



UNIVERSIDADE FEDERAL DE SANTA CATARINA

Centro Tecnológico, de Ciências Exatas e Educação  
Departamento de Matemática

PIBIC  
RELATÓRIO FINAL

Geometria de Distâncias e Álgebras Geométricas: novas perspectivas  
geométricas, computacionais e aplicações

---

**Geometria de Distâncias e Álgebras  
Geométricas Aplicadas a Conformação  
Molecular**

---

Guilherme Philippi ([guilherme.philippi@hotmail.com](mailto:guilherme.philippi@hotmail.com)),

ORIENTADOR: Felipe Delfini Caetano Fidalgo ([felipe.fidalgo@ufsc.br](mailto:felipe.fidalgo@ufsc.br)).

Dedicatória.

# Agradecimentos

Somos muito gratos ao CNPq, tanto pelo incentivo financeiro da bolsa PIBIC quanto por tanto proporcionar as condições para a pesquisa em nosso país. Agradecimentos especiais também à UFSC, por dar as condições de infraestrutura para que este projeto pudesse acontecer. Este agradecimento busca estender-se à todos os profissionais destas duas instituições.

# Sumário

<b>1</b>	<b>Introdução</b>	<b>1</b>
<b>2</b>	<b>Preliminares</b>	<b>2</b>
2.1	Elementos de Álgebra Abstrata . . . . .	2
2.1.1	Relações entre Conjuntos e Operações . . . . .	2
2.1.2	Grupos . . . . .	4
2.1.3	Anéis e Corpos . . . . .	16
2.1.4	Módulos, Espaços Vetoriais e Álgebras . . . . .	21
2.2	Álgebra Geométrica . . . . .	26
2.2.1	O Produto Externo de Grassmann . . . . .	26
2.2.2	Álgebra Exterior $\wedge \mathbb{R}^3$ . . . . .	31
2.2.3	Álgebra Geométrica $\mathcal{Cl}_3$ . . . . .	32
2.2.4	Álgebra dos Quatérnios . . . . .	35
2.3	Geometria de Distâncias Euclidianas . . . . .	39
2.3.1	Como tudo Começou . . . . .	39
2.3.2	O Problema Fundamental . . . . .	45
2.3.3	A Busca de uma Solução . . . . .	48
2.3.4	Ferramentas Combinatórias na Solução do DGP . . . . .	49
2.3.5	<i>MDGP Discretizável</i> . . . . .	59
2.3.6	<i>Branch-and-Prune</i> . . . . .	62
<b>3</b>	<b>Materiais e Métodos</b>	<b>67</b>
3.1	BP com Quatérnios . . . . .	67
<b>4</b>	<b>Resultados e Discussão</b>	<b>68</b>
4.1	Contando Operações . . . . .	68
4.2	Pré-processamento Molecular . . . . .	68
4.3	Resultados Computacionais . . . . .	68
4.4	Publicações Relacionadas . . . . .	68
<b>5</b>	<b>Considerações Finais</b>	<b>69</b>
	<b>Referências Bibliográficas</b>	<b>69</b>
<b>A</b>	<b>Teoria de Grafos</b>	<b>74</b>
<b>B</b>	<b>Um Passeio pela Bioquímica</b>	<b>80</b>
<b>C</b>	<b>Vinte Aminoácidos Naturais</b>	<b>90</b>

## Abstract

The classical modeling of the Discretizable Molecular Distance Geometry Problem is done using matrices as linear transformations and has a set of rotations at its core. This work studies the computational benefits of applying quaternion algebra to represent these rotations in place of matrices. Some computer simulations are performed.

**Keywords:** Distance Geometry, Quaternion Algebra, Molecular Geometry.

## Resumo

A modelagem clássica do Problema de Geometria de Distâncias Moleculares Discretizável é feita utilizando matrizes como transformações lineares e possui um conjunto de rotações em seu núcleo. Este trabalho faz um estudo sobre os benefícios computacionais de aplicar a álgebra de quatérnios para representar estas rotações no lugar das matrizes. Algumas simulações computacionais são realizadas.

**Palavras-chave:** Geometria de Distâncias, Álgebra de Quatérnios, Geometria molecular.

1

# Introdução

# 2

## Preliminares

### 2.1 Elementos de Álgebra Abstrata

#### 2.1.1 Relações entre Conjuntos e Operações

**Definição 2.1.1** (Produto cartesiano). Sejam  $A$  e  $B$  conjuntos. O conjunto

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\}$$

é o *produto cartesiano de  $A$  e  $B$* .

**Exemplo 2.1.1.** Se  $A = \{1, 2, 3\}$  e  $B = \{3, 4\}$ , então

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)\}.$$

**Definição 2.1.2** (Relação). Uma *relação* entre dois conjuntos  $A$  e  $B$  é um subconjunto  $\mathcal{R} \subset A \times B$ . Lê-se  $(a, b) \in \mathcal{R}$  como “ $a$  está relacionado com  $b$ ” e escreve-se  $a \mathcal{R} b$ .

**Exemplo 2.1.2** (Relação de igualdade). A realação  $=$ , chamada *relação de igualdade*, é definida sobre um conjunto  $S$  por

$$= \text{ é o subconjunto } \{(x, x) \mid x \in S\} \subset S \times S.$$

**Observação 2.1.1.** Sempre que uma relação for definida entre um conjunto  $S$  e ele mesmo, como no exemplo 2.1.2, diremos que esta é uma relação *sobre  $S$* .

**Definição 2.1.3** (Função). Uma *função*  $\varphi$  que mapeia  $X$  em  $Y$  é uma relação entre  $X$  e  $Y$  com a propriedade de que cada  $x \in X$  só irá aparecer uma única vez, e exatamente uma, em um par ordenado  $(x, y) \in \varphi$ . Também chamamos  $\varphi$  de *mapa* ou *mapeamento* de  $X$  em  $Y$ . Escrevemos  $\varphi : X \rightarrow Y$  e expressaremos  $(x, y) \in \varphi$  por  $\varphi(x) = y$ . O *domínio* de  $\varphi$  é o conjunto  $X$  e o conjunto  $Y$  é dito *contradomínio* de  $\varphi$ . Chama-se de *alcance* de  $\varphi$  o conjunto  $\varphi[X] = \{\varphi(x) \mid x \in X\}$ .

**Definição 2.1.4** (Função injetiva e sobrejetiva). Uma função  $\varphi : X \rightarrow Y$  é *injetiva* se  $\varphi(x_1) = \varphi(x_2) \iff x_1 = x_2$ . Também,  $\varphi$  é dita *sobrejetiva* se o alcance de  $\varphi$  é  $Y$ . Se uma função é injetiva e sobrejetiva, então dizemos que a função é *bijetiva*.

## Leis de composição

**Definição 2.1.5** (Lei de composição). Uma *lei de composição* sobre um conjunto  $S$  é uma função (ou, uma operação binária)  $* : S \times S \rightarrow S$ .

**Observação 2.1.2** (Notação de operação). Usaremos a notação  $*(a, b) = a * b$ , para simplificar a escrita de propriedades. Também, quando não houver ambiguidade, suprimiremos o símbolo da lei, fazendo  $a * b = ab$ .

**Definição 2.1.6.** Para  $a, b, c \in S$ , uma lei de composição  $*$  é dita

- *Associativa*, se  $(a * b) * c = a * (b * c)$ ;
- *Comutativa*, se  $a * b = b * a$ .

**Proposição 2.1.1.** Seja uma lei associativa dada sobre o conjunto  $S$ . Há uma única forma de definir, para todo inteiro  $n$ , um produto de  $n$  elementos  $a_1, \dots, a_n \in S$  (diremos  $[a_1 \cdots a_n]$ ) com as seguintes propriedades:

1. o produto  $[a_1]$  de um elemento é o próprio elemento;
2. o produto  $[a_1 a_2]$  de dois elementos é dado pela lei de composição;
3. para todo inteiro  $1 \leq i \leq n$ ,  $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$ .

*Demonstração.* A demonstração dessa proposição é feita por indução em  $n$ .  $\square$

**Definição 2.1.7.** Dizemos que  $e \in S$  é *identidade* para uma lei de composição se  $ea = ae = a$  para todo  $a \in S$ .

**Proposição 2.1.2.** O elemento identidade é único.

*Demonstração.* Se  $e, e'$  são identidades, já que  $e$  é identidade, então  $ee' = e'$  e, como  $e'$  é uma identidade,  $ee' = e$ . Logo  $e = e'$ , isto é, a identidade é única.  $\square$

**Observação 2.1.3.** Usaremos  $\vec{1}$  para representar a identidade multiplicativa e  $\vec{0}$  para denotar a aditiva.

**Definição 2.1.8** (Elemento inverso). Seja uma lei de composição que possua uma identidade. Um elemento  $a \in S$  é chamado *invertível* se há um outro elemento  $b \in S$  tal que  $ab = ba = 1$ . Desde que  $b$  exista, ela é única e a denotaremos por  $a^{-1}$  e a chamaremos *inversa de  $a$* .

**Proposição 2.1.3.** Se  $a, b \in S$  possuem inversa, então a composição  $(ab)^{-1} = b^{-1}a^{-1}$ .

**Observação 2.1.4** (Potências). Usaremos as seguintes notações:

- $a^n = a^{n-1}a$  é a composição de  $a \cdots a$   $n$  vezes;
- $a^{-n}$  é a inversa de  $a^n$ ;
- $a^0 = \vec{1}$ .

Com isso, tem-se que  $a^{r+s} = a^r a^s$  e  $(a^r)^s = a^{rs}$ . (Isso não induz uma notação de fração  $\frac{b}{a}$  a menos que seja uma lei comutativa, visto que  $ba^{-1}$  pode ser diferente de  $a^{-1}b$ ). Para falar de uma lei de composição aditiva, usaremos  $-a$  no lugar de  $a^{-1}$  e  $na$  no lugar de  $a^n$ .

## 2.1.2 Grupos

**Definição 2.1.9** (Grupo). Um *grupo*  $(G, *)$  é um conjunto  $G$  onde uma lei de composição  $*$  é dada sobre  $G$  tal que os seguintes axiomas são satisfeitos:

1. (*Associatividade*). Para todo  $a, b, c \in G$ , tem-se

$$(a * b) * c = a * (b * c);$$

2. (*Existência da identidade*). Existe um elemento  $\vec{1} \in G$  tal que, para todo  $a \in G$ ,

$$\vec{1} * a = a * \vec{1} = a;$$

3. (*Existência do inverso*). Para todo  $a \in G$  existe um elemento  $a' \in G$  tal que

$$a * a' = a' * a = \vec{1}.$$

**Observação 2.1.5.** É comum abusar da notação e chamar um grupo  $(G, *)$  e o conjunto de seus elementos  $G$  pelo mesmo símbolo, omitindo a lei de composição na falta de ambiguidade.

**Definição 2.1.10** (Grupo abeliano). Um *grupo abeliano* é um grupo com uma lei de composição comutativa. Costuma-se usar a notação aditiva para grupos abelianos.

**Proposição 2.1.4** (Lei do cancelamento). *Seja  $a, b, c$  elementos de um grupo  $G$ . Se  $ab = ac$ , então  $b = c$ .*

### Subgrupos

**Definição 2.1.11** (Subgrupo). Um subconjunto  $H$  de um grupo  $G$  é chamado de *subgrupo* de  $G$  (e escreve-se  $H \leq G$ ) se possuir as seguintes propriedades:

1. (*Fechado*). Se  $a, b \in H$ , então  $ab \in H$ ;
2. (*Identidade*).  $1 \in H$ ;
3. (*Inversível*). Se  $a \in H$ , então  $a^{-1} \in H$ .

**Observação 2.1.6** (Lei de composição induzida). Veja que a propriedade 1 necessita de uma lei de composição. Usamos a lei de composição de  $G$  para definir uma lei de composição de  $H$ , chamada *lei de composição induzida*. Essas propriedades garantem que  $H$  é um grupo com respeito a sua lei induzida.

**Definição 2.1.12** (Subgrupo apropriado). Todo grupo  $G$  possui dois subgrupos triviais: O subgrupo formado por todos os elementos de  $G$  e o subgrupo  $\{\vec{1}\}$ , formado pela identidade de  $G$ . Diz-se que um subgrupo é um *subgrupo apropriado* se for diferente desses dois.

**Definição 2.1.13** (Centro de um grupo). O *centro*  $Z(G)$  de um grupo  $G$  é o conjunto de elementos que comutam com todo elemento de  $G$ :

$$Z(G) = \{z \in G \mid zx = xz \text{ para todo } x \in G\}.$$

**Exemplo 2.1.3.** Utilizando da notação multiplicativa, define-se o *subgrupo cíclico*  $H$  gerados por um elemento arbitrário  $x$  de um grupo  $G$  como o conjunto de todas as potências de  $x$ :  $H = \{\dots, x^{-2}, x^{-1}, \vec{1}, x, x^2, \dots\}$ .

**Definição 2.1.14.** Chama-se *ordem* de um grupo  $G$  o número  $|G|$  de elementos de  $G$ .

Também pode-se definir um subgrupo de um grupo  $G$  gerado por um subconjunto  $U \subset G$ . Esse é o menor subgrupo de  $G$  que contém  $U$  e consiste de todos os elementos de  $G$  que podem ser expressos como um produto de uma cadeia de elementos de  $U$  e seus inversos.

**Exemplo 2.1.4.** O *grupo de quaternions*  $H$  é o menor subgrupo do conjunto de matrizes  $2 \times 2$  complexas invertíveis que não é cíclico. Isso consiste nas oito matrizes

$$H = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\},$$

onde

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Os dois elementos  $\mathbf{i}, \mathbf{j}$  geram  $H$ , e o calculo leva as formulas

$$\mathbf{i}^4 = 1, \quad \mathbf{i}^2 = \mathbf{j}^2, \quad \mathbf{j}\mathbf{i} = \mathbf{i}^3\mathbf{j}.$$

### Homomorfismos e isomorfismos

**Definição 2.1.15** (Homomorfismo de grupo). Sejam  $(G, *)$  e  $(G', \cdot)$  dois grupos. Um *homomorfismo*  $\varphi : G \rightarrow G'$  é um mapeamento tal que

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \quad \forall a, b \in G. \quad (\text{propriedade de homomorfismo})$$

**Exemplo 2.1.5** (Inclusão). Seja  $H$  o subgrupo de um grupo  $G$ . O homomorfismo  $i : H \rightarrow G$  é dito *inclusão* de  $H$  em  $G$ , definido por  $i(x) = x$ .

**Proposição 2.1.5.** Um homomorfismo  $\varphi : G \rightarrow G'$  mapeia a identidade de  $G$  à identidade de  $G'$  e transforma as inversas de  $G$  nas respectivas inversas em  $G'$ . Isto é, as seguintes propriedades valem

- $\varphi(\vec{1}) = \vec{1}$  e
- $\varphi(a^{-1}) = \varphi(a)^{-1}$ .

**Observação 2.1.7.** Por conta da Proposição 2.1.5, dizemos que o mapeamento  $\varphi$  preserva a estrutura algébrica de grupo.

**Exemplo 2.1.6.** Seja  $\varphi : G \rightarrow G'$  um homomorfismo de grupo sobrejetivo de  $G$  em  $G'$ . Queremos mostrar que, se  $G$  é abeliano, então  $G'$  deve ser abeliano. Isto é, seja  $a', b' \in G'$ , queremos mostrar que  $a'b' = b'a'$ . Como  $\varphi$  é sobrejetiva, existe  $a, b \in G$  tal que  $\varphi(a) = a'$  e  $\varphi(b) = b'$ . Pela propriedade de homomorfismo,  $a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'$ . Segue que  $G'$  deve ser abeliano.

**Definição 2.1.16** (Imagen). A *imagen* de um homomorfismo  $\varphi : G \rightarrow G'$  é o subconjunto de  $G'$

$$\text{im } \varphi = \{x \in G' \mid x = \varphi(a), \text{ para algum } a \in G\} = \varphi(G).$$

**Proposição 2.1.6.** A *imagen* de um homomorfismo  $\varphi : G \rightarrow G'$  é um subgrupo de  $G'$ .

**Definição 2.1.17** (Núcleo). O *núcleo* do homomorfismo  $\varphi : G \rightarrow G'$  é o subconjunto de  $G$  formado pelos elementos que são mapeados pela identidade em  $G'$ :

$$\text{núcl } \varphi = \{a \in G \mid \varphi(a) = \vec{1}\} = \varphi^{-1}(\vec{1}).$$

**Proposição 2.1.7.** O *núcleo* de um homomorfismo  $\varphi : G \rightarrow G'$  é um subgrupo de  $G$ .

**Definição 2.1.18** (Isomorfismo de grupos). Dois grupos  $(G, *)$  e  $(G', \cdot)$  são ditos *isomórfos* se possuírem um homomorfismo bijetivo entre si, isto é, há um mapeamento *bijetivo*  $\varphi : G \rightarrow G'$  (chamado *relação de isomorfismo*) que respeita a propriedade de homomorfismo:

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \text{ para todo } a, b \in G.$$

**Observação 2.1.8.** Usa-se a notação  $G \approx G'$  para dizer que  $G$  é isomorfo a  $G'$ .

**Definição 2.1.19** (Classe de isomorfismo). Diz-se que o conjunto de grupos isomórfos a um dado grupo  $G$  é a *classe de isomorfismo de  $G$* .

**Proposição 2.1.8.** Qualquer dois grupos em uma mesma classe de isomorfismo também são isomórfos entre si.

**Definição 2.1.20** (Automorfismo). Quando uma relação de isomorfismo  $\varphi : G \rightarrow G$  é definida de um grupo  $G$  para ele mesmo, chamamos esse tipo de isomorfismo de *automorfismo* de  $G$ .

**Exemplo 2.1.7** (Conjugação). Seja  $b \in G$  um elemento fixo. Então, a *conjugação de  $G$  por  $b$*  (também chamado *automorfismo interno de  $G$  por  $b$* ) é o mapeamento  $\varphi$  de  $G$  para ele mesmo definido por

$$\varphi_b(x) = bxb^{-1}.$$

Esse é um automorfismo porque:

- é compatível com a propriedade de homomorfismo:

$$\varphi_b(xy) = bxyb^{-1} = bx\vec{1}yb^{-1} = bxb^{-1}byb^{-1} = \varphi_b(x)\varphi_b(y);$$

- é um mapa bijetivo visto que existe a função inversa  $\varphi_b^{-1}(x) = b^{-1}xb = \varphi_{b^{-1}}(x)$  (isto é, a conjugação por  $b^{-1}$ ) que, de forma análoga, também é compatível com a propriedade de homomorfismo.

**Observação 2.1.9** (Abelianos). Se o grupo é abeliano possui a conjugação trivial:  $bab^{-1} = abb^{-1} = a$  (mapa identidade). Porém, qualquer grupo não comutativo tem alguma conjugação não trivial, isto é, existe ao menos um  $b$  que não está no centro do grupo, portanto, ao menos o automorfismo não trivial dado pela conjugação do grupo por  $b$  existe.

**Definição 2.1.21** (Conjugado). O elemento  $bab^{-1}$  é chamado *conjugado de  $a$  por  $b$* . Dois elementos  $a, a' \in G$  são ditos *conjugados* se existe  $b \in G$  tal que  $a' = bab^{-1}$ .

**Observação 2.1.10.** O conjugado tem uma interpretação muito útil: Se escrevermos  $bab^{-1}$  como  $a'$ , então

$$ba = a'b.$$

Ou seja, pode-se pensar na conjugação como a mudança em  $a$  que resulta de mover  $b$  de um lado para o outro na equação.

**Proposição 2.1.9.** *Seja  $\varphi : G \rightarrow G'$  um homomorfismo. Se  $a \in \text{núcleo } \varphi$  e  $b$  é qualquer elemento do grupo  $G$ , então o conjugado  $bab^{-1} \in \text{núcleo } \varphi$ .*

**Definição 2.1.22** (Subgrupo normal). Um subgrupo  $N$  de um grupo  $G$  é chamado *subgrupo normal* (escreve-se  $N \trianglelefteq G$ ) se para cada  $a \in N$  e  $b \in G$ , o conjugado  $bab^{-1} \in N$ .

**Observação 2.1.11.** Fica claro que o núcleo de um homomorfismo é um subgrupo normal. Além disso, todo subgrupo de um grupo abeliano também é um subgrupo normal, porém, isso não é necessariamente verdade em subgrupos de grupos não abelianos (veja Observação 2.1.9).

**Proposição 2.1.10.** *O centro de todo grupo é um subgrupo normal do grupo.*

### Grupos de Permutação

**Definição 2.1.23** (Permutação de um conjunto). Uma permutação de um conjunto  $A$  é uma função bijetiva  $\varphi : A \rightarrow A$  do conjunto para ele mesmo.

**Proposição 2.1.11** (Multiplicação de permutações). *Seja  $A$  um conjunto onde duas permutações  $\tau, \sigma$  são dadas. A composição de funções  $\tau \circ \sigma$  (chamada multiplicação de permutações) é uma lei de composição sobre  $A$ .*

**Proposição 2.1.12.** *Sejam  $A$  um conjunto não vazio,  $S_A$  o conjunto de todas as permutações de  $A$  e  $\circ$  uma multiplicação de permutações sobre  $A$ . Então,  $(S_A, \circ)$  é um grupo.*

**Definição 2.1.24** (Grupo simétrico sobre  $n$  símbolos). Seja  $A$  o conjunto finito  $\{1, 2, \dots, n\}$ . O grupo de todas as permutações de  $A$  é um *grupo simétrico sobre os  $n$  símbolos*  $1, 2, \dots, n$  e é representado por  $S_n$ .

**Observação 2.1.12.** É importante perceber que  $S_n$  possui  $n!$  elementos, isso é, a quantidade de toda combinação de  $n$  elementos.

