que: $C^+ \bullet C^+ \subseteq C^+$, $C^+ \bullet C^- \subseteq C^-$, $C^- \bullet C^+ \subseteq C^-$ e $C^- \bullet C^- \subseteq C^+$.

Exemplo 6.2. *Seja $\mathbb{V} \cong \mathbb{R}$, gerado pelo vetor e e $q(xe) = x^2$, então $q(e) = 1$. A álgebra de Clifford será: $C_{1,0,0} = \{a \cdot 1 + b \cdot e \mid a, b \in \mathbb{R}, e^2 = -1\} = \mathbb{C}$.*

Exemplo 6.3. *Seja $\mathbb{V} \cong \mathbb{R}^2$, gerado pelos vetores e_1 e e_2. Tomemos agora $q(xe_1 + ye_2) = x^2 + y^2$, então $q(e) = 1$. A álgebra de Clifford será: $C_{2,0,0} = \{a \cdot 1 + be_1 + ce_2 + de_1 \bullet e_2 \mid a, b, c, d \in \mathbb{R}, e_i \bullet e_j + e_j \bullet e_i = -2\delta_{ij}\}$.*

Note que denominando $i = e_1, j = e_2, k = e_1 \bullet e_2$, temos que $i^2 = j^2 = k^2 = ijk = -1$. De fato: $k^2 = ijk = e_1 \bullet e_2 \bullet e_1 \bullet e_2 = -e_1 \bullet e_1 \bullet e_2 \bullet e_2 = -(-1)(-1) = -1$.

Ou seja, claramente $C_{2,0,0}$ é a álgebra dos quatérnions $\mathbb{H}$.

6.4 Grupos Pin e Spin

Seja $C = C(\mathbb{V}, q)$, onde q não é a forma quadrática identicamente nula. Então, C possui elementos inversíveis. De fato, seja $v \in \mathbb{V} : q(v) \neq 0$, então:

$$v^2 = -q(v) \Rightarrow v \bullet \frac{v}{-q(v)} = 1$$

Para cada elemento inversível $x \in C^\times$, podemos definir a aplicação Ad_x, que associa a cada elemento $y \in C$ o elemento $xyx^{-1} \in C$.

Da mesma maneira que fizemos para os quatérnions, podemos mostrar que Ad_x é um automorfismo em C. Com isso, temos:

$$\begin{array}{cccc} Ad: & C^\times & \longrightarrow & Aut(C) \\ & x & \longmapsto & Ad_x \end{array}$$

Teorema 6.5. *Seja $v \in \mathbb{V} \subset C$ um vetor tal que $q(v) \neq 0$. Então $Ad_v(\mathbb{V}) \subseteq \mathbb{V}$. Além disso, para todo $w \in \mathbb{V}$ temos que $-Ad_v(w) = w - 2\dfrac{b(v,w)}{q(v)}v$.*

Demonstração 6.2.

$$Ad_v(w) = vwv^{-1} = -\frac{1}{q(v)}vwv = -\frac{1}{q(v)}v(-vw - 2b(v,w)) =$$
$$= \frac{1}{q(v)}(v^2 w + 2b(v,w)v) = \frac{1}{q(v)}(-q(v)w + 2b(v,w)v) = -w + 2\frac{b(v,w)}{q(v)}v$$

□

Definição 6.11. *Seja $P(\mathbb{V}, q) \subseteq C(\mathbb{V}, q)^\times$ o subgrupo multiplicativo gerado pelos vetores $v \in \mathbb{V}$ tais que $q(v) \neq 0$. Se $v \in \mathbb{V}$ é tal que $q(v) \neq 0$, então para qualquer $w \in \mathbb{V}$ temos:*

$$q(Ad_v(w)) = b\left(-w + 2\frac{b(v,w)}{q(v)}v, -w + 2\frac{b(v,w)}{q(v)}v\right) =$$
$$= q(w) - 4\frac{b(v,w)}{q(v)}b(v,w) + 4\left(\frac{b(v,w)}{q(v)}\right)^2 q(v) = q(w)$$

Com isso, restringimos a aplicação Ad para $Ad : P(\mathbb{V}, q) \longrightarrow O(\mathbb{V}, q)$, onde $O(\mathbb{V}, q)$ é o grupo das transformações ortogonais em $\mathbb{V}$ relativas à forma quadrática q, ou seja, se b é a forma bilinear simétrica em $\mathbb{V}$ relacionada a q, então o grupo consistirá de transformações que preservem $b(u,v) = \frac{1}{2}(q(u+v) - q(u) - q(v))$.

Definição 6.12. *O subgrupo $Pin(\mathbb{V}, q)$ é definido como o subgrupo de $P(\mathbb{V}, q)$ gerado pelos vetores $v \in \mathbb{V}$ tais que $q(v) = \pm 1$. O subgrupo $Spin(\mathbb{V}, q)$ é a intersecção dada por $Spin(\mathbb{V}, q) = Pin(\mathbb{V}, q) \cap C(\mathbb{V}, q)^+$.*

Finalmente, o resultado mais importante envolvendo esses grupos é:

Teorema 6.6. *Seja $C(\mathbb{V}, q)$ uma álgebra de Clifford sobre um espaço vetorial $\mathbb{V}$. Então, existe um homomorfismo de grupo sobrejetivo entre $Spin(\mathbb{V}, q)$ e $SO(\mathbb{V}, q)$ cujo kernel é igual a $\{+1, -1\}$.*

De fato, as álgebras de Clifford generalizam os números complexos e os quatérnions, sendo que esse último resultado generaliza o *Teorema 3.1.*

7 Referências

[1] A. Garcia, Y. Lequain, *Elementos de Álgebra,* 6. ed. Projeto Euclides, Rio de Janeiro, 2018.

[2] S. L. Zani, *Álgebra Linear,* Notas de aula, Departamento de Matemática, ICMC - USP, 2003.

[3] E. Batista, M. V. Santos, *Rotações, quatérnions e álgebras de Clifford,* Notas de minicurso da VI bienal da sociedade brasileira de matemática, Campinas, 2012.