**Exemplo 2.1.8** (Grupos diedrais). O grupo  $S_3$  de  $3! = 6$  elementos forma um grupo de simetrias de um triângulo equilátero com vértices 1, 2 e 3. As 6 permutações que formam esse grupo são as 3 rotações e os 3 espelhamentos possíveis sobre os vértices do triângulo. Também chamamos  $S_3$  de  $D_3$ , pois  $D_3$  forma o terceiro *grupo diedral*. O  $n$ -ésimo grupo diedral  $D_n$  é o grupo de simetrias de um polígono regular de  $n$  vértices.

**Definição 2.1.25** (Restrição da imagem de uma função). Sejam  $f : A \rightarrow B$  uma função e  $H$  um subconjunto de  $A$ . A *imagem de  $H$  por  $f$*  é  $\{f(h) \mid h \in H\}$  e é representada por  $f|_H$ .

**Lema 2.1.1.** Sejam  $G$  e  $G'$  grupos e  $\varphi : G \rightarrow G'$  um homomorfismo injetivo. Então,  $\varphi|_G$  é um subgrupo de  $G'$  e  $\varphi$  provê um isomorfismo de  $G$  com  $\varphi|_G$ .

**Teorema 2.1.1** (Teorema de Cayley). Todo grupo é isomorfo a um grupo de permutações.

### Relações de Equivalência e Partições

**Definição 2.1.26** (Partições). Seja  $S$  um conjunto. Uma *partição*  $P$  de  $S$  é uma subdivisão de  $S$  em subconjuntos não vazios e não sobrepostos, isto é, uma união de conjuntos disjuntos.

**Exemplo 2.1.9.** Pode-se particionar o conjunto dos números inteiros  $\mathbb{Z}$  na união de disjuntos  $P \cup I$ , onde  $P = \{z \in \mathbb{Z} \mid z \text{ é par}\}$  e  $I = \{z \in \mathbb{Z} \mid z \text{ é ímpar}\}$ .

**Definição 2.1.27** (Relações de equivalência). Uma *relação de equivalência* sobre um conjunto  $S$  é uma relação que se mantém sobre um subconjunto de elementos de  $S$ . Escreve-se  $a \sim b$  para representar a equivalência de  $a, b \in S$ , que precisa respeitar os seguintes axiomas:

1. (*Transitiva*). Se  $a \sim b$  e  $b \sim c$ , então  $a \sim c$ ;
2. (*Simétrica*). Se  $a \sim b$ , então  $b \sim a$ ;
3. (*Reflexiva*).  $a \sim a$ .

**Observação 2.1.13.** A noção de partição em  $S$  e a relação de equivalência em  $S$  são lógicamente equivalentes: Dada uma partição  $P$  sobre  $S$ , pode-se definir uma relação de equivalência  $R$  tal que, se  $a$  e  $b$  estão no mesmo subconjunto partição, então  $a \sim b$  e, dada uma relação de equivalência  $R$ , podemos definir uma partição  $P$  tal que o subconjunto que contém  $a$  é o conjunto de todos os elementos  $b$  onde  $a \sim b$ . Esse subconjunto é chamado de *classe de equivalência de a*

$$C_a = \{b \in S \mid a \sim b\}$$

e  $S$  é particionado em classes de equivalência.

**Proposição 2.1.13.** Sejam  $C_a$  e  $C_b$  duas classes de equivalência do conjunto  $S$ . Se existe  $d$  tal que  $d \in C_a$  e  $d \in C_b$ , então  $C_a = C_b$ .

**Observação 2.1.14** (Representante). Seja um conjunto  $S$ . Suponha que exista uma relação de equivalência ou uma partição sobre  $S$ . Então, pode-se construir um novo conjunto  $\bar{S}$  formado pelas classes de equivalência ou os subconjuntos partições de  $S$ . Essa construção induz uma notação muito útil: para  $a \in S$ , a classe de equivalência de  $a$  ou o subconjunto partição que contém  $a$  serão denotados como o elemento  $\bar{a} \in \bar{S}$ . Desta forma, a notação  $\bar{a} = \bar{b}$  significa que  $a \sim b$  e chamamos  $a, b \in S$  de *representantes* das respectivas classes de equivalência  $\bar{a}, \bar{b} \in \bar{S}$ .

**Definição 2.1.28** (Equivalência induzida por aplicação). Seja um mapeamento  $\varphi : S \rightarrow T$ . Chama-se de *relação de equivalência determinada por  $\varphi$*  a relação dada por  $\varphi(a) = \varphi(b) \Rightarrow a \sim b$ . Além disso, para um elemento  $t \in T$ , o subconjunto de  $\varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}$  é dito *imagem inversa de  $t$  por  $\varphi$* .

**Proposição 2.1.14.** Seja um mapeamento  $\varphi : S \rightarrow T$  e  $t \in T$  um elemento qualquer de  $T$ . Se a imagem inversa  $\varphi^{-1}(t)$  é não vazia, então  $t \in \text{im } \varphi$  e  $\varphi^{-1}(t)$  forma uma classe de equivalência  $\bar{\varphi} \in \bar{S}$  através da relação determinada por  $\varphi$ .

**Definição 2.1.29** (Congruência). Seja  $\varphi : G \rightarrow G'$  um homomorfismo. A relação de equivalência definida por  $\varphi$  é usualmente denotada por  $\equiv$  ao invés de  $\sim$  e a chamamos de *congruência*:

$$\varphi(a) = \varphi(b) \Rightarrow a \equiv b, \text{ para } a, b \in G.$$

**Proposição 2.1.15.** Seja  $\varphi : G \rightarrow G'$  um homomorfismo e  $a, b \in G$ . Então as seguintes afirmações são equivalentes:

- $\varphi(a) = \varphi(b)$
- $b = an$ , para algum  $n \in \text{nu } \varphi$
- $a^{-1}b \in \text{nu } \varphi$ .

**Definição 2.1.30** (classe lateral em relação ao núcleo). Seja  $\varphi : G \rightarrow G'$  um homomorfismo,  $a \in G$  e  $n \in \text{nu } \varphi$ . O conjunto

$$a \text{ nu } \varphi = \{g \in G \mid g = an, \text{ para algum } n \in \text{nu } \varphi\}$$

é dito *classe lateral de nu*  $\varphi$  *em*  $G$ .

**Observação 2.1.15.** Pode-se partitionar o grupo  $G$  em *classes de congruência*, formadas pelas classes laterais  $a \text{ nu } \varphi$ . Estas são imagens inversas do mapeamento  $\varphi$ .

**Proposição 2.1.16.** O homomorfismo de grupo  $\varphi : G \rightarrow G'$  é injetivo se, e somente se, seu núcleo é o subgrupo trivial  $\{\bar{1}\}$ .

**Observação 2.1.16.** Esse resultado da uma forma de verificar se um homomorfismo  $\varphi$  é também um isomorfismo: Se  $\text{nu } \varphi = \{1\}$  e  $\text{im } \varphi = G'$ , então  $\varphi$  é, pelos respectivos motivos, injetiva e sobrejetiva. Então é um isomorfismo.

### Orbitas, ciclos e grupos alternados

**Definição 2.1.31** (Órbita). Seja  $\sigma$  uma permutação de um conjunto  $A$ . Chamamos de *órbitas de*  $\sigma$  a classe de equivalência em  $A$  determinada pela relação de equivalência  $\sim$ :

$$\text{para } a, b \in A, a \sim b \iff b = \sigma^n(a), \text{ para algum } n \in \mathbb{Z}.$$

**Observação 2.1.17.** A relação apresentada na Definição 2.1.31 é, de fato, uma relação de equivalência. Como segue:

- é reflexiva, já que  $a = \sigma^0(a) \implies a \sim a$ ;
- é simétrica pois, se  $a \sim b \implies \exists n \in \mathbb{Z}$  tal que  $b = \sigma^n(a)$ , então  $a = \sigma^{-n}(b)$ . Como  $-n \in \mathbb{Z}$ , então  $b \sim a$ ;

- é transitiva, visto que  $a \sim b \implies b = \sigma^n(a)$  e  $b \sim c \implies c = \sigma^m(b)$ , para algum  $n, m \in \mathbb{Z}$ , então  $c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a) \implies a \sim c$ .

**Exemplo 2.1.10** (Órbita trivial). Já que a permutação identidade  $i$  de  $A$  leva cada elemento de  $A$  para a mesma posição, as órbitas de  $i$  são os subconjuntos de apenas um elemento de  $A$ .

**Definição 2.1.32** (Ciclo). Uma permutação  $\sigma \in S_n$  é um *ciclo* se possuir no máximo uma órbita contendo mais que um elemento. O *comprimento* de um ciclo é o número de elementos de sua maior órbita.

**Exemplo 2.1.11.** Seja a permutação

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

Como a órbita  $(1, 3, 6)$  é a única que contém mais de um elemento, essa permutação sobre o conjunto  $\{1, 2, 3, 4, 5, 6, 7, 8\}$  é um ciclo de comprimento 3.

**Observação 2.1.18** (Notação de ciclos). Podemos representar um ciclo com a notação de uma única linha, da forma

$$\mu = (1, 3, 6),$$

indicando apenas os elementos da maior órbita do ciclo. Perceba que as demais órbitas não precisam ser representadas pois serão os índices fixos da permutação.

**Exemplo 2.1.12** (Produto de ciclos). Pode-se construir uma permutação como um multiplicação de ciclos (veja a definição 2.1.11). Por exemplo,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1, 3, 6)(2, 8)(4, 7, 5).$$

**Proposição 2.1.17.** *Toda permutação  $\sigma$  de um conjunto finito é um produto de ciclos disjuntos.*

**Definição 2.1.33** (Transposição). Um ciclo de comprimento 2 é uma transposição.

**Corolário 2.1.1.** *Qualquer permutação de um conjunto finito de pelo menos dois elementos é um produto de transposições.*

**Definição 2.1.34** (Permutações pares e ímpares). Uma permutação de um conjunto finito é *par* ou *ímpar* se pode ser expressa, respectivamente, por um número par ou ímpar de produtos de transposições.

**Proposição 2.1.18.** *Uma permutação em  $S_n$  pode ser expressa como um produto de um número ímpar de transposições se e somente se não puder ser expressa como um número par de transposições e vice-versa.*

**Proposição 2.1.19.** *Seja o grupo simétrico  $S_n$  com  $n \geq 2$ . Então, a coleção de todas as permutações ímpares de  $\{1, \dots, n\}$  forma um subgrupo de  $S_n$  de ordem  $\frac{n!}{2}$ .*

**Definição 2.1.35** (Grupo alternado). O subgrupo de  $S_n$  formado pelas permutações ímpares de  $n$  símbolos é chamado *grupo alternado*  $A_n$ .

**Observação 2.1.19.** Os grupos  $S_n$  e  $A_n$  são muito importantes. O teorema de Cayley mostra que todo grupo finito  $G$  é estruturalmente idêntico a algum subgrupo de  $S_n$ , para  $n = |G|$ . Pode-se mostrar que não há formulas envolvendo apenas radicais para solucionar uma equação polinomial de grau  $n \geq 5$ . Por mais que isso não seja óbvio, esse fato se deve, na verdade, a estrutura de  $A_n$ .

### Classes laterais

Definimos classe lateral somente em relação ao núcleo de um homomorfismo mas, na verdade, pode-se definir uma classe lateral para qualquer subgrupo  $H$  de um grupo  $G$ .

**Definição 2.1.36** (classe lateral a esquerda). Seja um subgrupo  $H$  de um grupo  $G$ . O subconjunto da forma

$$aH = \{ah \mid h \in H\}$$

é dito *classe lateral a esquerda de  $H$  em  $G$* .

**Proposição 2.1.20.** A classe lateral é uma classe de equivalência para a relação de congruência

$$b = ah \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

**Observação 2.1.20.** Daí segue que, como classes de equivalência particionam um grupo, classes laterais a esquerda de um subgrupo particionam o grupo.

**Definição 2.1.37** (Índice de um subgrupo). O número de classes laterais a esquerda de um subgrupo  $H$  em um grupo  $G$  chama-se *índice de  $H$  em  $G$*  e é denotado como  $[G : H]$ .

**Observação 2.1.21.** Como há uma bijeção do subgrupo  $H$  para a classe lateral  $aH$ , a cardinalidade de  $aH$  tem de ser a mesma de  $H$ . Isto é, as classes laterais de  $H$  particionam  $G$  em partes de mesma ordem.

**Proposição 2.1.21.** Seja  $aH$  a classe lateral do subgrupo  $H$  no grupo  $G$ . Então, a ordem  $|G|$  do grupo  $G$  é dada por

$$|G| = |H|[G : H].$$

**Proposição 2.1.22** (Teorema de Lagrange). Seja  $G$  um grupo finito e  $H$  um subgrupo de  $G$ . A ordem de  $H$  divide a ordem de  $G$ .

**Definição 2.1.38** (Ordem de um elemento). Seja  $G$  um grupo. A *ordem de um elemento*  $a \in G$  é a ordem do grupo cíclico gerado por  $a$ .

**Proposição 2.1.23.** Seja um grupo  $G$  com  $p$  elementos tal que  $p$  é primo e  $a \in G$  diferente da identidade. Então  $G$  é o grupo cíclico  $\{1, a, \dots, a^{p-1}\}$  gerado por  $a$ .

**Observação 2.1.22.** Também podemos obter uma expressão para calcular a ordem de um grupo de homomorfismo. Seja  $\varphi : G \rightarrow G'$  um homomorfismo. Como as classes laterais a esquerda do núcleo de  $\varphi$  são as imagens inversas  $\varphi^{-1}$ , elas estão em uma correspondência biunívoca com a imagem. Daí segue que

$$[G : \text{núcleo } \varphi] = |\text{im } \varphi|.$$

**Proposição 2.1.24.** Seja  $\varphi : G \rightarrow G'$  um homomorfismo onde  $G$  e  $G'$  são finitos. Então

$$|G| = |\text{núcleo } \varphi| \cdot |\text{im } \varphi|.$$

**Definição 2.1.39** (classes laterais a direita). Os conjuntos da forma

$$Ha = \{ha \mid h \in H\}$$

chamam-se *classes laterais a direita de um subgrupo  $H$* . Esses são classes de equivalência para a relação de congruência a direita

$$b = ha \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

**Proposição 2.1.25.** Seja um subgrupo  $H$  de um grupo  $G$ . As seguintes afirmações são equivalentes:

- $H$  é subgrupo normal,
- $aH = Ha$  para todo  $a \in G$ .

### Restrição de um homomorfismo para um subgrupo

**Observação 2.1.23.** O objetivo dessa seção é apresentar ferramentas para analisar um subgrupo  $H$  do grupo  $G$  a fim de garantir propriedades do grupo  $G$ . No geral, os subgrupos são mais específicos e menos complexos de se trabalhar.

**Proposição 2.1.26.** Sejam  $K$  e  $H$  dois subgrupos do grupo  $G$  tal que a interseção  $K \cap H$  é um subgrupo de  $H$ . Se  $K$  é um subgrupo normal de  $G$ , então  $K \cap H$  é um subgrupo normal de  $H$ .

**Exemplo 2.1.13.** Com esse resultado, se  $G$  é finito pode-se utilizar o Teorema de Lagrange para obter informações sobre a interseção dos dois subgrupos: a interseção divide  $|H|$  e  $|K|$ . Se  $|H|$  e  $|K|$  não tem o mesmo fator de divisão, então  $K \cap H = \{1\}$ .

**Definição 2.1.40** (Restrição de um homomorfismo para um subgrupo). Sejam o homomorfismo  $\varphi : G \rightarrow G'$  e  $H$  um subgrupo de  $G$ . Uma *restrição de  $\varphi$  para o subgrupo  $H$*  é o homomorfismo  $\varphi|_H : H \rightarrow G'$  definido como

$$\varphi|_H(h) = \varphi(h), \text{ para todo } h \in H.$$

**Proposição 2.1.27.** Sejam o homomorfismo  $\varphi : G \rightarrow G'$  e  $H$  um subgrupo de  $G$ . O núcleo de uma restrição  $\varphi|_H$  é a interseção do núcleo de  $\varphi$  e  $H$ .

**Proposição 2.1.28.** Sejam  $\varphi : G \rightarrow G'$  um homomorfismo,  $H'$  um subgrupo de  $G'$  e  $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$  a imagem inversa de  $H'$ . Então

- $\varphi^{-1}(H')$  é um subgrupo de  $G$ .
- Se  $H'$  é um subgrupo normal de  $G'$ , então  $\varphi^{-1}(H')$  é um subgrupo normal de  $G$ .
- $\varphi^{-1}(H')$  contém o núcleo de  $\varphi$
- A restrição de  $\varphi$  para  $\varphi^{-1}(H')$  define um homomorfismo  $\varphi^{-1}(H') \rightarrow H'$ , de forma que o núcleo desse homomorfismo é o núcleo de  $\varphi$ .

## Produto de Grupos

**Definição 2.1.41** (Produto de grupos). Seja  $G, G'$  dois grupos. O *produto*  $G \times G'$  é um grupo formado pelo produto das componentes dos grupos  $G$  e  $G'$ , isso é, pela regra

$$(a, a'), (b, b') \mapsto (ab, a'b'),$$

onde  $a, b \in G$  e  $a', b' \in G'$ . O par  $(1, 1)$  é uma identidade e  $(a, a')^{-1} = (a^{-1}, a'^{-1})$ . A propriedade associativa é preservada em  $G \times G'$  pois também é em  $G$  e  $G'$ .

**Proposição 2.1.29.** A ordem de  $G \times G'$  é o produto das ordens de  $G$  e  $G'$ .

**Observação 2.1.24** (Projeções). O produto de grupos é composto pelos homomorfismos:

$$i : G \longrightarrow G \times G', \quad i' : G' \longrightarrow G \times G', \quad p : G \times G' \longrightarrow G, \quad p' : G \times G' \longrightarrow G',$$

definidos como

$$i(x) = (x, 1), \quad i'(x') = (1, x'), \quad p(x, x') = x, \quad p'(x, x') = x'.$$

Os mapeamentos  $i, i'$  são injetivos, já os mapeamentos  $p, p'$  são sobrejetivos, onde nu  $p = 1 \times G'$  e nu  $p' = G \times 1$ . Esses mapeamentos são chamados de *projeções*. Já que são núcleos,  $G \times 1$  e  $1 \times G'$  são subgrupos normais de  $G \times G'$ .

**Proposição 2.1.30** (Propriedades de Mapeamento dos Produtos). *Seja  $H$  um grupo qualquer. O homomorfismo  $\Phi : H \longrightarrow G \times G'$  tem correspondência biunívoca com o par  $\Phi(h) = (\varphi(h), \varphi'(h))$  de homomorfismos*

$$\varphi : H \longrightarrow G, \quad \varphi' : H \longrightarrow G'.$$

O núcleo de  $\Phi$  é a interseção (*nu*  $\varphi$ )  $\cap$  (*nu*  $\varphi'$ ).

**Observação 2.1.25.** É extremamente desejável encontrar uma relação isomorfa entre um grupo  $G$  e um produto de outros dois grupos  $H \times H'$ . Quando isso acontece, e infelizmente não são muitas as vezes, trabalhar com os grupos  $H$  e  $H'$  costumam ser mais simples que  $G$ .

**Proposição 2.1.31.** *Sejam  $r, s \in \mathbb{Z}$  não divisíveis entre si. Um grupo cíclico de ordem  $rs$  é isomorfo ao produto dos grupos cíclicos de ordem  $r$  e  $s$ .*

**Observação 2.1.26.** Em contrapartida, um grupo cíclico de ordem par 4, por exemplo, não é isomorfo ao produto de dois grupos cíclicos de ordem 2. Também não podemos afirmar nada com base no resultado anterior sobre grupos não cíclicos.

**Definição 2.1.42** (Conjunto de produtos). Sejam dois subgrupos  $A, B$  de um grupo  $G$ . Chamamos o *conjunto de produtos de elementos de  $A$  e  $B$*  por

$$AB = \{x \in G \mid x = ab \text{ para algum } a \in A \text{ e } b \in B\}.$$

**Proposição 2.1.32.** *Sejam  $H$  e  $K$  subgrupos de um grupo  $G$ .*

- Se  $H \cap K = \{1\}$ , o mapeamento de produto  $p : H \times K \longrightarrow G$  definido por  $p(h, k) = hk$  é injetivo e sua imagem é o subconjunto  $HK$ ;
- Se um dos subgrupos  $H$  ou  $K$  é um subgrupo normal de  $G$ , então os conjuntos de produtos  $HK$  e  $KH$  são iguais e  $HK$  é subgrupo de  $G$ ;
- Se ambos  $H$  e  $K$  são subgrupos normais,  $H \cap K = \{1\}$  e  $HK = G$ , então  $G$  é isomorfo ao grupo de produto  $H \times K$ .

## Aritmética Modular

**Definição 2.1.43** (Congruente modulo  $n$ ). Seja  $n \in \mathbb{N}$ . Dizemos que dois inteiros  $a, b$  são *congruentes modulo  $n$* , e escrevemos

$$a \equiv b \pmod{n},$$

se  $n$  divide  $b - a$ , ou se  $b = a + nk$  para algum inteiro  $k$ . Chamamos as classes de equivalência definidas por essa relação de *classes de equivalência módulo  $n$* , ou *classes de resíduo módulo  $n$* .

**Exemplo 2.1.14.** A classe de congruência de 0 é o subgrupo  $\bar{0}$  de todos os múltiplos de  $n$

$$\bar{0} = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}.$$

**Proposição 2.1.33.** Há  $n$  classes de congruência módulo  $n$  (denotamos esse conjunto por  $\mathbb{Z}/n\mathbb{Z}$ ), isto é, o índice  $[\mathbb{Z} : n\mathbb{Z}]$  é  $n$ . São elas

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}.$$

**Definição 2.1.44** (Soma e produto). Seja  $\bar{a}$  e  $\bar{b}$  as classes de congruência representadas pelos inteiros  $a$  e  $b$ . Define-se a *soma* como a classe de congruência de  $a + b$  e o *produto* pela classe de congruência  $ab$ , isto é,

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{e} \quad \bar{a}\bar{b} = \overline{ab}.$$

**Proposição 2.1.34.** Se  $a' \equiv b' \pmod{n}$  e  $a \equiv b \pmod{n}$ , então  $a' + b' \equiv a + b \pmod{n}$  e  $a'b' \equiv ab \pmod{n}$ .

**Observação 2.1.27.** Além disso, a soma e produto também continuam respeitando as propriedades associativas, comutativas e distributivas, desde que o mesmo se mantém para soma e multiplicação de inteiros.

**Exemplo 2.1.15.** Seja  $n = 13$ , então

$$\mathbb{Z}/13\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{12}\}.$$

Com isso,

$$(\bar{7} + \bar{9})(\bar{11} + \bar{6}) = \bar{3} \cdot \bar{4} = \bar{12}.$$

## Estrutura de grupos abelianos finitamente gerados

**Teorema 2.1.2** (Teorema fundamental dos grupos abelianos finitamente gerados). Todo grupo abeliano finitamente gerado  $G$  é isomorfo a um produto de grupos cíclicos na forma

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

onde os  $p_i$  são primos, não necessariamente distintos, os  $r_i$  são inteiros positivos e o conjunto  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ . O produto é único, exceto por possíveis rearranjos dos fatores; isso é, o número (chamado número Betti de  $G$ ) de fatores  $\mathbb{Z}$  é único e as potências de primos  $(p_i)^{r_i}$  são únicas.

**Exemplo 2.1.16.** Queremos encontrar todos os grupos abelianos de ordem 360, *a menos de isomorfismos*. Dizer *a menos de isomorfismo* significa que qualquer grupo abeliano de ordem 360 deve ser estruturalmente idêntico — isto é, isomorfo — a algum presente no conjunto solução.

*Solução.* Já que nossos grupos são da ordem finita 360, não aparecerão  $\mathbb{Z}$  no produto. Primeiro, vamos expressar 360 como um produto de potências de primos:  $360 = 2^3 3^2 5$ . Então, pelo Teorema 2.1.2, temos as seguintes possibilidades

1.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2.  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
4.  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
5.  $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
6.  $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Então, esses são os seis diferentes grupos abelianos (a menos de isomorfismos) de ordem 360.  $\triangle$

**Definição 2.1.45** (Grupo decomponível e indecomponível). Um grupo é dito *decomponível* se ele é isomorfo a um produto direto de dois subgrupos não triviais. Do contrário, é dito *indecomponível*.

**Proposição 2.1.35.** *Os grupos abelianos finitos indecomponível são exatamente os grupos cíclicos que possuem a ordem de uma potência prima.*

**Proposição 2.1.36.** *Se  $m$  divide a ordem de um grupo abeliano finito  $G$ , então  $G$  tem um subgrupo de ordem  $m$ .*

**Proposição 2.1.37.** *Se  $m$  é um quadrado inteiro livre, isto é,  $m$  não é divisível por nenhum quadrado de primo, então todo grupo abeliano de ordem  $m$  é cíclico.*

## Grupos Quociente

**Definição 2.1.46** (Produto de classes laterais). Sejam  $N \trianglelefteq G$  e as classes laterais  $\bar{a} = aN$  e  $\bar{b} = bN$ , para  $a, b \in G$ . Chamamos de *produto das classes laterais*  $\bar{a}$  e  $\bar{b}$  a classe lateral  $\bar{a}\bar{b} = abN$ , isto é, a classe lateral que contém  $ab$ .

**Proposição 2.1.38.** *Sejam  $G$  um grupo e  $S$  um conjunto qualquer com uma lei de composição. Seja também  $\varphi : G \rightarrow S$  um mapeamento sobrejetivo tal que  $\varphi(a)\varphi(b) = \varphi(ab)$  para todo  $a, b \in G$ . Então  $S$  é um grupo.*

**Definição 2.1.47** (Operação induzida por bijeção). Seja um grupo  $G$  e um conjunto  $S$  com a mesma cardinalidade de  $G$ . Por conta disso, há uma correspondência injetiva  $\leftrightarrow$  entre  $S$  e  $G$ . Podemos definir uma *operação binária sobre  $S$  induzida pela relação com os elementos de  $G$* , da forma

$$\text{se } x \leftrightarrow g_1, y \leftrightarrow g_2 \text{ e } z \leftrightarrow g_1g_2 \text{ então } xy = z,$$

onde  $x, y, z \in S$  e  $g_1g_2 \in G$ . Também, a direção  $\rightarrow$  da correspondência biunívoca  $s \leftrightarrow g$  define uma função bijetiva  $\mathcal{U}: S \rightarrow G$ , isto é

$$\text{se } \mathcal{U}(x) = g_1, \mathcal{U}(y) = g_2 \text{ e } \mathcal{U}(z) = g_1g_2 \text{ então } xy = z.$$

Assim, como  $\mathcal{U}(xy) = \mathcal{U}(z) = g_1g_2 = \mathcal{U}(x)\mathcal{U}(y)$ , a Proposição 2.1.38 garante que  $S$  é um grupo e, além disso,  $\mathcal{U}$  representa um isomorfismo que mapeia o grupo  $S$  no grupo  $G$ .

**Teorema 2.1.3** (Grupo quociente). *Seja  $\phi: G \rightarrow G'$  um homomorfismo de grupos com núcleo  $H$ . O conjunto de todas as classes laterais de  $H$  formam o chamado grupo de quociente  $G/H$  (lê-se  $G$  sobre  $H$ , não confundir com  $G$  dividido por  $H$ ), onde  $(aH)(bH) = (ab)H$ , para todo  $a, b \in G$ . Também, o mapa  $\mathcal{U}: G/H \rightarrow \phi[G]$  definido por  $\mathcal{U}(aH) = \phi(a)$  é um isomorfismo. Tanto a multiplicação de classes laterais como  $\mathcal{U}$  estão bem definidos, isto é, independem das escolhas de  $a$  e  $b$ .*

**Proposição 2.1.39.** *Seja  $H$  um subgrupo de um grupo  $G$ . Então, a multiplicação da classe lateral a esquerda é bem definida pela equação*

$$(aH)(bH) = (ab)H$$

*se e somente se  $H$  é um subgrupo normal de  $G$ .*

**Corolário 2.1.2.** *Se  $N \trianglelefteq G$ , então as classes laterais de  $N$  formam um grupo  $G/N$  sobre a operação binária  $(aN)(bN) = (ab)N$ .*

**Definição 2.1.48** (Grupo quociente). O grupo  $G/H$  no corolário 2.1.2 se chama *grupo quociente* (ou, *grupo fator*) de  $G$  por  $H$ .

**Exemplo 2.1.17.** Como  $\mathbb{Z}$  é um grupo abeliano,  $n\mathbb{Z}$  é um subgrupo normal. O corolário 2.1.2 permite a construção do grupo quociente  $\mathbb{Z}/n\mathbb{Z}$  sem citar um homomorfismo.

**Proposição 2.1.40** (Homomorfismo induzido por grupo quociente). *Seja  $H \trianglelefteq G$ . Então  $\gamma: G \rightarrow G/H$  dado por  $\gamma(x) = xH$  é um homomorfismo com núcleo  $H$ .*

**Corolário 2.1.3.** *Todo subgrupo normal de um grupo  $G$  é o núcleo de um homomorfismo.*

**Teorema 2.1.4** (Teorema fundamental do homomorfismo). *Seja  $\phi: G \rightarrow G'$  um homomorfismo de grupo com núcleo  $H$ . Então  $\phi[G]$  é um grupo e  $\mu: G/H \rightarrow \phi[G]$  dado por  $\mu(gH) = \phi(g)$  é um isomorfismo. Se  $\gamma: G \rightarrow G/H$  é o homomorfismo dado por  $\gamma(g) = gH$ , então  $\phi(g) = \mu\gamma(g)$  para cada  $g \in G$ .*

### 2.1.3 Anéis e Corpos

**Definição 2.1.49** (Anel). Um *anel*  $(R, +, \cdot)$  é um conjunto  $R$  acompanhado de duas operações binárias  $+$  e  $\cdot$  definidas sobre  $R$  tais que os seguintes axiomas são satisfeitos:

1.  $(R, +)$  é um grupo abeliano.
2. A operação  $\cdot$  é associativa.

3. Para todo  $a, b, c \in R$  vale a *lei da distributividade à esquerda* e a *lei de distributividade à direita*, respectivamente,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{e} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

**Exemplo 2.1.18.** Todo subconjunto dos números complexos que é fechado para a adição e multiplicação usual dos complexos é um anel. Por exemplo,  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  e  $(\mathbb{C}, +, \cdot)$  são todos anéis. Outro exemplo interessante é de um anel contendo apenas o elemento 0. Chamamos esse de *anel trivial*.

**Observação 2.1.28** (Notação). Da mesma forma que com os grupos, costuma-se denotar o anel  $(R, +, \cdot)$  apenas por seu conjunto  $R$ . Também, para um anel  $(R, +, \cdot)$ , chama-se sua primeira operação  $+$  de *adição do anel* e sua segunda operação  $\cdot$  de *multiplicação do anel*. O grupo  $(R, +)$  é chamado *grupo aditivo de  $R$* .

**Proposição 2.1.41.** Se  $R$  é um anel com identidade aditiva  $\vec{0}$ , então,  $\forall a \in R$ ,

$$\vec{0} \cdot a = a \cdot \vec{0} = \vec{0}.$$

*Demonstração.* Pelas propriedades do grupo  $(R, +)$ ,

$$a\vec{0} + a\vec{0} = a(\vec{0} + \vec{0}) = a\vec{0} = \vec{0} + a\vec{0}.$$

E, pela lei de cancelamento do grupo,

$$a\vec{0} + a\vec{0} = \vec{0} + a\vec{0} \implies a\vec{0} = \vec{0}.$$

De forma semelhante,

$$\vec{0}a + \vec{0}a = (\vec{0} + \vec{0})a = \vec{0}a = \vec{0} + \vec{0}a \implies \vec{0}a = \vec{0}.$$

Daí, segue que  $a\vec{0} = \vec{0}a = \vec{0}$ . □

**Proposição 2.1.42.** Se  $R$  é um anel, então, para todo  $a, b \in R$  vale

- $a(-b) = (-a)b = -(ab)$  e
- $(-a)(-b) = ab$ .

**Definição 2.1.50** (Anel associativo).

**Definição 2.1.51** (Anel comutativo).

**Definição 2.1.52** (Anel com identidade).

**Definição 2.1.53** (subanel). Um subconjunto  $S$  de um anel  $R$  é um subanel de  $R$  (escreve-se  $S \leq R$ ) se, e somente se, valem os seguintes axiomas:

1. (*Existência do elemento nulo*).  $0 \in S$ ;
2. (*Subtração fechada*).  $a - b \in S$ , para todo  $a, b \in S$ ;
3. (*Produto fechado*).  $ab \in S$ , para todo  $a, b \in S$ .

**Proposição 2.1.43.** Seja  $(S, +, \cdot)$  um subanel de  $(R, +, \cdot)$ . Então  $(S, +, \cdot)$  é um anel.

**Definição 2.1.54** (Divisor de zero). pag 2 hazenwinkel;

**Definição 2.1.55** (Domínio de integridade). Um anel  $R$  é chamado *domínio de integridade* se  $ab \neq 0$  para todo elemento não-nulo  $a, b \in R$ . Isto é, se  $R$  não possuir divisores de zero.

**Definição 2.1.56** (Unidade).

**Proposição 2.1.44** (Grupo multiplicativo). *O conjunto das unidades  $R^*$  de um anel  $R$  formam um grupo com respeito a multiplicação. Chamamos  $(R^*, \cdot)$  de grupo multiplicativo.*

**Definição 2.1.57** (Elemento idempotente). Um elemento  $e$  de um anel  $R$  é chamado *idempotente* se  $e^2 = e$ . Além disso, dois elementos idempotentes  $e, f$  são ditos *ortogonais* se  $ef = fe = 0$ .

**Exemplo 2.1.19.** Seja um anel  $R$  com identidade. Então  $0, 1 \in R$  são elementos idempotentes e ortogonais.

**Definição 2.1.58** (Anel de divisão). Um *anel de divisão*  $D$  é um anel não trivial onde todos os elementos não-nulos de  $D$  formam um grupo sobre a multiplicação.

**Proposição 2.1.45.** *Um anel não trivial  $D$  é anel de divisão se, e somente se, todo elemento não-nulo de  $D$  é uma unidade.*

### Homomorfismos de anéis

**Definição 2.1.59** (Homomorfismo de anéis). Sejam dois anéis  $(R, +, \cdot)$  e  $(R', +', \cdot')$ . Um mapa  $\phi : R \rightarrow R'$  é um *homomorfismo* se a *propriedade de homomorfismo* vale para ambas as operações, isso é, se, para todo  $a, b \in R$ ,

$$\phi(a + b) = \phi(a) +' \phi(b) \quad \text{e} \quad \phi(a \cdot b) = \phi(a) \cdot' \phi(b).$$

**Exemplo 2.1.20** (Homomorfismo trivial). Sejam os anéis  $R, R'$  e o elemento neutro  $\vec{0}$  da adição do anel  $R'$ . A aplicação  $\phi : R \rightarrow R'$  definida por  $\phi(a) = \vec{0}$ , para todo  $a \in R$ , é um homomorfismo de anéis porque

$$\phi(a + b) = \vec{0} = \vec{0} +' \vec{0} = f(a) +' f(b) \quad \text{e} \quad f(a \cdot b) = \vec{0} = \vec{0} \cdot' \vec{0} = f(a) \cdot' f(b).$$

A essa aplicação dá-se o nome *homomorfismo trivial de anéis*.

**Definição 2.1.60** (Homomorfismo injetivo e sobrejetivo). Chama-se de *homomorfismo injetivo* e *homomorfismo sobrejetivo* um homomorfismo de anéis definido, respectivamente, por uma função injetiva ou uma função sobrejetiva.

**Exemplo 2.1.21.** Seja o homomorfismo de anéis  $\phi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  tal que  $\phi(n) = (n, 0)$ , para todo  $n \in \mathbb{Z}$ . Perceba que, para cada  $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$  tem-se um único  $n \in \mathbb{Z}$  tal que  $\phi(n) = (n, 0)$ , daí,  $\phi$  é injetiva e esse é um homomorfismo injetivo. Também, seja  $\mu : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  o homomorfismo tal que  $\mu(n, m) = n$  para todo  $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ . É fácil perceber que para todo  $z \in \mathbb{Z}$ , existirá  $(z, 0) \in \mathbb{Z} \times \mathbb{Z}$ , donde  $\mu$  é um homomorfismo sobrejetivo.

**Proposição 2.1.46.** *Se  $\phi : R \rightarrow R'$  é um homomorfismo de anéis, então, para todo  $a, b \in A$ ,*

- $\phi(0_R) = 0_{R'}$ ,
- $\phi(-a) = -\phi(a)$  e
- $\phi(a - b) = \phi(a) - \phi(b)$ .

*Demonstração.* Como  $\phi(a) = \phi(a + 0_R) = \phi(a) + \phi(0_R)$ , pela propriedade de homomorfismo, então,

$$\phi(a) = \phi(a) + \phi(0_R) \implies -\phi(a) + \phi(a) = -\phi(a) + \phi(a) + \phi(0_R),$$

isto é,  $0_{R'} = \phi(0_R)$ .

Daí segue que,

$$0_{R'} = \phi(0_R) = \phi(a - a) = \phi(a) + \phi(-a),$$

e como  $0_{R'} = \phi(a) + \phi(-a)$ ,

$$\phi(-a) = -\phi(a).$$

Fica evidente que

$$\phi(a - b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b).$$

□

**Proposição 2.1.47.** Seja  $\phi : R \rightarrow R'$  um homomorfismo de anéis onde  $1_R \in R$  é identidade do produto de  $R$ . Então

- $R'$  possui identidade multiplicativa  $1_{R'}$  e  $\phi(1_R) = 1_{R'}$ ;
- se  $a \in R$  possui inversa multiplicativa  $a^{-1}$ , então  $\phi(a)^{-1} = \phi(a^{-1})$ .

**Definição 2.1.61** (Imagen de homomorfismo de anéis). A *imagem* de um homomorfismo de anéis  $\phi : R \rightarrow R'$  é o subconjunto de  $R'$

$$\text{im } \phi = \{x \in R' \mid x = \phi(a), \text{ para algum } a \in R\} = \phi(R).$$

**Proposição 2.1.48.** Seja um homomorfismo de anéis  $\phi : R \rightarrow R'$ , então a imagem  $\phi(R) \leq R'$  e, além disso, se  $S \leq R$  então  $\phi(S) \leq R'$ .

*Demonstração.* Como  $S$  é um subanel de  $R$ , então  $0_R \in S$  e  $\phi(0_R) = 0_{R'}$  implica que  $0_{R'} \in \phi(S)$ . Além disso, sejam  $a, b \in \phi(S)$ , então existem  $s_1, s_2 \in S$  tais que  $\phi(s_1) = a$ ,  $\phi(s_2) = b$  e, como  $S$  é anel,  $s_1 - s_2 \in S$  e segue que  $\phi(s_1 - s_2) \in \phi(S)$ . Como  $\phi(s_1 - s_2) = \phi(s_1) - \phi(s_2) = a - b$ ,  $a - b \in \phi(S)$ . De forma semelhante para o produto,  $a, b \in \phi(S) \implies s_1 s_2 \in S \implies ab \in \phi(S)$ . □

**Proposição 2.1.49.** Sejam  $\phi : R \rightarrow T$  e  $\mu : T \rightarrow R'$  homomorfismos de anéis. Então,  $\mu \circ \phi : R \rightarrow R'$  também é um homomorfismo de anéis.

*Demonstração.* Sejam  $a, b \in R$ . Como  $\phi$  é homomorfismo, segue que

$$\phi(a + b) = \phi(a) + \phi(b) \text{ e } \phi(ab) = \phi(a)\phi(b).$$

Portanto, aplicando  $\mu$ ,

$$\mu \circ \phi(a + b) = \mu(\phi(a) + \phi(b)) \text{ e } \mu \circ \phi(ab) = \mu(\phi(a)\phi(b)),$$

Mas como  $\mu$  também respeita a propriedade de homomorfismo, segue que

$$\begin{aligned}\mu(\phi(a) + \phi(b)) &= \mu(\phi(a)) + \mu(\phi(b)) = \mu \circ \phi(a) + \mu \circ \phi(b) \text{ e} \\ \mu(\phi(a)\phi(b)) &= \mu(\phi(a))\mu(\phi(b)) = \mu \circ \phi(a)\mu \circ \phi(b).\end{aligned}$$

□

**Definição 2.1.62** (Núcleo). O *núcleo* do homomorfismo de anéis  $\phi : R \rightarrow R'$  é o subconjunto de  $R$  formado pelos elementos que são mapeados pelo elemento nulo em  $R'$ :

$$\text{nu } \phi = \{a \in R \mid \phi(a) = 0\}.$$

**Exemplo 2.1.22.** Seja  $\phi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  definida por  $\phi(a, b) = a$ . Então  $\phi$  é um homomorfismo de anéis e

$$\text{nu } \phi = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a = 0\}.$$

**Proposição 2.1.50.** Seja um homomorfismo  $\phi : R \rightarrow R'$  com núcleo  $\text{nu } \phi$  e seja  $0_R$  o elemento nulo de  $R$ . Então  $0_R \in \text{nu } \phi$ .

**Proposição 2.1.51.** Seja  $\phi : R \rightarrow R'$  um homomorfismo de anéis. Então

- $\text{nu } \phi \leq R$ ;
- $\phi$  é injetor se, e somente se,  $\text{nu } \phi = \{0_R\}$ .

**Definição 2.1.63** (Isomorfismo de anéis).

## Corpos

**Definição 2.1.64** (Corpo). Um *corpo*  $(F, +, \cdot)$  é um anel de divisão comutativo.

**Exemplo 2.1.23.**  $\mathbb{Q}, \mathbb{R}$  e  $\mathbb{C}$  são exemplos clássicos de corpos sobre suas respectivas adições e multiplicações usuais. Note que  $\mathbb{Z}$  não é corpo, visto que suas únicas unidades são 1 e -1. No entanto,  $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$  é o menor corpo possível (a menos de isomorfismos).

**Proposição 2.1.52.** Todo domínio de integridade finito é um corpo.

**Proposição 2.1.53.** Em um corpo  $(F, +, \cdot)$ ,  $(F \setminus \{0\}, \cdot)$  é um grupo abeliano.

**Definição 2.1.65** (Subcorpo). Seja um corpo  $F$ . Um corpo  $K \leq F$  é dito *subcorpo* de  $F$  e  $F$  é dito *extensão* de  $K$ .

**Definição 2.1.66** (Elemento algébrico e transcidente). Sejam um corpo  $K$  e sua extensão  $F$ . Um elemento  $\alpha$  de  $F$  é dito *algébrico sobre  $K$*  se existe algum polinômio não-nulo  $f(x) \in K[x]$  tal que  $f(\alpha) = 0$ . Se  $\alpha \in F$  não é algébrico sobre  $K$ , então  $\alpha$  é *transcidente sobre  $K$* .

**Definição 2.1.67** (Extensão algébrica). Um corpo de extensão  $E$  de um corpo  $F$  é uma *extensão algébrica de  $F$*  se todo elemento em  $E$  é algébrico sobre  $F$ .

## 2.1.4 Módulos, Espaços Vetoriais e Álgebras

**Definição 2.1.68** (Módulo). Seja  $(R, +, \cdot)$  um anel. Um grupo abeliano  $(M, \oplus)$  é chamado de *módulo sobre um anel R* (ou, simplesmente *R-módulo*) se existir uma aplicação

$$\begin{array}{ccc} R \times M & \longrightarrow & M \\ (r, m) & \mapsto & rm \end{array},$$

chamada *multiplicação por escalar*, tal que para todo  $r, r' \in R$  e  $m, m' \in M$  valham

1.  $0_R m = 0_M$ ;
2. se  $R$  tem identidade 1, então  $1m = m$ ;
3.  $(r + r')m = (rm) \oplus (r'm)$ ;
4.  $r(m \oplus m') = (rm) \oplus (rm')$ ;
5.  $(r \cdot r')m = r(r'm)$ .

**Observação 2.1.29** (Notação). Na falta de ambiguidades, costuma-se usar 0 para se referir tanto a identidade aditiva  $0_R$  de  $R$  quanto a  $0_M$  de  $M$ . De forma semelhante, usa-se o símbolo de adição + tanto para  $\oplus$  de  $M$  quanto + de  $R$ .

**Exemplo 2.1.24** ( $\mathbb{Z}$ -módulo). Seja o anel  $(\mathbb{Z}, +, \cdot)$ . Podemos fazer qualquer grupo abeliano  $(A, +)$  virar um  $\mathbb{Z}$ -módulo através do seguinte produto escalar: para  $n \in \mathbb{Z}$  e  $a \in A$ ,

$$na = \begin{cases} a + a + \cdots + a & (n \text{ vezes}), & \text{se } n > 0 \\ 0, & \text{se } n = 0 \\ -a - a - \cdots - a & (-n \text{ vezes}), & \text{se } n < 0 \end{cases}.$$

**Proposição 2.1.54.** Seja  $M$  um grupo.  $M$  é um  $\mathbb{Z}$ -módulo se, e somente se,  $M$  é um grupo abeliano.

**Definição 2.1.69** (Submódulo). Sejam  $R$  um anel e  $M$  um  $R$ -módulo. Um  $R$ -submódulo de  $M$  é um subgrupo  $N$  de  $M$  que é fechado sob a ação dos elementos do anel, i.e., para todo  $r \in R$  e  $n \in N$ ,  $rn \in N$ .

**Proposição 2.1.55** (Critério de submódulo). Sejam  $R$  um anel e  $M$  um  $R$ -módulo. Um subconjunto  $N$  de  $M$  é um submódulo de  $M$  se, e somente se,

1.  $N \neq \emptyset$ ;
2. para todo  $r \in R$  e  $x, y \in N$ ,  $x + ry \in N$ .

**Definição 2.1.70** (Produto direto). Seja  $M_1, \dots, M_k$  uma coleção de  $R$ -módulos. A coleção de  $k$ -tuplas  $(m_1, m_2, \dots, m_k)$ , onde  $m_i \in M_i$ , com adição e ação de  $R$  definidos componente a componente, é chamado de *produto direto de  $M_1, \dots, M_k$*  e é denotado por  $M_1 \times \cdots \times M_k$ .

**Definição 2.1.71** (Módulo livre, base e grau). Um  $R$ -módulo  $L$  é dito *livre* no subconjunto  $A$  de  $L$  se, para todo elemento não-nulo  $x \in L$ , existirem únicos elementos não-nulos  $r_1, r_2, \dots, r_n \in R$  e únicos  $a_1, a_2, \dots, a_n \in A$  tais que

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n, \text{ para algum } n \in \mathbb{Z}^+.$$

Nesse caso, dizemos que  $A$  é uma *base* ou *conjunto de geradores livres* para  $L$ . Se  $R$  é um anel comutativo, a cardinalidade de  $A$  é chamada de *grau* de  $L$ .

## Álgebras

**Definição 2.1.72** (*R*-álgebra). Seja  $R$  um anel comutativo com identidade. Uma *R*-álgebra é um anel  $A$  com identidade onde existe um homomorfismo  $f : R \rightarrow A$  levando  $1_R$  para  $1_A$ , tal que o subanel  $f(R) \leq A$  está contido no centro de  $A$ .

**Exemplo 2.1.25.** Todo anel  $A$  com identidade é uma  $\mathbb{Z}$ -álgebra.

**Proposição 2.1.56.** Se o anel  $(A, +, \cdot)$  é uma *R*-álgebra pelo homomorfismo  $f : R \rightarrow A$ , então  $A$  tem um *R*-módulo através da multiplicação por escalar induzida por  $f$ , i.e.,  $r \cdot a = a \cdot r = f(r)a$ , onde  $r \in R$  e  $a \in A$ .

**Proposição 2.1.57.** Sejam  $R$  um anel comutativo com identidade e  $(A, +, \cdot)$  um anel com identidade. Então,  $A$  é uma *R*-álgebra se e somente se  $A$  é um *R*-módulo satisfazendo

$$r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$$

para todo  $r \in R$  e  $a, b \in A$ .

## Espaços Vetoriais

**Definição 2.1.73** (Espaço vetorial). Seja o grupo abeliano  $E$  um  $K$ -módulo. Se  $K$  é um corpo, dizemos que  $E$  é um espaço vetorial sobre o corpo  $K$ . Também, passamos a nos referenciar aos elementos de  $K$  por *escalares* e aos de  $E$  por *vetores*.

**Exemplo 2.1.26** ( $n$ -espaço afim sobre um corpo). Sejam  $K$  um corpo e  $n \in \mathbb{Z}^+$  um inteiro positivo. Seja o conjunto

$$K^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in K, \text{ para todo } 1 \leq i \leq n\}.$$

Tornamos  $K^n$  em um espaço vetorial ao definirmos sua adição e uma multiplicação escalar componente a componente, como segue:

$$\begin{aligned} (a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \\ \alpha(a_1, \dots, a_n) &= (\alpha a_1, \dots, \alpha a_n), \quad \alpha \in K. \end{aligned}$$

Chamamos  $K^n$  de *n-espaço afim sobre K*. Por exemplo, chamamos o *n*-espaço afim  $\mathbb{R}^n$  sobre  $\mathbb{R}$  de *n-espaço Euclidiano*, que é um espaço vetorial sobre  $K$ .

**Definição 2.1.74** (Subespaço). Um submódulo de um espaço vetorial é chamado de *subespaço*.

**Definição 2.1.75** (Independência linear). Seja  $V$  um espaço vetorial sobre  $K$ . Um subconjunto  $S$  de  $V$  é chamado de conjunto de *vetores linearmente independentes* se uma equação

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

com  $\alpha_i \in K$  e  $v_i \in S$ , para todo  $1 \leq i \leq n$ , implicar que

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0.$$

Um conjunto ordenado de vetores linearmente independentes que geram  $V$  formam uma *base* do espaço vetorial  $V$ .

**Proposição 2.1.58.** Qualquer espaço vetorial sobre  $K$  finitamente gerado é um  $K$ -módulo livre.

**Definição 2.1.76** (Dimensão). Seja  $E$  um espaço vetorial. Se  $E$  é um  $K$ -módulo livre em um subconjunto  $A \subset E$ , então o grau de  $E$  é chamado de *dimensão de  $E$* . Senão, diz-se que  $E$  tem dimensão infinita.

**Definição 2.1.77** (Extensão finita). Se um corpo de extensão  $E$  de um corpo  $F$  é de dimensão finita  $n$  como um espaço vetorial sobre  $F$ , então  $E$  é uma *extensão finita de grau  $n$  sobre  $F$* . Denotaremos por  $[E : F]$  o grau  $n$  de  $E$  sobre  $F$ .

**Proposição 2.1.59.** Se o grau de uma extensão  $[E : F]$  é  $n$ , então para qualquer elemento  $a \in E$ , os elementos  $1, \alpha, \dots, \alpha^n$  são linearmente dependentes sobre  $F$  e, portanto,  $\alpha$  é uma raiz de algum polinômio  $f(x) \in F[x]$ .

**Proposição 2.1.60.** Um corpo de extensão finito  $E$  sobre um corpo  $F$  é uma extensão algébrica de  $F$ .

**Proposição 2.1.61.** Se  $E$  é um corpo de extensão finito de um corpo  $F$  e  $K$  é um corpo de extensão finito de  $E$ , então  $K$  é um corpo de extensão finita de  $F$  e

$$[K : F] = [K : E][E : F].$$

**Definição 2.1.78** (Métrica). Seja  $E$  um espaço vetorial com dimensão finita  $n$  sobre  $\mathbb{R}$ . Métrica é uma função de dois argumentos que mapeia pares ordenados de elementos em  $E$  para um número real não negativo. Precisamente, para todo  $x, y$  e  $z \in E$ , uma função  $d(\cdot, \cdot) : E \times E \rightarrow \mathbb{R}$  é uma métrica se satisfaz os seguintes axiomas:

1.  $d(x, y) = 0$  se, e somente se,  $x = y$ ;
2.  $d(x, y) = d(y, x)$ ;
3.  $d(x, z) \leq d(x, y) + d(y, z)$ ;
4.  $d(x, y) \geq 0$

**Definição 2.1.79** (Transformação linear). Sejam  $E$  e  $V$  dois espaços vetoriais sobre um mesmo corpo  $K$ . A função  $T : E \rightarrow V$  uma *transformação linear* se, para todo  $u, v \in E$  e  $\alpha \in K$ , valem

1.  $T(u + v) = T(u) + T(v)$ ;
2.  $T(\alpha u) = \alpha T(u)$ .

Se  $E$  e  $V$  forem o mesmo espaço vetorial, dizemos que  $T$  é um *operador linear*.

**Exemplo 2.1.27.** Seja o espaço vetorial  $E \times E$  dado pelo produto direto do espaço vetorial  $E$ . A função  $T : E \times E \rightarrow E$  definida pelo mapeamento  $(e, v) \mapsto e + v$  é uma transformação linear.

**Proposição 2.1.62.** Seja  $T : E \rightarrow V$  uma transformação linear. Então vale, para todo  $\alpha \in K$  e  $u, v \in E$ ,

$$T(\alpha u + v) = \alpha T(u) + T(v).$$

**Proposição 2.1.63** (Injetividade). *Seja  $T : E \rightarrow V$  uma transformação linear. São condições suficientes para a injetividade de  $T$ :*

1. *O núcleo de  $T$  é  $\{0_E\}$ .*
2. *O núcleo de  $T$  tem dimensão 0.*

**Definição 2.1.80** (Isomorfismo). Seja  $T : E \rightarrow V$  uma transformação linear. Se  $T$  é bijetiva, então dizemos que ela é um *isomorfismo entre  $E$  e  $V$* . Também chamamos  $E$  e  $V$  de *espaços vetoriais isomorfos*.

**Teorema 2.1.5.** *Se  $E$  é um espaço vetorial de dimensão  $n$  sobre um corpo  $K$ , então  $E$  é isomorfo a  $K^n$ .*

*Demonstração.* Sejam  $e_1, \dots, e_n$  bases de  $E$  e o mapeamento  $\phi : K^n \rightarrow E$  dado por

$$\phi(\alpha_1, \dots, \alpha_n) = \alpha_1 e_1 + \dots + \alpha_n e_n.$$

Lembre que  $K^n$  também é um espaço vetorial sobre  $K$  e é fácil ver que  $\phi$  respeita os axiomas de transformação linear. Também, já que  $e_i$  é base de  $V$ ,  $\phi$  é sobrejetiva e, além disso,  $e_i$  é linearmente independente pois é base, donde o núcleo de  $\phi$  tem que ser o elemento neutro  $(0, \dots, 0)$ . Então  $\phi$  é injetiva. Segue que  $\phi$  é bijetiva e define um isomorfismo entre  $K^n$  e  $E$ .  $\square$

**Corolário 2.1.4.** *Sejam  $E$  e  $V$  dois espaços vetoriais de mesma dimensão  $n$  sobre um mesmo corpo  $K$ . Então,  $E$  é isomorfo a  $V$ .*

**Definição 2.1.81** (Operações entre transformações lineares). A *soma* de duas transformações lineares  $A, B : E \rightarrow V$  é a transformação linear  $A + B : E \rightarrow V$  definida por  $e \mapsto A(e) + B(e)$  e, se  $K$  é o corpo sobre o qual  $E$  e  $V$  estão definidos, o *produto de  $A$  por um escalar  $\alpha \in K$*  é a transformação linear  $\alpha A : E \rightarrow V$  definida por  $e \mapsto A(\alpha e)$ .

**Proposição 2.1.64** (Espaço de transformações lineares). *Seja  $\mathcal{L}(E, V)$  o conjunto de todas as transformações lineares de  $E$  em  $V$  monido das operações de soma e produto por escalar. Então  $\mathcal{L}(E, V)$  é um espaço vetorial, denominado espaço de transformações lineares de  $E$  em  $V$ .*

**Definição 2.1.82** (Espaço dual). Seja  $E$  um espaço vetorial sobre um corpo  $K$ . Chamamos o espaço das transformações lineares  $\mathcal{L}(E, K)$  de *espaço dual de  $E$*  e o denotamos por  $E^*$ . Os elementos de um espaço dual são transformações lineares do tipo  $T : E \rightarrow K$  e são chamadas de *funcionais lineares*.

**Definição 2.1.83** (Base dual). Se  $\mathcal{B} = \{e_1, \dots, e_n\}$  é uma base do espaço vetorial de dimensão finita  $E$ , então ela induz uma base para o espaço dual  $E^*$  através dos elementos  $e_i^* \in E^*$ , para  $i \in \{1, \dots, n\}$ , pelas suas ações na base  $\mathcal{B}$ :

$$e_i^*(e_j) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases} \quad 1 \leq j \leq n.$$

Chamamos a base  $\{e_1^*, \dots, e_n^*\}$  do espaço dual  $E^*$  de *base dual induzida por  $\mathcal{B}$* .

**Proposição 2.1.65.** *Se  $E$  é um espaço vetorial de dimensão finita  $n$ , então  $E^*$  tem dimensão  $n$ .*

**Definição 2.1.84** (Bidual). Já que o dual  $E^*$  é um espaço vetorial, pode-se definir um espaço dual sobre ele mesmo. Assim, chamamos de *espaço bidual* os espaço das transformações lineares  $\mathcal{L}(E^*, K)$  e o denotamos por  $E^{**}$ .

**Corolário 2.1.5.** *Se  $E$  é um espaço vetorial de dimensão finita  $n$ , então  $E^{**}$  também tem dimensão  $n$ . Além disso, como  $E$ ,  $E^*$  e  $E^{**}$  são todos espaços vetoriais de dimensão  $n$  sobre um mesmo corpo  $K$ , então  $E$  é isomorfo a  $E^*$  e a  $E^{**}$ .*

## 2.2 Álgebra Geométrica

Neste capítulo iremos introduzir o estudo da *Álgebra Geométrica* — nome definido por William Kingdon Clifford (1845-1879), o que eventualmente fez com que essa área também fosse chamada de Álgebra de Clifford [1]. Para isso, começaremos com alguns conceitos da *Teoria da Expansão* (ou, em alemão, *Ausdehnungslehre* [2]), introduzidos por Hermann Günther Grassmann (1809-1877), precursor do que hoje entendemos como a Álgebra Linear.

*“Until recently I was unacquainted with the Ausdehnungslehre, and knew only so much of it as is contained in the author’s geometrical papers (...). I may, perhaps, therefore be permitted to express my profound admiration of that extraordinary work, and my conviction that its principles will exercise a vast influence upon the future of mathematical science.”*

— Clifford, *Applications of Grassmann’s Extensive Algebra* [3]

No que se segue, entende-se que o leitor já esteja familiarizado com os conceitos básicos de Álgebra Linear tratados em um curso regular de graduação. Contudo, como deseja-se construir a teoria, vamos retomar algumas das ideias lá apresentadas.

### 2.2.1 O Produto Externo de Grassmann

Tanto em física quanto em suas aplicações na engenharia, o uso de espaços vetoriais é recorrente: separa-se as grandezas em classes de escalares e vetoriais, onde a primeira sempre trata de elementos de um corpo, representando magnitudes (massa, temperatura, distância), e a segunda de elementos do próprio espaço vetorial, que não só carregam a informação de magnitude (comprimento) como de direção e sentido (assim, podem representar, por exemplo, deslocamentos, forças e velocidades).

Pode-se interpretar geometricamente um vetor  $\mathbf{a}$  como um segmento ordenado  $(0, A)$  (como na Figura 2.1), contendo um comprimento  $|\mathbf{a}|$  (do próprio segmento  $OA$ ), uma direção (dada pela reta que passa pelos pontos  $O$  e  $A$ ) e um sentido (de  $O$  para  $A$ ). Vale ressaltar que o vetor nulo  $\vec{0}$  não possui direção ou sentido especificados.

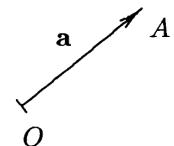


Figura 2.1: Vetor [4].

Assim, um vetor  $\mathbf{a}$  e seu oposto  $-\mathbf{a}$  tem o mesmo comprimento e direção, mas possuem sentidos opostos. Também, dois vetores são iguais se, e somente se, possuem a mesma magnitude, direção e sentido. Isso é, para  $\mathbf{a}$  e  $\mathbf{b}$  vetores,

$$\mathbf{a} = \mathbf{b} \iff |\mathbf{a}| = |\mathbf{b}| \text{ e } \mathbf{a} \uparrow\!\!\! \uparrow \mathbf{b}.$$

Aqui introduz-se a notação de mesma direção e sentido como  $\uparrow\!\!\! \uparrow$ , absorvida de [4], donde retirou-se vários dos resultados aqui mostrados. Escreveremos  $\uparrow\!\!\! \uparrow$  quando as direções forem iguais, mas o sentido oposto.

Quando se trata da operação do espaço vetorial (a adição) também temos uma interpretação geométrica. Dados dois vetores  $\mathbf{a}$  e  $\mathbf{b}$ , desenha-se um paralelogramo com lados formados por estes vetores (conforme Figura 2.2) e a diagonal deste paralelogramo será a soma de  $\mathbf{a}$  com  $\mathbf{b}$ . Perceba que a interpretação respeita a comutatividade e que compreende a subtração, dada a soma pelo oposto.

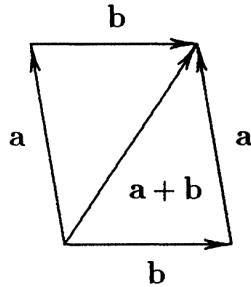


Figura 2.2: Interpretação geométrica da soma de vetores [4].

Podemos tecer uma interpretação geométrica da multiplicação por escalar associada a um espaço vetorial. Se  $\lambda \in K$  é um escalar de um espaço vetorial  $E$  sobre  $K$ , então o vetor  $\mathbf{a}$  pode ser “esticado” por um escalar  $\lambda$  (se  $\lambda > 1$ ) ou “comprimido” (se  $0 < \lambda < 1$ ). Também, se  $\lambda < 0$ , então  $\lambda\mathbf{a}$  terá sentido contrário ao de  $\mathbf{a}$ . Isso é fácil de compreender visto a associatividade do produto por escalar  $(-\lambda)\mathbf{a} = \lambda(-\mathbf{a})$ .

Assim, temos que

$$\lambda\mathbf{a} \uparrow\uparrow \mathbf{a}, \text{ se } \lambda > 0,$$

$$\lambda\mathbf{a} \uparrow\downarrow \mathbf{a}, \text{ se } \lambda < 0.$$

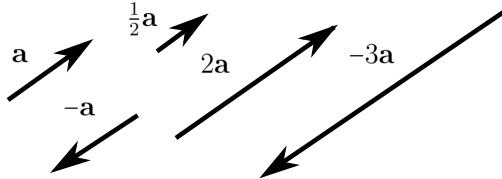


Figura 2.3: Produto por escalar.

Por fim, também temos uma interpretação para um produto entre dois vetores, que chamamos de produto escalar. Essa operação associa dois elementos  $\mathbf{a}, \mathbf{b}$  no espaço vetorial  $E$  sobre  $K$  com um elemento do corpo  $K$  que é proporcional ao produto dos módulos de  $\mathbf{a}$  e  $\mathbf{b}$  e o cosseno do ângulo  $\varphi$  entre estes dois vetores. Ou seja,

$$\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}| |\mathbf{b}| \cos \varphi, \quad \text{com } 0 \leq \varphi \leq 180^\circ.$$

Dessa forma, se o ângulo entre os vetores é  $90^\circ$  (i.e., são perpendiculares),  $\mathbf{a} \cdot \mathbf{b} = 0$ .

Com isso, estamos familiarizados com as noções de soma entre vetores (consequentemente com subtração), soma e multiplicação entre escalares (que, como são elementos de um corpo, subentendem subtração e divisão), com a de multiplicação de um vetor por um escalar (resultando em vetor) e com a noção de multiplicação entre vetores (resultando em escalar). É intuitivo se perguntar se é possível multiplicar dois vetores e obter um vetor. De fato, existe um produto do tipo em Álgebra Linear, chamado de produto vetorial, mas ele é apenas definido sobre o  $\mathbb{R}^3$ . Agora iremos introduzir um produto entre vetores mais geral (chamado *produto exterior*) mas, para isso, primeiro precisaremos abordar a natureza do elemento que ele resultará.

## Bivetores

Seja  $\mathbf{A}$  uma área de superfície plana em um plano  $P$ , dotada de um “sentido” (representado por uma flecha de rotação, assim como na Figura 2.4). Se  $\mathbf{A}'$  representa

outra área de superfície plana em outro plano  $P'$ , também dotada de um sentido, então pode-se definir a seguinte relação de equivalência:  $\mathbf{A}$  é equivalente a  $\mathbf{A}'$  se, e somente se,  $P$  e  $P'$  são paralelos, as áreas de  $\mathbf{A}$  e  $\mathbf{A}'$  são iguais e se os seus sentidos (de rotação) são o mesmo depois de transladar  $\mathbf{A}'$  em  $\mathbf{A}$  (ou seja,  $P'$  para  $P$ ). As classes de equivalência formadas por essas áreas orientadas de superfície plana são chamadas de *2-vetor* (ou, um *bivector*).

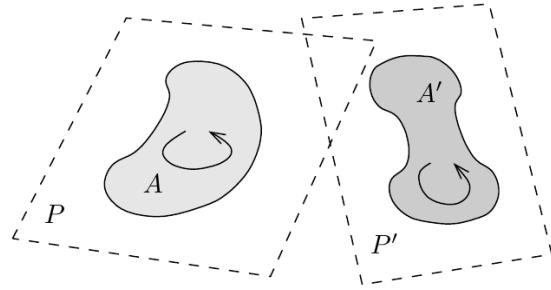


Figura 2.4: Áreas de superfícies planas  $\mathbf{A}$  e  $\mathbf{A}'$  nos respectivos planos  $P$  e  $P'$  [5].

Perceba que o bivector  $\mathbf{A}$  (de qualquer formato) pode ser representado por um paralelogramo de lados  $\mathbf{a}$  e  $\mathbf{b}$  tais que a área orientada de superfície plana assim formada seja equivalente a  $\mathbf{A}$  (vide Figura 2.5). A esse quadrilátero chamamos de *produto exterior de  $\mathbf{a}$  com  $\mathbf{b}$*  e escrevemos  $\mathbf{a} \wedge \mathbf{b}$ . Se a área de  $\mathbf{A}$  é zero, então escrevemos  $\mathbf{A} = 0$ . Assim,  $\mathbf{a} \wedge \mathbf{a} = 0$ . Também, por  $-\mathbf{A}$  expressamos a classe de equivalência de todas as áreas orientadas de superfície plana com a mesma área e no mesmo plano que  $\mathbf{A}$ , mas com um sentido de rotação contrário ao de  $\mathbf{A}$ . Perceba que  $-(\mathbf{a} \wedge \mathbf{b}) = \mathbf{b} \wedge \mathbf{a}$  (Figura 2.5). Um *bivector unidade* é um bivector  $\mathbf{A}$  com  $|\mathbf{A}| = 1$ .

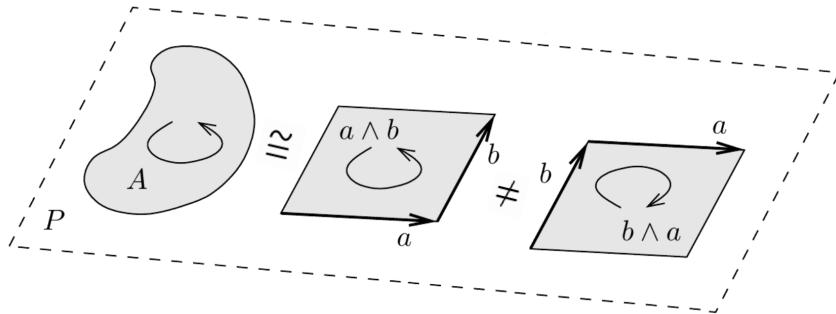


Figura 2.5: Um bivector representado por um produto exterior  $\mathbf{a} \wedge \mathbf{b}$  e  $\mathbf{b} \wedge \mathbf{a}$  [5].

### Adição de bivetores

A interpretação geométrica da adição de bivetores pode ser facilmente vista se existir um vetor comum entre os bivetores e, por sorte, em três dimensões sempre existe ao menos uma reta que intercepta dois planos quaisquer. Dessa forma, sejam  $\mathbf{A} = \mathbf{a} \wedge \mathbf{c}$  e  $\mathbf{B} = \mathbf{b} \wedge \mathbf{c}$  dois bivetores, então o bivector  $\mathbf{A} + \mathbf{B}$  é definido por

$$\mathbf{A} + \mathbf{B} = \mathbf{a} \wedge \mathbf{c} + \mathbf{b} \wedge \mathbf{c} = (\mathbf{a} + \mathbf{b}) \wedge \mathbf{c}.$$

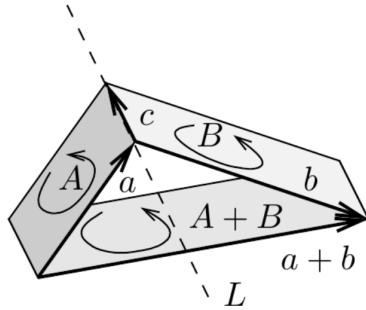


Figura 2.6: Interpretação geométrica da soma  $\mathbf{A} + \mathbf{B} = (\mathbf{a} + \mathbf{b}) \wedge \mathbf{c}$  [5].

Perceba que, como a soma de vetores é comutativa,  $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$  e, portanto, o conjunto de bivetores sobre a adição forma um grupo abeliano. Bivetores também podem ser operados com escalares do corpo dos reais, donde eles se tornam um espaço vetorial. Descrevemos esse espaço por  $\Lambda^2 \mathbb{R}^3$ . Uma base para esse espaço vetorial pode ser construída usando a base  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$  do espaço vetorial  $\mathbb{R}^3$ . As áreas orientadas de superfície plana obtidas através dos produtos exteriores  $\mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_3 \wedge \mathbf{e}_1, \mathbf{e}_2 \wedge \mathbf{e}_3$ , entre os elementos da base de  $\mathbb{R}^3$ , formam uma base para o espaço vetorial  $\Lambda^2 \mathbb{R}^3$ .

Assim, um bivetor arbitrário  $\mathbf{B}$  é uma combinação linear dos elementos da base:

$$\mathbf{B} = B_{1,2}\mathbf{e}_1 \wedge \mathbf{e}_2 + B_{3,1}\mathbf{e}_3 \wedge \mathbf{e}_1 + B_{2,3}\mathbf{e}_2 \wedge \mathbf{e}_3.$$

O produto escalar do  $\mathbb{R}^3$  é estendido para um produto simétrico bilinear no espaço dos bivetores  $\Lambda^2 \mathbb{R}^3$ , da forma

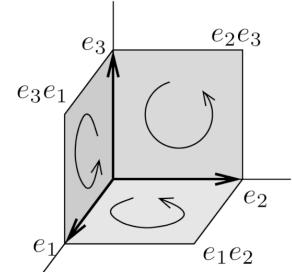


Figura 2.7: Base do  $\Lambda^2 \mathbb{R}^3$  [4].

$$\langle \mathbf{x}_1 \wedge \mathbf{x}_2, \mathbf{y}_1 \wedge \mathbf{y}_2 \rangle = \begin{vmatrix} \mathbf{x}_1 \cdot \mathbf{y}_1 & \mathbf{x}_1 \cdot \mathbf{y}_2 \\ \mathbf{x}_2 \cdot \mathbf{y}_1 & \mathbf{x}_2 \cdot \mathbf{y}_2 \end{vmatrix}.$$

Em particular,  $\langle \mathbf{a} \wedge \mathbf{b}, \mathbf{a} \wedge \mathbf{b} \rangle = |\mathbf{a}|^2 |\mathbf{b}|^2 - (\mathbf{a} \cdot \mathbf{b})^2$ . Pode-se definir a norma (ou área) de  $\mathbf{B}$  como

$$|\mathbf{B}| = \sqrt{B_{1,2}^2 + B_{3,1}^2 + B_{2,3}^2}.$$

Nesse momento podemos traçar uma relação entre o produto vetorial estudado em Álgebra Linear e o produto exterior de Grassmann. Sejam  $\mathbf{a} = a_1\mathbf{e}_1 + a_2\mathbf{e}_2 + a_3\mathbf{e}_3$  e  $\mathbf{b} = b_1\mathbf{e}_1 + b_2\mathbf{e}_2 + b_3\mathbf{e}_3$  vetores. O bivetor

$$\mathbf{a} \wedge \mathbf{b} = (a_2b_3 - a_3b_2)\mathbf{e}_2 \wedge \mathbf{e}_3 + (a_3b_1 - a_1b_3)\mathbf{e}_3 \wedge \mathbf{e}_1 + (a_1b_2 - a_2b_1)\mathbf{e}_1 \wedge \mathbf{e}_2$$

pode ser expresso como um “determinante”

$$\mathbf{a} \wedge \mathbf{b} = \begin{vmatrix} \mathbf{e}_2 \wedge \mathbf{e}_3 & \mathbf{e}_3 \wedge \mathbf{e}_1 & \mathbf{e}_1 \wedge \mathbf{e}_2 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}.$$

E relembrando, define-se o *produto vetorial de a por b* como

$$\mathbf{a} \times \mathbf{b} = (a_2b_3 - a_3b_2)\mathbf{e}_1 + (a_3b_1 - a_1b_3)\mathbf{e}_2 + (a_1b_2 - a_2b_1)\mathbf{e}_3,$$

que, por sua vez, pode ser representado pelo “determinante”

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}.$$

A interpretação geométrica de  $\mathbf{a} \times \mathbf{b}$  é um vetor perpendicular ao plano de  $\mathbf{a} \wedge \mathbf{b}$  e com norma igual a área do paralelogramo formado por  $\mathbf{a}$  e  $\mathbf{b}$ , isso é,

$$|\mathbf{a} \times \mathbf{b}| = |\mathbf{a} \wedge \mathbf{b}| = |\mathbf{a}| |\mathbf{b}| \sin \varphi,$$

onde  $0 \leq \varphi \leq 180^\circ$  é o ângulo entre  $\mathbf{a}$  e  $\mathbf{b}$ .

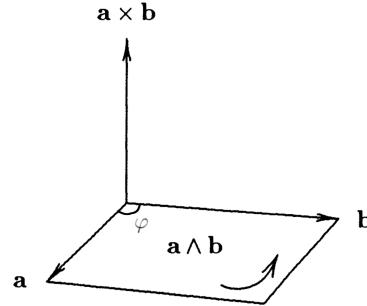


Figura 2.8: Interpretação geométrica de  $\mathbf{a} \times \mathbf{b}$  [4].

### Trivetores

O produto exterior  $\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c}$  de três vetores  $\mathbf{a} = a_1 \mathbf{e}_1 + a_2 \mathbf{e}_2 + a_3 \mathbf{e}_3$ ,  $\mathbf{b} = b_1 \mathbf{e}_1 + b_2 \mathbf{e}_2 + b_3 \mathbf{e}_3$  e  $\mathbf{c} = c_1 \mathbf{e}_1 + c_2 \mathbf{e}_2 + c_3 \mathbf{e}_3$  representa o volume orientado do paralelepípedo com lados  $\mathbf{a}$ ,  $\mathbf{b}$  e  $\mathbf{c}$ :

$$\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3.$$

Esse é um elemento do espaço vetorial unidimensional de trivetores (ou, 3-vetores)  $\Lambda^3 \mathbb{R}^3$ , com base  $\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3$ . O produto exterior é associativo, isso é,

$$(\mathbf{a} \wedge \mathbf{b}) \wedge \mathbf{c} = \mathbf{a} \wedge (\mathbf{b} \wedge \mathbf{c}),$$

e antissimétrica:

$$\mathbf{a} \wedge \mathbf{b} \wedge \mathbf{c} = \mathbf{b} \wedge \mathbf{c} \wedge \mathbf{a} = \mathbf{c} \wedge \mathbf{a} \wedge \mathbf{b} = -\mathbf{c} \wedge \mathbf{b} \wedge \mathbf{a} = -\mathbf{a} \wedge \mathbf{c} \wedge \mathbf{b} = -\mathbf{b} \wedge \mathbf{a} \wedge \mathbf{c}, \quad \forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^3$$

O produto exterior dos elementos da base  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$  do  $\mathbb{R}^3$  é o volume orientado unitário  $\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3 \in \Lambda^3 \mathbb{R}^3$ . O volume (ou norma)  $|\mathbf{V}|$  de um trivector  $\mathbf{V} = V \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3$  é  $|V|$ , isso é,  $|V \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3| = V$  para  $V \geq 0$  e  $|V \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3| = -V$  para  $V < 0$ .

### O dual de Hodge

Como tanto o espaço vetorial do  $\mathbb{R}^3$  quanto o  $\Lambda^2 \mathbb{R}^3$  possuem dimensão finita igual a 3 e ambos são definidos sobre o corpo dos reais  $\mathbb{R}$ , então eles são isomorfos. Pode-se usar a métrica sobre o espaço vetorial  $\mathbb{R}^3$  para gerar um isomorfismo entre

estes espaços vetoriais. O dual de Hodge relaciona um vetor  $\mathbf{a} \in \mathbb{R}^3$  a um bivetor  $*\mathbf{a} \in \Lambda^2 \mathbb{R}^3$ , através de

$$\mathbf{b} \wedge *\mathbf{a} = (\mathbf{b} \cdot \mathbf{a}) \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3, \quad \text{para todo } \mathbf{b} \in \mathbb{R}^3.$$

O dual de Hodge depende não apenas da métrica (induzida pelo produto interno) mas também da escolha da orientação. Costuma-se usar a mão direita e a base ortonormal  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ .

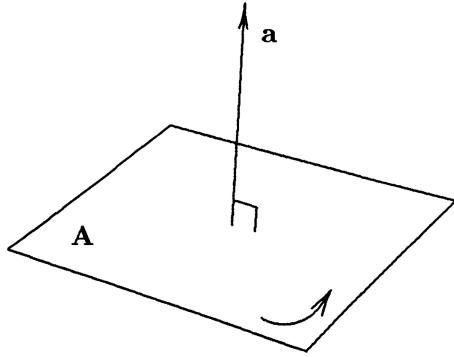


Figura 2.9: O vetor  $\mathbf{a}$  e seu dual  $\mathbf{A} = \mathbf{a}\mathbf{e}_{123}$

Assim, associamos a cada vetor

$$\mathbf{a} = a_1 \mathbf{e}_1 + a_2 \mathbf{e}_2 + a_3 \mathbf{e}_3 \in \mathbb{R}^3$$

um bivetor

$$\mathbf{A} = *\mathbf{a} = a_1 \mathbf{e}_2 \wedge \mathbf{e}_3 + a_2 \mathbf{e}_3 \wedge \mathbf{e}_1 + a_3 \mathbf{e}_1 \wedge \mathbf{e}_2 \in \bigwedge^2 \mathbb{R}^3.$$

Usando a métrica induzida sobre o espaço de bivetores  $\Lambda^2 \mathbb{R}^3$ , pode-se estender o dual de Hodge para um mapeamento que associa um bivetor  $\mathbf{A} \in \Lambda^2 \mathbb{R}^3$  com um vetor  $*\mathbf{A} \in \mathbb{R}^3$ , definido por

$$\mathbf{B} \wedge *\mathbf{A} = \langle \mathbf{B}, \mathbf{A} \rangle \mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3, \quad \text{para todo } \mathbf{B} \in \bigwedge^2 \mathbb{R}^3.$$

Usando esta dualidade, pode-se escrever a relação entre o produto externo e o produto vetorial como

$$\mathbf{a} \wedge \mathbf{b} = *(\mathbf{a} \times \mathbf{b}), \quad \text{e} \quad \mathbf{a} \times \mathbf{b} = *(\mathbf{a} \wedge \mathbf{b}).$$

## 2.2.2 Álgebra Exterior $\Lambda \mathbb{R}^3$

A álgebra exterior  $\Lambda \mathbb{R}^3$  do espaço vetorial  $\mathbb{R}^3$  foi construída por Grassmann em 1844, em sua Teoria da Expansão [2], e é uma soma direta dos subespaços de escalares ( $\mathbb{R}$ , com base  $\{1\}$ ), de vetores ( $\mathbb{R}^3$ , com base  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$ ), de bivetores ( $\Lambda^2 \mathbb{R}^3$ , com base  $\{\mathbf{e}_1 \wedge \mathbf{e}_2, \mathbf{e}_2 \wedge \mathbf{e}_3, \mathbf{e}_3 \wedge \mathbf{e}_1\}$ ) e de trivetores ( $\Lambda^3 \mathbb{R}^3$ , com base  $\{\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3\}$ ). Podemos reescrever  $\mathbb{R} = \Lambda^0 \mathbb{R}^3$  e  $\mathbb{R}^3 = \Lambda^1 \mathbb{R}^3$  e, assim, escrevemos a álgebra exterior como

$$\Lambda \mathbb{R}^3 = \bigwedge^0 \mathbb{R}^3 \oplus \bigwedge^1 \mathbb{R}^3 \oplus \bigwedge^2 \mathbb{R}^3 \oplus \bigwedge^3 \mathbb{R}^3.$$

Como as respectivas dimensões de  $\mathbb{R}$ ,  $\mathbb{R}^3$ ,  $\Lambda^2 \mathbb{R}^3$  e  $\Lambda^3 \mathbb{R}^3$  são 1, 3, 3, 1, a dimensão de  $\Lambda \mathbb{R}^3$  é 8.

A álgebra exterior  $\Lambda \mathbb{R}^3$  é uma álgebra associativa com unidade 1 e satisfazendo

$$\mathbf{e}_i \wedge \mathbf{e}_i = 0 \quad \text{e} \quad \mathbf{e}_i \wedge \mathbf{e}_j = -\mathbf{e}_j \wedge \mathbf{e}_i, \text{ para } i \neq j$$

para a base  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$  do espaço vetorial  $\mathbb{R}^3$ . O produto exterior de dois elementos homogêneos satisfaçõa

$$\mathbf{a} \wedge \mathbf{b} \in \bigwedge^{i+j} \mathbb{R}^3 \text{ para } \mathbf{a} \in \bigwedge^i \mathbb{R}^3, \mathbf{b} \in \bigwedge^j \mathbb{R}^3.$$

### 2.2.3 Álgebra Geométrica $\mathcal{C}\ell_3$

A álgebra exterior  $\Lambda \mathbb{R}^3$  contém uma cópia do  $\mathbb{R}^3$ , o que permite a aplicações de diversos cálculos para a geometria do  $\mathbb{R}^3$  [4]. Porém, um inconveniente que aparece quando se trabalha com  $\Lambda \mathbb{R}^3$  é que essa álgebra não preserva a norma, isso é,  $|\mathbf{a} \wedge \mathbf{b}| \leq |\mathbf{a}| |\mathbf{b}|$ . Encontrar um novo produto entre vetores de forma que se preservasse a igualdade  $|“\mathbf{ab}”| = |\mathbf{a}| |\mathbf{b}|$  possibilitaria, por exemplo, a representação de rotações como operações nesta álgebra.

#### O produto de Clifford

Um novo tipo de produto entre vetores, chamado *produto de Clifford dos vetores*  $\mathbf{a}$  e  $\mathbf{b}$  é obtido pela adição do escalar  $\mathbf{a} \cdot \mathbf{b}$  e do bivetor  $\mathbf{a} \wedge \mathbf{b}$ :

$$\mathbf{ab} = \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \wedge \mathbf{b}.$$

Estamos unindo um produto comutativo com um anticomutativo. Por conta disso, temos que

$$\mathbf{ba} = \mathbf{a} \cdot \mathbf{b} - \mathbf{a} \wedge \mathbf{b},$$

o que implica que  $\mathbf{a} \cdot \mathbf{b} = \frac{1}{2}(\mathbf{ab} + \mathbf{ba})$  e  $\mathbf{a} \wedge \mathbf{b} = \frac{1}{2}(\mathbf{ab} - \mathbf{ba})$ .

Como o produto interno e o exterior zeram quando os vetores são, respectivamente, perpendiculares e paralelos, segue que dois vetores  $\mathbf{a}$  e  $\mathbf{b}$  são paralelos se seu produto comuta, isso é,  $\mathbf{ab} = \mathbf{ba}$  e são perpendiculares quando seu produto anticomuta, isso é,  $\mathbf{ab} = -\mathbf{ba}$ .

Pode-se calcular o produto  $\mathbf{abba}$  para obter que  $\mathbf{a}^2 \mathbf{b}^2 = (\mathbf{a} \cdot \mathbf{b})^2 - (\mathbf{a} \wedge \mathbf{b})^2$  e usar que  $(\mathbf{a} \wedge \mathbf{b})^2 = -|\mathbf{a} \wedge \mathbf{b}|^2$  para obter a identidade

$$\mathbf{a}^2 \mathbf{b}^2 = (\mathbf{a} \cdot \mathbf{b})^2 + |\mathbf{a} \wedge \mathbf{b}|^2$$

que implica que  $(\mathbf{ab})^2 = (|\mathbf{a}| |\mathbf{b}| \cos \varphi)^2 + (|\mathbf{a}| |\mathbf{b}| \sin \varphi)^2 = |\mathbf{a}|^2 |\mathbf{b}|^2$ , isso é, se e somente se

$$|\mathbf{ab}| = |\mathbf{a}| |\mathbf{b}|.$$

#### Base de $\mathcal{C}\ell_3$

Assim, através desse novo produto, definimos uma base para a chamada Álgebra Geométrica  $\mathcal{C}\ell_3$  do espaço Euclidiano  $\mathbb{R}^3$ . A base  $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$  da cópia do espaço vetorial  $\mathbb{R}^3$  dentro de  $\mathcal{C}\ell_3$  satisfará as seguintes propriedades

$$\mathbf{e}_i \mathbf{e}_j = -\mathbf{e}_j \mathbf{e}_i, \text{ para } i \neq j \quad \text{e} \quad \mathbf{e}_i \mathbf{e}_i = 1,$$

que dizem respeito respectivamente a ortogonalidade entre diferentes elementos da base e ao paralelismo entre dois vetores iguais. Clifford inventou essas novas regras partindo da álgebra exterior em 1882, buscando uma álgebra associativa que mantivesse  $\mathbf{e}_i \mathbf{e}_j = \mathbf{e}_i \wedge \mathbf{e}_j$  e, inicialmente, em 1878, propôs um produto que levava  $\mathbf{e}_i \mathbf{e}_i = -1$ .

Pode-se associar a base do espaço vetorial de  $\mathcal{Cl}_3$  com a base de  $\bigwedge \mathbb{R}^3$ , pois da mesma forma que em  $\bigwedge \mathbb{R}^3$ , construímos a Álgebra Geométrica  $\mathcal{Cl}_3$  como as somas diretas

$$\mathcal{Cl}_3 = \mathbb{R} \oplus \mathbb{R}^3 \oplus \bigwedge^2 \mathbb{R}^3 \oplus \bigwedge^3 \mathbb{R}^3.$$

Essa separação em bases induz uma estrutura de multivetor na Álgebra Geométrica  $\mathcal{Cl}_3$ . Essa estrutura de multivetor é única, isso é, um elemento arbitrário  $u \in \mathcal{Cl}_3$  pode ser decomposto unicamente como uma soma de  $k$ -vetores, as  $k$ -vetores partes  $\langle u \rangle_k$  de  $u$ , escritas

$$u = \langle u \rangle_0 + \langle u \rangle_1 + \langle u \rangle_2 + \langle u \rangle_3, \text{ onde } \langle u \rangle_k \in \bigwedge^k \mathbb{R}^3.$$

## Reflexões e rotações

Como o produto entre vetores de  $\mathcal{Cl}_3$  preserva a métrica, podemos construir rotações operando seus elementos.

Da identidade  $\mathbf{a} \cdot \mathbf{r} = \frac{1}{2}(\mathbf{a}\mathbf{r} + \mathbf{r}\mathbf{a})$  obtemos, ao multiplicarmos toda a expressão por  $\mathbf{a}^{-1}$  e reorganizando seus termos, o elemento  $\mathbf{a}\mathbf{r}\mathbf{a}^{-1} = 2(\mathbf{a} \cdot \mathbf{r})\mathbf{a}^{-1} - \mathbf{r}$ . No espaço Euclidiano  $\mathbb{R}^3$  os vetores  $\mathbf{r}$  e  $\mathbf{a}\mathbf{r}\mathbf{a}^{-1}$  são simétricos com respeito ao eixo  $\mathbf{a}$  (veja a Figura 2.10). O elemento oposto de  $\mathbf{a}\mathbf{r}\mathbf{a}^{-1}$  é o vetor

$$-\mathbf{a}\mathbf{r}\mathbf{a}^{-1} = \mathbf{r} - 2\frac{\mathbf{a} \cdot \mathbf{r}}{\mathbf{a}^2}\mathbf{a}$$

obtido pela reflexão de  $\mathbf{r}$  através do plano perpendicular a  $\mathbf{a}$ , isto é, pelo dual  $\mathbf{a}\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3$ .

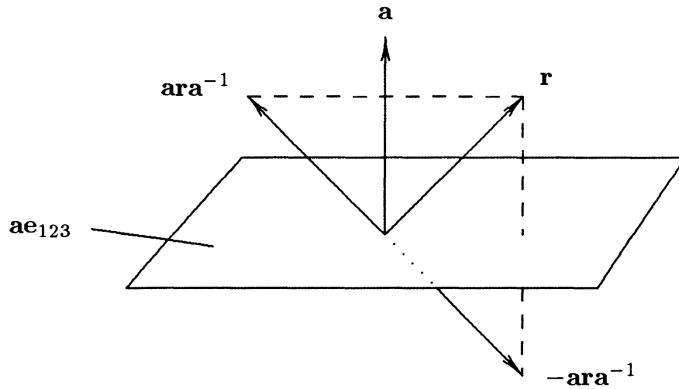


Figura 2.10: Representação da reflexão de  $\mathbf{r}$  por  $\mathbf{a}$  [4].

Duas reflexões sucessivas nos planos perpendiculares a  $\mathbf{a}$  e  $\mathbf{b}$  resultam em uma rotação  $\mathbf{r} \rightarrow \mathbf{b}(\mathbf{a}\mathbf{r}\mathbf{a}^{-1})\mathbf{b}^{-1}$  ao redor do eixo que é perpendicular a ambos  $\mathbf{a}$  e  $\mathbf{b}$  (veja Figura 2.11).

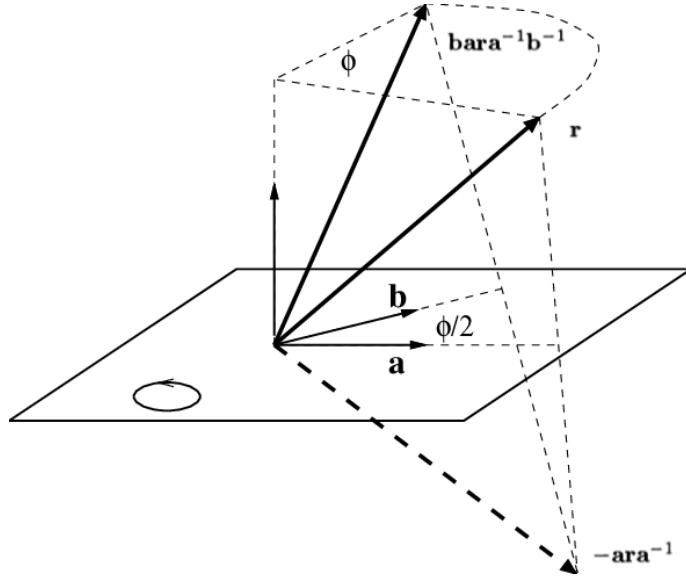


Figura 2.11: Representação da rotação por duas reflexões

### Partes pares e ímpares

Assim como a álgebra exterior, a  $\mathcal{C}\ell_3$  é uma soma direta de dois subespaços que chamamos de

1. parte par  $\mathcal{C}\ell_3^+ : \Lambda^0 \mathbb{R}^3 \oplus \Lambda^2 \mathbb{R}^3$  e
2. a parte ímpar  $\mathcal{C}\ell_3^- : \Lambda^1 \mathbb{R}^3 \oplus \Lambda^3 \mathbb{R}^3$ .

Para ambas as álgebras, a parte par também é uma subálgebra. A subálgebra par  $(\Lambda \mathbb{R}^3)^+ = \mathbb{R} \oplus \Lambda^2 \mathbb{R}^3$  de  $\Lambda \mathbb{R}^3$  é comutativa, porém, a subálgebra  $\mathcal{C}\ell_3^+ = \mathbb{R} \oplus \Lambda^2 \mathbb{R}^3$  de  $\mathcal{C}\ell_3$  não é.

Na verdade, a subálgebra  $\mathcal{C}\ell_3^+$  nos interessa bastante. Os elementos gerados por  $1 \in \mathbb{R}$  e pelos bivetores  $\mathbf{e}_1\mathbf{e}_2$ ,  $\mathbf{e}_3\mathbf{e}_1$  e  $\mathbf{e}_2\mathbf{e}_3 \in \Lambda^2 \mathbb{R}^3$  são chamados pares, porque são produtos de um número par de vetores (lembrando 0 é par). Esses elementos pares são escritos como

$$w + x\mathbf{e}_2\mathbf{e}_3 + y\mathbf{e}_3\mathbf{e}_1 + z\mathbf{e}_1\mathbf{e}_2$$

e formam um subespaço real

$$\mathbb{R} \oplus \bigwedge^2 \mathbb{R}^3 = \{w + x\mathbf{e}_2\mathbf{e}_3 + y\mathbf{e}_3\mathbf{e}_1 + z\mathbf{e}_1\mathbf{e}_2 \mid w, x, y, z \in \mathbb{R}\}$$

que é fechado sobre a multiplicação e, portanto, o subespaço  $\mathbb{R} \oplus \Lambda^2 \mathbb{R}^3$  é de fato uma subálgebra. Na verdade, essa subálgebra é isomorfa ao anel de divisão dos quatérnios  $\mathbb{H}$  (que abordaremos melhor na próxima seção) através da correspondência

$$\mathbf{e}_2\mathbf{e}_3 \rightarrow i, \quad \mathbf{e}_1\mathbf{e}_2 \rightarrow j, \quad \mathbf{e}_3\mathbf{e}_1 \rightarrow k.$$

## 2.2.4 Álgebra dos Quatérnios

William Rowan Hamilton foi uma criança extremamente precoce. De origem irlandesa, viveu entre 1805 e 1865 e aos três anos de idade já lia perfeitamente em inglês [6]. Devido a morte antecipada de seus pais, teve como orientador um tio linguista e aos seus cinco anos já sabia latim e hebraico. Até os dez anos já era familiarizado com italiano, francês, árabe, sânscrito, persa, caldeu e algumas outras línguas orientais. Ainda criança, Hamilton demonstrou grande interesse pela matemática, influenciado por autores como Newton e Laplace caminhava a passos largos para o mundo da física e astronomia. Trata-se de um dos grandes nomes da ciência do século XIX [7].

Hamilton percebeu que uma notação utilizada na teoria dos números complexos não era a mais adequada, pois a expressão  $a + bi$  não era realmente uma soma, isto é, não é como somar dois números reais que pertencem a mesma dimensão — o que dá sentido a soma. Dessa forma, Hamilton estava convencido de que o sinal ‘+’ é um equívoco, um acidente histórico, e que as duas partes não podiam ser naturalmente somadas. A partir deste pensamento, publicou em 1833 a teoria de números complexos formalmente como conhecemos hoje, definindo a soma e produto em pares ordenados da forma

$$(a, b) + (c, d) = (a + b, c + d)$$

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

Visto sua proximidade com a física, Hamilton percebeu como esta nova abordagem permitiria uma visão dos números complexos como entidades orientadas no plano e se perguntou como seria esta relação se fosse expandida para o espaço tridimensional. Infelizmente as respostas não foram fáceis e por dez anos trabalhou tentando desenvolver ternas que pudessem ser multiplicadas com as propriedades que desejava. Na verdade, Hamilton jamais poderia encontrar sua terna, como é apresentado em [4].

Em 1843, Hamilton andava ao lado de sua esposa na ponte Brougham sobre o Royal Canal a caminho de presidir uma reunião do Conselho da Real Sociedade da Irlanda e dividia-se entre conversas ocasionais e no pensar sobre seu trabalho. Lá teve um *insight*: percebeu que poderia ter sua generalização se utilizasse quádruplas em vez de ternas e ignorasse a comutatividade para a multiplicação. Percebeu que para quádruplas  $a + bi + cj + dk$  teria as leis

$$i^2 = j^2 = k^2 = ijk = -1. \quad (2.1)$$

**Definição 2.2.1** (Quatérnio). Seja  $\{i, j, k\}$  a base do  $\mathbb{R}^3$ . Um *quatérnio* é definido como um elemento da forma

$$q = q_0 + \mathbf{q}_v,$$

onde  $q_0 \in \mathbb{R}$  é um escalar e  $\mathbf{q}_v = q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$  é um vetor de  $\mathbb{R}^3$ .

Ou seja, todo elemento  $q$  da forma  $q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$  é um quatérnio e a medida que variamos os valores dos coeficientes reais  $q_0, q_1, q_2$  e  $q_3$  independentemente uns dos outros geramos o *conjunto numérico dos Quatérnios*  $\mathbb{H}$ .

**Definição 2.2.2** (Adição). Dados dois quatérnios  $p = p_0 + \mathbf{p}_v$  e  $q = q_0 + \mathbf{q}_v$  em  $\mathbb{H}$ , define-se a adição de  $p$  a  $q$  como

$$p + q = (p_0 + q_0) + (\mathbf{p}_v + \mathbf{q}_v)$$

**Proposição 2.2.1.** *O conjunto  $\mathbb{H}$  é fechado para adição.*

*Demonstração.* Considerando  $r = p + q$ , podemos escrever o elemento  $r$  como

$$r = r_0 + \mathbf{r}_v$$

onde sua parte escalar é dada por  $r_0 = p_0 + q_0$  e sua parte vetorial é dada por  $\mathbf{r}_v = \mathbf{p}_v + \mathbf{q}_v$ .  $\square$

**Proposição 2.2.2.**  *$(\mathbb{H}, +)$  é um grupo abeliano.*

*Demonstração.* Dados  $p, q, r \in \mathbb{H}$ , temos que  $(p+q)+r = [(p_0+\mathbf{p}_v)+(q_0+\mathbf{p}_v)]+(r_0+\mathbf{r}_v) = [(p_0+q_0)+(\mathbf{p}_v+\mathbf{q}_v)]+(r_0+\mathbf{r}_v) = [(p_0+q_0+r_0)+(\mathbf{p}_v+\mathbf{q}_v+\mathbf{r}_v)] = [(p_0+q_0+r_0)+(\mathbf{p}_v+\mathbf{q}_v+\mathbf{r}_v)] = \{(p_0+(q_0+r_0)) + [\mathbf{p}_v+(\mathbf{q}_v+\mathbf{r}_v)]\} = (p_0+\mathbf{p}_v) + [(q_0+r_0)+(\mathbf{q}_v+\mathbf{r}_v)] = (p_0+\mathbf{p}_v) + [(q_0+\mathbf{q}_v) + (r_0+\mathbf{r}_v)] = p + (q + r)$ , donde é associativa.

Também temos que  $p+q = (p_0+\mathbf{p}_v) + (q_0+\mathbf{q}_v) = (p_0+q_0) + (\mathbf{p}_v+\mathbf{q}_v) = (q_0+p_0) + (\mathbf{q}_v+\mathbf{p}_v) = q+p$ , isso é, é comutativa.

Seja  $0_{\mathbb{H}} = 0 + \mathbf{0}_v$ . Como  $p + 0_{\mathbb{H}} = (p_0 + \mathbf{p}_v) + (0 + \mathbf{0}_v) = (p_0 + 0) + (\mathbf{p}_v + \mathbf{0}_v) = (0 + p_0) + (\mathbf{0}_v + \mathbf{p}_v) = p_0 + \mathbf{p}_v = p$ , então existe um elemento neutro, a saber,  $0_{\mathbb{H}}$ .

Também existe elemento oposto, afinal,  $p + (-p) = (p_0 + \mathbf{p}_v) + (-p_0 - \mathbf{p}_v) = [p_0 + (-p_0)] + [\mathbf{p}_v + (-\mathbf{p}_v)] = (p_0 - p_0) + (\mathbf{p}_v - \mathbf{p}_v) = 0 + \mathbf{0}_v = 0_{\mathbb{H}}$ .  $\square$

**Definição 2.2.3** (Multiplicação por escalar). Dado um quatérnio  $q = q_0 + \mathbf{q}_v \in \mathbb{H}$  e uma constante escalar real  $\alpha \in \mathbb{R}$ , define-se a multiplicação de  $q$  pelo escalar  $\alpha$  da forma

$$\alpha q = (\alpha q_0) + (\alpha \mathbf{q}_v)$$

**Proposição 2.2.3.** *O conjunto  $\mathbb{H}$  é fechado para a multiplicação de escalares reais.*

*Demonstração.* Podemos considerar tal multiplicação como o elemento

$$r = r_0 + \mathbf{r}_v$$

onde sua parte escalar é dada por  $r_0 = \alpha q_0 \in \mathbb{R}$  e sua parte vetorial é dada por  $\mathbf{r}_v = \alpha \mathbf{q}_v \in \mathbb{R}^3$ .  $\square$

**Proposição 2.2.4.**  *$\mathbb{H}$  é um espaço vetorial sobre o corpo  $\mathbb{R}$ .*

*Demonstração.* Dados os números reais  $\alpha, \beta$  e os quatérnios  $p$  e  $q$ , temos que  $(\alpha\beta)q = (\alpha\beta)(q_0 + \mathbf{q}_v) = \alpha\beta q_0 + \alpha\beta \mathbf{q}_v = \alpha(\beta q_0 + \beta \mathbf{q}_v) = \alpha(\beta q)$ , então é associativa.

Também, como  $1q = 1(q_0 + \mathbf{q}_v) = (1q_0 + 1\mathbf{q}_v) = q_0 + \mathbf{q}_v = q$ , então  $1q = q$ .

A operação também é distributiva em relação à soma, pois por  $(\alpha + \beta)q = ((\alpha + \beta)q_0 + (\alpha + \beta)\mathbf{q}_v)$ ,  $((\alpha + \beta)q_0 + (\alpha + \beta)\mathbf{q}_v) = \alpha(q_0 + \mathbf{q}_v) + \beta(q_0 + \mathbf{q}_v) = \alpha q + \beta q$ . Analogamente para  $\alpha q + \beta q$ . Agora, por  $\alpha(p + q) = \alpha p + \alpha q$ . Aplicando as devidas distributividades, temos que  $\alpha p + \alpha q = (\alpha p_0 + \alpha \mathbf{p}_v) + (\alpha q_0 + \alpha \mathbf{q}_v) = \alpha p + \alpha q$ . Analogamente para  $\alpha p + \alpha q$ .  $\square$

**Proposição 2.2.5.**  $\mathbb{H} \simeq \mathbb{R}^4$ .

Na verdade, historicamente esse isomorfismo vem de que o cálculo vetorial como conhecemos hoje, onde define-se  $\mathbb{R}^4$ , é mera simplificação das ideias de Hamilton sobre quatérnios. Simplificação feita por Josiah Willard Gibbs (1839 – 1903) em um conjunto de notas para seus estudantes de física-matemática intitulado Elements of Vector Analysis [7].

Assim como os complexos, os quatérnios também tem conjugado.

**Definição 2.2.4** (Quatérnio conjugado). Seja  $q = q_0 + \mathbf{q}_v \in \mathbb{H}$ , define-se seu *conjugado* como  $q^* = q_0 - \mathbf{q}_v$ .

### Produto algébrico de quatérnios

Tendo as estruturas algébricas já estabelecidas, pode-se construir uma terceira operação dos quatérnios, baseando-se em [8]. Trata-se do *produto algébrico dos quatérnios*, que causou os dez anos de trabalho para Hamilton e que torna sua álgebra um tanto não trivial por conta da falta de comutatividade.

Suponha dois elementos  $p = p_0 + \mathbf{p}_v$  e  $q = q_0 + \mathbf{q}_v \in \mathbb{H} \setminus 0$ . Sabe-se que podemos escrever  $\mathbf{p}_v = p_1\mathbf{i} + p_2\mathbf{j} + p_3\mathbf{k}$  e  $\mathbf{q}_v = q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$ . Se multiplicarmos os dois elementos termo a termo, como na propriedade distributiva, teremos:

$$\begin{aligned} pq &= (p_0 + ip_1 + jp_2 + kp_3)(q_0 + iq_1 + jq_2 + kq_3) \\ &= (p_0q_0 + p_0 + ip_0q_1 + p_1q_0) + \mathbf{j}(p_0q_2 + p_2q_0) \\ &\quad + \mathbf{k}(p_0q_3 + p_3q_0) + \mathbf{i}^2p_1q_1 + \mathbf{j}^2p_2q_2 + \mathbf{k}^2p_3q_3 + \mathbf{ij}p_1q_2 + \mathbf{ji}p_2q_1 \\ &\quad + \mathbf{ik}p_1q_3 + \mathbf{ki}p_3q_1 + \mathbf{jk}p_2q_3 + \mathbf{kj}p_3q_2 \end{aligned} \tag{2.2}$$

Mas podemos utilizar das regras definidas na equação 2.1 para simplificar essa expressão. Historicamente, os produtos dos versores a seguir foram definidos por Hamilton por construção a partir de seus três planos retangulares intersectados utilizando de rotações [9], mas aproveitaremos a correspondência de  $i, j, k$  com os elementos de  $\mathcal{C}\ell_3$ . Temos que

$$\mathbf{ij} \rightarrow \mathbf{e}_2\mathbf{e}_3\mathbf{e}_1\mathbf{e}_2 = \mathbf{e}_3\mathbf{e}_1 \rightarrow \mathbf{k} = -\mathbf{ji}$$

$$\mathbf{jk} \rightarrow \mathbf{e}_1\mathbf{e}_2\mathbf{e}_3\mathbf{e}_1 = \mathbf{e}_2\mathbf{e}_3 \rightarrow \mathbf{i} = -\mathbf{kj}$$

$$\mathbf{ki} \rightarrow \mathbf{e}_3\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3 = \mathbf{e}_1\mathbf{e}_2 \rightarrow \mathbf{j} = -\mathbf{ik}$$

Assim, nosso produto fica

$$\begin{aligned} pq &= (p_0q_0 - p_1q_1 + p_2q_2 + p_3q_3) + p_0(\mathbf{ij}q_1 + \mathbf{jq}_2 + \mathbf{kq}_3 + q_0(\mathbf{ip}_1 + \mathbf{jp}_2 + \mathbf{kp}_3)) \\ &\quad + \mathbf{i}(p_2q_3 - p_3q_2) + \mathbf{j}(p_3q_1 - p_1q_3) + \mathbf{k}(p_1q_2 - p_2q_1). \end{aligned} \tag{2.3}$$

Perceba que a parte real quase representa o produto interno  $\langle \mathbf{p}_v, \mathbf{q}_v \rangle = p_1q_1 + p_2q_2 + p_3q_3$ , então, pode-se reescrever a expressão como

$$\begin{aligned} pq &= p_0q_0 - \langle \mathbf{p}_v, \mathbf{q}_v \rangle + p_0\mathbf{q}_v + q_0\mathbf{p}_v + \mathbf{i}(p_2p_3 - p_3p_2) + \mathbf{j}(p_3q_1 - p_1q_3) \\ &\quad + \mathbf{k}(p_1q_2 - p_2q_1) \end{aligned} \tag{2.4}$$

E, por fim, perceba que o produto vetorial  $\mathbf{p}_v \times \mathbf{q}_v = \mathbf{i}(p_2q_3 - p_3q_2) + \mathbf{j}(p_3q_1 - p_1q_3) + \mathbf{k}(p_1q_2 - p_2q_1)$  aparece no nosso produto, donde podemos reescrevê-lo como

$$pq = p_0q_0 - \langle \mathbf{p}_v, \mathbf{q}_v \rangle + p_0\mathbf{q}_v + q_0\mathbf{p}_v + \mathbf{p}_v \times \mathbf{q}_v.$$

**Proposição 2.2.6.** O conjunto dos quatérnios é fechado pelo produto algébrico de quatérnios.

*Demonstração.* Como o quatérnio produto algébrico  $r = pq$  pode ser escrito como

$$r = r_0 + \mathbf{r}_v, \tag{2.5}$$

onde  $r_0 = (p_0q_0 - \langle \mathbf{p}_v, \mathbf{q}_v \rangle)$  e  $\mathbf{r}_v = (p_0\mathbf{q}_v + q_0\mathbf{p}_v + \mathbf{p}_v \times \mathbf{q}_v)$ , então  $r \in \mathbb{H}$ .  $\square$

**Proposição 2.2.7.** *O produto algébrico de quatérnios é associativo. Ou seja, dados  $p, q, r \in \mathbb{H}$ , temos que*

$$(pq)r = p(qr)$$

**Proposição 2.2.8.** *O produto algébrico de quatérnios é distributivo em relação à adição, ou seja, para  $p, q, r \in \mathbb{H}$*

$$p(q + r) = pq + pr \quad e \quad (p + q)r = pr + qr$$

Assim, o conjunto dos quatérnios monido das operações de adição, multiplicação por escalar e do produto de quatérnios forma uma álgebra associativa, denominada *Álgebra dos Quatérnios*.

**Definição 2.2.5** (Elemento neutro do produto). Seja  $1_{\mathbb{H}} = 1 + \mathbf{0}_v \in \mathbb{H}$  o elemento da álgebra dos quatérnios definido como identidade do produto de quatérnios. Isto é, para todo  $q = q_0 + \mathbf{q}_v \in \mathbb{H}$ ,  $q1_{\mathbb{H}} = q$ .

**Proposição 2.2.9.** *Sejam  $p, q \in \mathbb{H}$ . Então  $(pq)^* = q^*p^*$ .*

**Definição 2.2.6** (Norma). Dado  $q \in \mathbb{H}$ , sua *norma* é dada por  $N(q) = q^*q$ .

**Proposição 2.2.10.** *Dado  $p \in \mathbb{H}$ , a norma do conjugado de  $p$  é igual a sua própria norma, ou seja,  $N(p^*) = N(p)$ .*

**Proposição 2.2.11.** *Sejam  $p, q \in \mathbb{H}$ , a norma do produto  $pq$  é igual ao produto das normas de  $p$  e  $q$ , isto é,  $N(pq) = N(p)N(q)$ .*

**Definição 2.2.7** (Inverso). Para cada  $q \in \mathbb{H} \setminus \{0\}$ , existe um elemento  $q^{-1} \in \mathbb{H}$  tal que  $qq^{-1} = q^{-1}q = 1_{\mathbb{H}}$  e que  $q^{-1} = \frac{1}{N^2(q)}q^*$  chamado de *inverso do quatérnio*  $q$ .

**Proposição 2.2.12.** *Seja  $q$  um quatérnio. Se  $q$  é unitário, isso é,  $N(q) = 1$ , então seu inverso coincide com seu conjugado:*

$$q^{-1} = q^*.$$

**Definição 2.2.8** (Quatérnio puro). O quatérnio  $q$  é dito *quatérnio puro* quando sua parte real for zero. O conjunto dos quatérnios puros é denotado por  $\mathbb{H}_0$ .

**Proposição 2.2.13.**  $\mathbb{H}_0 \simeq \Lambda^2 \mathbb{R}^3 \simeq \mathbb{R}^3$

**Definição 2.2.9** (Quatérnio real). O quatérnio  $q$  é dito *quatérnio real* quando sua parte vetorial for o elemento nulo. O conjunto dos quatérnios reais é denotado por  $\mathbb{R}$ , visto que é trivialmente isomorfo aos reais.

## Rotação com quatérnios

**Teorema 2.2.1.** *Seja  $p_x \in \mathbb{H}_0$  um quatérnio associado a um vetor  $\mathbf{x} \in \mathbb{R}^3$  dado. Então, o quatérnio unitário  $q = \cos(\frac{1}{2}\theta) + \sin(\frac{1}{2}\theta)\mathbf{v}$  induz uma rotação  $\theta$  de  $\mathbf{x}$  sobre o eixo  $\langle \mathbf{v} \rangle$ , determinando  $\mathbf{x}' \in \mathbb{R}^3$ , pelo mapa*

$$\begin{aligned} R_q: \quad \mathbb{H}_0 &\longrightarrow \mathbb{H}_0 \\ p_x &\longmapsto p_{x'} = R_q(\mathbf{x}) = qp_xq^{-1} \end{aligned}$$

**Corolário 2.2.1.** *Sejam  $q = q_0 + \mathbf{q}_v \in \mathbb{H}$  e  $\mathbf{x} \in \mathbb{R}^3$ . O resultado da rotação  $\mathbf{x}'$  de  $\mathbf{x}$  por  $R_q$  pode ser escrito como combinação linear da base  $\{\mathbf{x}, \mathbf{q}_v, \mathbf{q}_v \times \mathbf{x}\}$  da forma*

$$\mathbf{x}' = (q_0^2 - \mathbf{q}_v \cdot \mathbf{q}_v)\mathbf{x} + 2(\mathbf{q}_v \cdot \mathbf{x})\mathbf{q}_v + 2q_0(\mathbf{q}_v \times \mathbf{x}).$$

*Demonstração.* Esse resultado é construído de forma detalhada em [10]. □

## 2.3 Geometria de Distâncias Euclidianas

Apresenta-se nesta seção uma introdução a *Geometria de Distâncias Euclidianas*, seguindo principalmente o estudo feito em [11] e [12]. O nome “Geometria de Distâncias” diz respeito ao fato desta geometria basear-se em distâncias ao invés de pontos. A palavra “Euclidiana” é importante para caracterizar as arestas — elementos fundamentais associados as distâncias — como segmentos de reta, sem restringir seus ângulos de incidência.

### 2.3.1 Como tudo Começou

Por volta de 300 AC, Euclides de Alexandria organizou o conhecimento de sua época acerca da Geometria em uma obra composta por treze volumes, onde construiu, a partir de um pequeno conjunto de axiomas fortemente baseado nos conceitos de pontos e linhas, a chamada *Geometria Euclidiana* [13]. Em contraponto à visão original de Euclides, os primeiros conceitos geométricos usando *apenas distâncias* costumam estar associados aos trabalhos de Herão de Alexandria (10 a 80 d.C.), com o desenvolvimento de um teorema que leva seu nome, como segue:

**Teorema de Herão:** Sejam  $s$  o *Semiperímetro* de um triângulo (se  $p$  é o perímetro,  $s = \frac{p}{2}$ ) e  $a, b$  e  $c$  os comprimentos dos três lados deste triângulo. Então, a área  $A$  do triângulo é

$$A = \sqrt{s(s-a)(s-b)(s-c)}. \quad (\text{Fórmula de Herão})$$

**Demonstração** baseada em [14]: Considere um triângulo com lados  $a, b, c$  (opostos aos vértices  $A, B, C$ , respectivamente) e seu círculo inscrito centrado na origem  $O$  do sistema e raio  $r$  (Figura 2.12). As perpendiculares da origem até os lados do triângulo, dividindo os lados  $a$  em  $y, z$ , o  $b$  em  $x, z$  e o  $c$  em  $x, y$ . Seja  $u, v, w$  os segmentos indo da origem  $O$  até os vértices  $A, B, C$ , respectivamente.

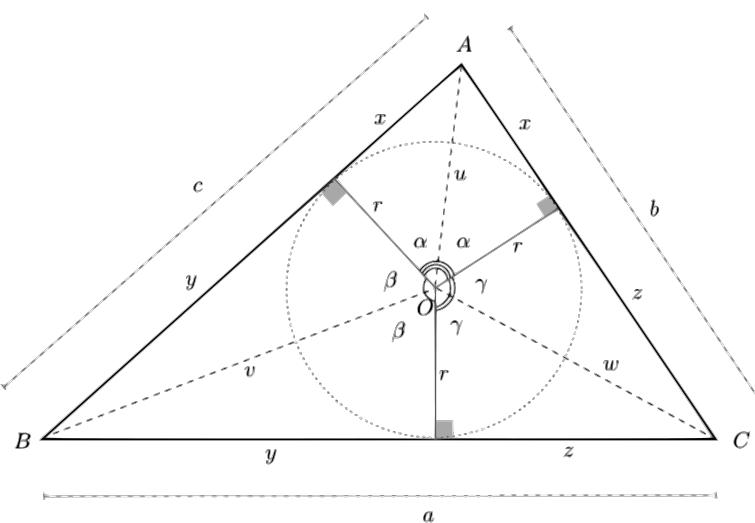


Figura 2.12: Formula de Herão: uma demonstração usando números complexos. [14]

Primeiro, nota-se que  $2\alpha + 2\beta + 2\gamma = 2\pi$ , o que implica  $\alpha + \beta + \gamma = \pi$ . Depois, as

seguintes identidades complexas são facilmente verificadas na Figura 2.12:

$$r + ix = ue^{i\alpha}, \quad r + iy = ve^{i\beta}, \quad r + iz = we^{i\gamma}.$$

Isso implica que:

$$(r + ix)(r + iy)(r + iz) = (uvw)e^{i(\alpha+\beta+\gamma)} = uvwe^{i\pi},$$

e, conhecendo a identidade de Euler  $e^{i\pi} = -1$ ,

$$uvwe^{i\pi} = -uvw.$$

Como  $-uvw$  é um número real, a parte imaginária de  $(r + ix)(r + iy)(r + iz)$  deve ser zero. Expandindo o produto e rearranjando seus termos, tem-se que  $r^2(x+y+z) = xyz$ . Ao isolar  $r$ , caí-se na raiz não negativa

$$r = \sqrt{\frac{xyz}{x+y+z}}. \quad (2.6)$$

Pode-se escrever o semiperímetro do triângulo  $ABC$  como  $s = \frac{1}{2}(a+b+c) = \frac{1}{2}(y+z+x+z+x+y) = x+y+z$ . Além disso,

$$s-a = x+y+z-y-z = x, \quad s-b = x+y+z-x-z = y, \quad s-c = x+y+z-x-y = z,$$

portanto  $xyz = (s-a)(s-b)(s-c)$ , implicando que a Equação 2.6 se torna:

$$r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}}.$$

Então escreve-se a área  $A$  do triângulo  $ABC$  como soma das áreas dos triângulos  $AOB$ ,  $BOC$  e  $COA$ , gerando

$$A = \frac{1}{2}(ra+rb+rc) = r \frac{a+b+c}{2} = rs = \sqrt{s(s-a)(s-b)(s-c)}.$$

□

Pode-se dizer que esse foi o nascimento da *Geometria de Distâncias* (*Distance Geometry*, ou DG) [14].

Algumas centenas de anos depois, em 1841, Arthur Cayley (1821 a 1895) generalizou a Fórmula de Herão através da construção de um determinante que calcula o conteúdo (volume  $n$ -dimensional) de um *Simplex*<sup>1</sup> em qualquer dimensão [15, 16]. Um século depois, em 1928, o matemático austríaco Karl Menger (1902 a 1985) re-organizou as ideias de Cayley e trabalhou em uma construção axiomática da geometria através de distâncias [17] — originando a alteração no nome do determinante de Cayley para como é conhecido hoje: “*Determinante de Cayley-Menger*”.

---

<sup>1</sup>Um simplex é uma generalização do conceito de triângulo a outras dimensões, i.e., é a envoltória convexa ao redor dos pontos: O  $0$ -simplex é um ponto,  $1$ -simplex é um segmento de reta,  $2$ -simplex é um triângulo e o  $3$ -simplex é um tetraedro.

**Definição:** O *Determinante de Cayley-Menger* de um conjunto de  $n + 1$  pontos  $p_0, p_1, \dots, p_n$ , onde  $d_{ij}$  corresponde a distância entre os pontos  $p_i$  e  $p_j$ , é dado por

$$D_{CM}(p_0, \dots, p_n) = \begin{vmatrix} 0 & d_{01}^2 & \dots & d_{0n}^2 & 1 \\ d_{01}^2 & 0 & \dots & d_{1n}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{0n}^2 & d_{1n}^2 & \dots & 0 & 1 \\ 1 & 1 & \dots & 1 & 0 \end{vmatrix}. \quad (\text{Determinante de Cayley-Menger})$$

**Lema:** Considere um  $K$ -simplex em  $\mathbb{R}^K$  de vértices  $x_i$ ,  $i = 0, \dots, k$ , cujas coordenadas  $x_i^j$  ( $j = 1, \dots, k$ ) são conhecidas. O *Volume Orientado*  $\mathbb{V}$  desse  $K$ -simplex é dado pela expressão

$$\mathbb{V} = \frac{1}{K!} \begin{vmatrix} x_0^1 & x_0^2 & \dots & x_0^K & 1 \\ x_1^1 & x_1^2 & \dots & x_1^K & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_K^1 & x_K^2 & \dots & x_K^K & 1 \end{vmatrix}. \quad (2.7)$$

**Demonastração** baseada em [16]: Em  $\mathbb{R}^2$ , três pontos não colineares determinam um triângulo. Se esses pontos possuem coordenadas as coordenadas  $x_0, x_1$  e  $x_2$ , utilizando Geometria Analítica, sabe-se que a área orientada do paralelogramo definido pelos vetores coluna  $x_1 - x_0$  e  $x_2 - x_0$  é dada por

$$A = \begin{vmatrix} (x_1 - x_0)^T \\ (x_2 - x_0)^T \end{vmatrix}.$$

Portanto, a área orientada  $\mathbb{V}_2$  do triangulo induzido pelos vetores  $x_1 - x_0$  e  $x_2 - x_0$  é

$$\mathbb{V}_2 = \frac{1}{2}|A|.$$

De forma semelhante, quatro pontos afimemente independentes em  $\mathbb{R}^3$  formam um tetraedro. Se as coordenadas de seus pontos forem  $x_0, x_1, x_2$  e  $x_3$ , o volume orientado  $\mathbb{V}_3$  deste tetraedro é dado por

$$\mathbb{V}_3 = \frac{1}{6} \begin{vmatrix} (x_1 - x_0)^T \\ (x_2 - x_0)^T \\ (x_3 - x_0)^T \end{vmatrix}.$$

Assim como em [18], a fórmula para o cálculo de um volume orientado  $\mathbb{V}_n$  de um  $n$ -simplex pode ser generalizada (por indução) a partir daqui. Um fator multiplicativo inversamente proporcional a  $K!$  aparece na expressão, de modo a ter-se

$$\mathbb{V}_K = \frac{1}{K!} \begin{vmatrix} (x_1 - x_0)^T \\ (x_2 - x_0)^T \\ \vdots \\ (x_K - x_0)^T \end{vmatrix}.$$

Ainda, pela expansão de Laplace, tem-se que

$$\mathbb{V}_K = \frac{1}{K!} \begin{vmatrix} (x_0)^T & 1 \\ (x_1 - x_0)^T & 0 \\ (x_2 - x_0)^T & 0 \\ \vdots & \vdots \\ (x_K - x_0)^T & 0 \end{vmatrix},$$

e pode-se somar a primeira linha as outras, sem alterar o valor do determinante, chegando ao nosso objetivo:

$$\mathbb{V}_K = \frac{1}{K!} \begin{vmatrix} (x_0)^T & 1 \\ (x_1)^T & 1 \\ (x_2)^T & 1 \\ \vdots & \vdots \\ (x_K)^T & 1 \end{vmatrix} = \frac{1}{K!} \begin{vmatrix} x_0^1 & x_0^2 & \dots & x_0^K & 1 \\ x_1^1 & x_1^2 & \dots & x_1^K & 1 \\ x_2^1 & x_2^2 & \dots & x_2^K & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_K^1 & x_K^2 & \dots & x_K^K & 1 \end{vmatrix}.$$

□

Com isso, pode-se enunciar o seguinte resultado:

**Teorema:** Considere os  $K + 1$  pontos  $p_0, \dots, p_K$  que definem os vértices de um  $K$ -simplex em um espaço euclidiano  $K$ -dimensional. Então, o quadrado do conteúdo  $\mathbb{V}_K$  desse  $K$ -simplex é

$$\mathbb{V}_K^2(p_0, \dots, p_K) = \frac{(-1)^{K+1}}{(K!)^2 2^K} D_{CM}(p_0, \dots, p_K). \quad (2.8)$$

*Demonstração* também baseada em [16]: Pelo Lema anterior, tem-se que

$$\mathbb{V} = \frac{1}{K!} \begin{vmatrix} x_0^1 & x_0^2 & \dots & x_0^K & 1 \\ x_1^1 & x_1^2 & \dots & x_1^K & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_K^1 & x_K^2 & \dots & x_K^K & 1 \end{vmatrix}.$$

Pode-se utilizar o modelo de *Coordenadas Homogêneas* para descrever a matriz do determinante acima em um *Hiperplano Afim* de uma dimensão superior, ao introduzirmos uma borda de zeros com um 1 na diagonal, o que não altera o valor do determinante. Obtém-se, então

$$\mathbb{V} = \frac{1}{K!} \begin{vmatrix} x_0^1 & x_0^2 & \dots & x_0^K & 1 & 0 \\ x_1^1 & x_1^2 & \dots & x_1^K & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ x_K^1 & x_K^2 & \dots & x_K^K & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{vmatrix}. \quad (2.9)$$

Agora, permuta-se as duas últimas colunas da matriz (o que alterna o sinal do determinante) e, como  $\det(A) = \det(A^T)$ , pode-se tomar a transposta, da forma

$$\mathbb{V} = -\frac{1}{K!} \begin{vmatrix} x_0^1 & x_1^1 & \dots & x_K^1 & 0 \\ x_0^2 & x_1^2 & \dots & x_K^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_0^K & x_1^K & \dots & x_K^K & 0 \\ 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & \dots & 1 & 1 \end{vmatrix}. \quad (2.10)$$

Sabendo que  $\det(AA^T) = \det(A)\det(A^T)$ , e que ambas a matriz do determinante acima tem dimensão  $(K+2) \times (K+2)$ , pode-se multiplicar a Equação 2.9 pela Equação 2.10 e obter

$$\mathbb{V}^2 = -\left(\frac{1}{K!}\right)^2 \begin{vmatrix} x_0^T x_0 & x_0^T x_1 & \dots & x_0^T x_K & 1 \\ x_1^T x_0 & x_1^T x_1 & \dots & x_1^T x_K & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_K^T x_0 & x_K^T x_1 & \dots & x_K^T x_K & 1 \\ 1 & 1 & \dots & 1 & 0 \end{vmatrix}.$$

E, sabendo que  $x_i^T x_j = \frac{1}{2}(x_i^T x_i + x_j^T x_j - d_{ij}^2)$ , pode-se alterar cada linha  $i$ , com  $0 \leq i \leq K$ , pela soma dela com a última linha multiplicada por  $-\frac{1}{2}x_i^T x_i$  (o que não altera o valor do determinante, por ser uma operação elementar). Também, pode-se fazer processo semelhante com as colunas: substituir cada coluna  $j$ , com  $0 \leq j \leq K$ , pela sua soma com a multiplicação da última coluna por  $-\frac{1}{2}x_j^T x_j$ . O que gera

$$\mathbb{V}^2 = -\left(\frac{1}{K!}\right)^2 \begin{vmatrix} -\frac{1}{2}d_{00}^2 & -\frac{1}{2}d_{01}^2 & \dots & -\frac{1}{2}d_{0K}^2 & 1 \\ -\frac{1}{2}d_{01}^2 & -\frac{1}{2}d_{11}^2 & \dots & -\frac{1}{2}d_{1K}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -\frac{1}{2}d_{0K}^2 & -\frac{1}{2}d_{1K}^2 & \dots & -\frac{1}{2}d_{KK}^2 & 1 \\ 1 & 1 & \dots & 1 & 0 \end{vmatrix}.$$

Visto que ao multiplicar uma coluna da matriz do determinante por um escalar  $\alpha$ , o próprio determinante é multiplicado por  $\alpha^{-1}$ , pode-se multiplicar as primeiras  $K+1$  colunas da matriz acima por -2, obtendo:

$$\mathbb{V}^2 = \frac{-1}{(K!)^2} \left(-\frac{1}{2}\right)^{K+1} \begin{vmatrix} d_{00}^2 & d_{01}^2 & \dots & d_{0K}^2 & 1 \\ d_{01}^2 & d_{11}^2 & \dots & d_{1K}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{0K}^2 & d_{1K}^2 & \dots & d_{KK}^2 & 1 \\ -2 & -2 & \dots & -2 & 0 \end{vmatrix}.$$

Como uma propriedade semelhante existe para multiplicações de linhas da matriz de um determinante, pode-se dividir a última linha da matriz anterior por -2. Também, ajeitando os coeficientes, tem-se

$$\mathbb{V}^2 = (-2) \frac{-1}{(K!)^2} \frac{(-1)^{K+1}}{2^{K+1}} \begin{vmatrix} d_{00}^2 & d_{01}^2 & \dots & d_{0K}^2 & 1 \\ d_{01}^2 & d_{11}^2 & \dots & d_{1K}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{0K}^2 & d_{1K}^2 & \dots & d_{KK}^2 & 1 \\ 1 & 1 & \dots & 1 & 0 \end{vmatrix}.$$

Por fim, como a distância  $d_{ii} = 0$  para qualquer valor de  $i$  (pela definição de métrica), obtém-se a expressão final, tal qual como desejava-se,

$$\mathbb{V}^2 = \frac{(-1)^{K+1}}{2^K(K!)^2} \begin{vmatrix} 0 & d_{01}^2 & \dots & d_{0K}^2 & 1 \\ d_{01}^2 & 0 & \dots & d_{1K}^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{0K}^2 & d_{1K}^2 & \dots & 0 & 1 \\ 1 & 1 & \dots & 1 & 0 \end{vmatrix} = \frac{(-1)^{K+1}}{2^K(K!)^2} D_{CM}(p_0, \dots, p_K).$$

□

Mas foi só com Leonard Blumenthal (1901 a 1984) que, em 1953, o termo Geometria de Distâncias foi cunhado — com a publicação de seu livro “*Theory and Applications of Distance Geometry*” [19]. Blumenthal dedicou sua vida de trabalho para clarificar, organizar e traduzir as obras originais em alemão. Ele acreditava que o problema mais importante nesta área era o “*Problema de Subconjunto*” (ou *Subset Problem*, originalmente), que consistia em encontrar condições necessárias e suficientes a fim de decidir quando uma matriz simétrica era, de fato, uma *Matriz de Distâncias*<sup>2</sup>. Uma restrição desse problema à métrica euclidiana chama-se *Problema de Matrizes de Distâncias Euclidianas* (ou EDMP, do inglês *Euclidean Distance Matrix Problem*), como segue definida:

**Problema de Matrizes de Distâncias Euclidianas:** Determinar se, para uma dada matriz quadrada  $D_{n \times n} = (d_{ij})$ , existe um inteiro  $K$  e um conjunto  $\{p_1, \dots, p_n\}$  de pontos em  $\mathbb{R}^K$  tal que  $d_{ij} = \|p_i - p_j\|$  para todo  $i, j \leq n$ .

Condições necessárias e suficientes para que uma matriz seja, de fato, uma matriz de distância euclidiana são dados em [20]. Para isso, apresenta-se um teorema onde se utiliza o Determinante de Cayley-Menger na criação de duas condições afirmando que, afim de  $D_{n \times n}$  ser uma matriz de distâncias euclidianas, deve haver um  $K$ -simplex  $S$  de referência com conteúdo  $v_K \neq 0$  em  $\mathbb{R}^K$  e que todos os  $(K+1)$ -simplex e  $(K+2)$ -simplex contendo  $S$  como uma das faces devem estar contidos em  $\mathbb{R}^K$  [12].

Blumenthal percebeu a importância em se respeitar as restrições métricas estabelecidas pelas matrizes de distâncias.

*Quando temos como dado um conjunto de distâncias entre pares de pontos, a geometria das distâncias pode dar uma dica para encontrar um conjunto de coordenadas correto para pontos no espaço Euclídeo tridimensional, satisfazendo as restrições de distâncias dadas.*

(Blumenthal, 1953, [19])

Pode-se dizer que resolver o Problema de Matrizes de Distâncias Euclidianas está intimamente relacionado com descobrir as coordenadas dos pontos que definem suas distâncias. Perceba que este é um problema inverso, onde o “problema direto” correspondente é calcular distâncias associadas a pares de pontos dados. Note que este estudo tem enorme aplicabilidade.

Adiante, em 1979, Yemini (atualmente professor emérito de Ciência da Computação na Universidade de Columbia) foi o primeiro a flexibilizar a definição do EDMP ao considerar um conjunto de distâncias esparso [21] — i.e., que não se tem todas as distâncias dadas a priori. Com isso, introduziu-se o que se chamou de *Problema Posição - Localização*, onde deseja-se calcular a localização de todos os objetos imersos em um espaço geográfico.

Assim, foi possível reformular o problema fundamental de Geometria de Distâncias, o qual pode ser caracterizado de forma mais moderna pela utilização da Teoria de Grafos.

---

<sup>2</sup>Seja o par  $(\mathcal{X}, d)$  um *Espaço Métrico* (vide Apêndice ??), onde  $\mathcal{X} = \{x_1, \dots, x_n\}$ . Uma *Matriz de Distância sobre  $\mathcal{X}$*  é uma matriz quadrada  $D_{n \times n} = (d_{uv})$  onde, para todo  $u, v \leq n$ , temos  $d_{uv} = d(x_u, x_v)$ .

### 2.3.2 O Problema Fundamental

Uma *Realização* é uma função que mapeia um conjunto de vértices de um grafo  $G$  para um espaço euclidiano de alguma dimensão dada.

**Problema de Geometria de Distâncias (DGP):** Dados um grafo simples, ponderado e conectado  $G = (V, E, d)$  e um inteiro  $K > 0$ , encontre uma realização  $x : V \rightarrow \mathbb{R}^K$  tal que:

$$\forall \{u, v\} \in E, \quad \|x(u) - x(v)\| = d(u, v). \quad (2.11)$$

Desde que uma realização seja encontrada, também dá-se a ela o nome de *Solução* do DGP. Por simplicidade — claramente um abuso de notação — pode-se escrever  $x_u$  e  $d_{uv}$  no lugar de  $x(u)$  e  $d(u, v)$ , respectivamente.

A principal diferença desta definição para o EDMP está acerca de que uma matriz de distância essencialmente representa um *Grafo Ponderado Completo*. Em contraponto, o DGP não empoe qualquer estrutura em  $G^3$ , seguindo o conceito de matriz esparsa estabelecido por Yemini.

Por fim, na equação 2.11, utiliza-se a norma euclidiana  $\|\cdot\|$  como métrica (ver Apêndice ??), donde pode-se reescrever esta equação como

$$\forall \{u, v\} \in E, \quad \sqrt{\sum_{i=1}^K (x_{ui} - x_{vi})^2} = d_{uv}.$$

Como a definição de métrica garante a positividade das distâncias, pode-se esconder a raiz quadrada na equação acima, i.e.

$$\forall \{u, v\} \in E, \quad \sum_{i=1}^K (x_{ui} - x_{vi})^2 = d_{uv}^2. \quad (2.12)$$

## Os Diferentes Problemas em DG

Em 2014, Leo Liberti *et al.* publicaram um ótimo compendio sobre a *Geometria de Distâncias Euclidianas e suas Aplicações* e, em particular, desenvolveram um estudo taxonômico muito interessante sobre os problemas clássicos da área. No que se segue, devido a grande quantidade de siglas e variações dentro de DG, apresenta-se parte desse estudo, visando organizar os conceitos.

As principais aplicações em DG são no *Calculo de Estruturas Moleculares* [22], na *Localização de Sensores em Redes Sem Fio* (*Wireless Sensor Network Localization*, ou WSNL) [23], em *Cinemática Inversa* (*Inverse Kinematic*, ou IK) [24] e em *Escalonamento Multidimensional* (*Multidimensional Scaling*, ou MDS) [25].

## Escalonamento Multidimensional

O problema de *Escalonamento Multidimensional* (*Multidimensional Scaling*, ou MDS) é definido como: Dado um conjunto  $X$  de vetores, encontre um conjunto  $Y$  de

---

<sup>3</sup>A menos, é claro, no que diz respeito a seus vértices estarem conectados. Porém, caso  $G$  não seja conectado, então ele consiste de um conjunto de diferentes subgrafos conectados, donde, a fim de solucionar o DGP, pode-se realizar cada subgrafo separadamente.

vetores com menor dimensão (com  $|X| = |Y|$ ) tal que a distância entre cada  $i$ -ésimo e  $j$ -ésimo vetores de  $Y$  tenham, aproximadamente, a mesma distância que seus pares de vetores correspondentes em  $X$ .

Esse problema é muito aplicado na análise de dados em Big Data [11]. É um meio de facilitar a visualização do nível de similaridade entre casos individuais — que não necessariamente precisam ter uma conexão aparente — em um conjunto de dados. Pode-se usá-lo, por exemplo, para visualizar em uma escala bidimensional ( $\mathbb{R}^2$ ) a evolução da locomoção de animais no espaço tridimensional utilizando dados de séries temporais (espaço em diferentes tempos, logo, dados em  $\mathbb{R}^4$ ).

## Conformações Moleculares

Existe uma relação muito forte com a forma geométrica das moléculas e suas funções em organismos vivos [26]. Projetar drogas para curar uma doença específica se trata basicamente de conhecer o que uma certa proteína pode fazer em um organismo [11]. Proteínas se ligam em outras moléculas através do equilíbrio de forças agindo entre elas<sup>4</sup>, portanto, suas ligações dependem do seu formato.

Proteínas são constituídas por um grande conjunto de átomos e, alguns pares destes, trocam ligações químicas — sabe-se quais são esses átomos através de experimentos de cristalografia [28]. Então, se os átomos de uma molécula forem rotulados da forma  $1, 3, 4, \dots, n$ , é possível inferir:

- O conjunto de ligações  $\{u, v\}$ , onde  $u, v$  são átomos em  $\{1, \dots, n\}$ ;
- A distância entre  $u$  e  $v$  (para cara par ligado);
- O ângulo interno  $\theta_v$  definido por duas ligações  $\{u, v\}$  e  $\{v, w\}$ , com um átomo  $v$  em comum.

Além desses dados, também é possível obter mais informações a partir de experimentos mais sofisticados, como a *Ressonância Magnética Nuclear* (RMN). Neste experimento é escolhida uma faixa de radiofrequência para bombardear uma amostra que está imersa em um campo magnético bastante intenso. Dependendo da radiofrequência utilizada (costuma-se usar a do hidrogênio), alguns núcleos atômicos irão absorver energia e outros não. Caso atinja-se uma frequência exata de ressonância dentro destes núcleos atômicos, é possível medir essa ressonância como um sinal de radiofrequência enviado dos núcleos atômicos para calcular distâncias entre átomos próximos, com distâncias menores que 5 Å.

De posse dessas informações, deseja-se realizar (localizar) todos os átomos da molécula. Esse problema, com todas as informações moleculares disponíveis, denomina-se *Estrutura Proteica a Partir de Dados Brutos* (*Protein Structure from Raw Data*, ou PSRD). Em particular, como as coordenadas atômicas pertencem ao  $\mathbb{R}^3$ , há uma particularização do DGP para o caso molecular chamado *Problema de Geometria de Distâncias Moleculares* (*Molecular DGP*, ou MDGP). Trata-se do DGP com  $K = 3$  fixo.

---

<sup>4</sup>Ou seja, o equilíbrio da energia potencial das moléculas, proporcional, principalmente, as variações nos comprimentos das ligações covalentes, as variações nos ângulos entre duas ligações covalentes consecutivas, as rotações sobre as ligações covalentes e as interações de van der Waals e interações eletrostáticas entre átomos [27].

## Localização de Sensores

O *Problema de Localização de Sensores em Rede sem Fio* (ou *WSNL Problem*) surge quando é necessário localizar um conjunto de objetos equipados com sensores eletrônicos capazes de medir distâncias entre si, geograficamente distribuídos, usando apenas medidas de distâncias entre pares destes objetos [23].

Por exemplo, *smartphones* com WIFI ativo podem criar uma rede conhecida por *Rede Ad-Hoc*, *i.e.*, eles conseguem criar uma rede para comunicar-se entre si, de forma *Peer-to-Peer*, sem a necessidade de uma torre central — cada aparelho funciona como uma pequena torre, de forma que a distância entre os aparelhos não pode ser excessiva. Dessa forma, os *smartphones* podem estimar a distância  $r$  de emparelhamento das suas conexões ao medir, por exemplo, qual a potência de transmissão do sinal, uma vez que sabe-se que a potência  $P$  de uma transmissão eletromagnética cai da forma

$$P = \frac{X}{r^n}, \quad (2.13)$$

onde  $X$  e  $n$  são constantes e dependem muito das condições do experimento, sendo obtidas experimentalmente [29].

Em essência, um problema do tipo WSNL segue a mesma definição do DGP, porém, com um subconjunto  $A \subset V$  de vértices (chamados *Âncoras*), onde os elementos de  $A$  tem uma posição em  $\mathbb{R}^k$  dada a priori — isso é feito pois, normalmente, interessa saber a posição relativa de um objeto a outro, como é o caso do Sistema de Posicionamento Global, onde temos os satélites como âncoras e desejamos saber a posição dos aparelhos GPS em relação aos satélites.

Por motivos práticos — semelhantes ao caso molecular — as variações de interesse desse problema tem o  $K$  fixo em  $K = 2$  ou  $K = 3$ . É comum, também, que se defina um WSNL como *Solucionável* somente se seu grafo possua uma única realização válida — noção conhecida como *Globalmente Rígido*: Diz-se que um grafo é *Globalmente Rígido* quando ele possui uma realização genérica  $x$  e, para todas as outras realizações  $x'$ ,  $x$  é congruente a  $x'$ .

## Dinâmicas em Cinemática Inversa

Muito utilizada em robótica e animação computadorizada, a cinemática inversa cerne sobre mecanismos e seus movimentos rígidos, onde restringe-se os movimentos de forma a preservar a geometria do sistema. Sem o auxílio computacional e matemático a manipulação de mecanismos com muitos graus de liberdade pode ser inviável: Imagine a manipulação manual de cem vértices em uma haste simulando o comportamento de um braço articulado em uma animação. Com o auxílio da DG, um animador pode apenas configurar a posição final de um pequeno grupo de vértices (como os da extremidade da aresta, por exemplo) e um algoritmo de cinemática inversa é capaz de verificar se aquela posição é ou não viável e, se viável, qual a realização de todo o conjunto de vértices em razão da posição configurada [24].

Visando tal restrição mecânica, define-se o *Problema de Cinemática Inversa (Inverse Kinematic Problem*, ou IKP) como uma variação do WSNL — logo, tem o objetivo de descobrir posições em relação a certos pontos previamente realizados — com uma restrição no grafo que define o problema: deve ser um caminho simples com seus vértices finais sempre sendo âncoras.

### 2.3.3 A Busca de uma Solução

A abordagem mais simples, pode-se pensar, para encontrar um conjunto de soluções que satisfação a equação 2.12 é resolver o sistema de equações diretamente [30]. Infelizmente, para  $K \geq 2$ , há evidências de que uma solução de forma fechada onde todo componente de  $x$  é expresso por raízes, não é possível.

No entanto, pode-se reformular o problema como um Problema de Otimização Global, onde o objetivo é minimizar a soma dos *Erros*<sup>5</sup> entre as distâncias dadas a priori e as calculadas. Para isso, pode-se considerar uma única expressão que englobe todos os  $n$  erros, da forma

$$f(x_1, \dots, x_n) = \sum_{(i,j) \in E} (\|x_i - x_j\|^2 - d_{ij}^2)^2. \quad (2.14)$$

Fica claro que encontrar uma solução para o DGP é equivalente a encontrar realizações  $x_i \in \mathbb{R}^3$ ,  $i = 1, \dots, n$ , tal que  $f(x_1, \dots, x_n) = 0$ . Visto que esta função se trata de uma soma de quadrados e que não há restrições nesse problema de Otimização Global, 0 é o valor mínimo de  $f$ . Deseja-se, portanto, minimizar a função  $f : \mathbb{R}^n \rightarrow \mathbb{R}$ . Isto é,

$$\min_{x_i \in \mathbb{R}^n} f(x_1, \dots, x_n). \quad (2.15)$$

E, no caso da métrica euclidiana (vide Apêndice ??), o problema 2.15 torna-se

$$\min_{x_j \in \mathbb{R}^n} \sum_{(u,v) \in E} \left( \sum_{i=1}^K (x_{ui} - x_{vi})^2 - d_{uv}^2 \right)^2. \quad (2.16)$$

Perceba que a introdução conveniente de quadrados nas distâncias da função 2.14 eliminou o cálculo da raiz na norma euclidiana presente na Equação 2.16 — uma otimização, principalmente por (i) multiplicação tem um custo numérico inferior ao da radiciação [31] e (ii) a radiciação pode apresentar alguns problemas numéricos para valores próximos de zero [32]. Portanto, a equação 2.16 tem como objetivo a minimização de um polinômio de múltiplas variáveis de grau quatro.

Um dos desafios da Otimização Global é que muitos dos métodos existentes — em especial, os mais eficientes — não garantem que uma otimização *global* será encontrada. Isso se dá pois podem existir muitos ótimos locais e, visto que os métodos de otimização continua dispõem apenas de informações locais, estes não conseguem diferenciá-los de um global [30] (vide Figura 2.13).

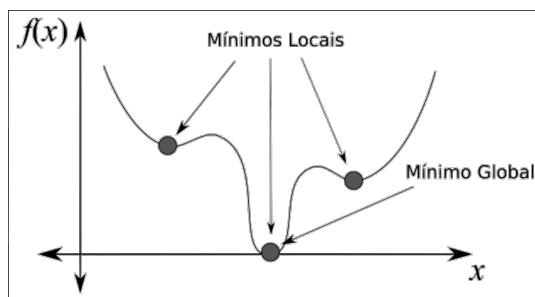


Figura 2.13: Diferenças entre mínimos locais e globais [30].

---

<sup>5</sup>Em otimização, vê-se a equação 2.11 de forma não exata:  $\|x_u - x_v\| = d_{uv} + \varepsilon$ , onde  $\varepsilon$  é chamado *Erro*. Ou seja, para minimizar o erro, precisa-se minimizar a expressão  $f(x_u, x_v) = \|x_u - x_v\| - d_{uv}$ .

Infelizmente, essa abordagem via Otimização Global é custosa do ponto de vista computacional — como mostrado em [33], onde Carlile *et. al.* citam as limitações dos métodos contínuos. Saxe demonstrou em 1979 [34] que resolver um DGP para qualquer dimensão — i.e., para qualquer valor de  $K$  — tem a complexidade computacional da classe **NP-Hard**. Em outras palavras, isso significa que a quantidade de mínimos locais de um DGP cresce exponencialmente proporcional a  $|V|$  [35].

## A Quantidade de Soluções do Problema

Seja  $\bar{X} = \{x : V \rightarrow \mathbb{R}^K \mid x \text{ satisfaça (2.11)}\}$  o conjunto de todas as soluções de uma instância DGP. Então, para qualquer transformação ortogonal  $T$  de  $\mathbb{R}^K$  (por exemplo, uma rotação ou translação) tem-se que, pela própria definição de ortogonalidade, se  $x \in \bar{X}$  então  $T(x) \in \bar{X}$ . Define-se uma relação de equivalência  $\sim$  sobre  $\bar{X}$  como  $\bar{x} \sim \bar{y}$  se e somente se existir uma transformação ortogonal  $T$  tal que  $\bar{y} = T\bar{x}$ . Finalmente, define-se  $X = \bar{X}/\sim$  e identifica-se a classe de equivalência de  $X$  com um de seus representantes  $x \in \bar{X}$ . Em [33] o conjunto  $X$  é identificado como o conjunto de “interesse” para as soluções de uma instância DGP, pois este não leva em consideração soluções “redundantes” advindas de transformações ortogonais — e pode-se obter facilmente um número incontável de transformações ortogonais [32].

Mesmo que a definição da classe de equivalência acima possa remover uma quantidade não enumerável de soluções do problema,  $|X|$  não é necessariamente finito. No geral, a quantidade de soluções do DGP depende da estrutura geométrica do grafo que a define: (i) podem não haver nenhuma realização; (ii) uma única realização; (iii) uma quantidade finita (não única) de realizações; ou, (iv) um número incontável de realizações. Perceba que, curiosamente, a quantidade de soluções de um DGP somente não pode ser um número infinito e enumerável — sabe-se isso através de estudos em *Geometria Algébrica Real* [36].

Ou seja, supondo que o conjunto solução de um DGP seja não vazio, sabe-se que ele é não enumerável ou finito. Se for não enumerável, pode-se tentar fazer uma busca contínua no espaço euclidiano — como o algorítimo *spatial Branch-and-Bound* (sBB), que faz uma  $\epsilon$ -aproximação para solucionar *Nonlinear Programs* (NLPs) não convexos e *Mixed-Integer NLPs* [12]. Se for finito (normalmente o caso desejado), além de poder aplicar métodos de Otimização Global — já definidos como custosos computacionalmente —, pode-se explorar outras abordagens, como a Otimização Combinatória.

### 2.3.4 Ferramentas Combinatórias na Solução do DGP

Nesta seção, estuda-se sobre as condições que garantem a finitude do conjunto solução do problema ao analisar o espaço de busca por uma solução. Em particular, para um DGP definido em um espaço euclidiano de dimensão  $K$ , apresenta-se uma classe de grafos com propriedades muito interessantes: dos  $(K + 2)$ -cliques, ou seja, dos grafos completos com dois vértices a mais do que o número de dimensões do seu espaço.

## Realização de Grafos Completos

Dependendo da estrutura do grafo que define um DGP, obter uma solução do problema pode garantir a unicidade desta solução [37]. A noção que estuda a unicidade de uma realização é a de rigidez: diz-se que um grafo é *Globalmente Rígido* se ele tem uma realização genérica  $x$  e, para todas todas as outras realizações  $x'$ ,  $x$  é *Congruente* a  $x'$ . Um grafo globalmente rígido tem realização única [38]. Essa característica é de fundamental importância para algumas classes de problemas em DG, como o caso da WSNL, onde somente realizações únicas são consideradas como soluções.

A seguir, baseado em [11] e [39], apresenta-se um método para calcular uma realização de um  $(K + 2)$ -clique em  $\mathbb{R}^K$ .

Considere um 3-clique ponderado com  $V = \{1, 2, 3\}$ , onde  $d_{12} = d_{23} = 1$  e  $d_{13} = 2$ . Então, uma possível realização sobre a reta real  $\mathbb{R}$  que satisfaça todas as distâncias é  $x_1 = 0$ ,  $x_2 = 1$  e  $x_3 = 2$  (conforme Figura 2.14). Uma forma de obter o valor de  $x_3$ , dado os valores de  $x_1$  e  $x_2$  e as distâncias  $d_{13}$  e  $d_{23}$ , é a *Trilateração*.

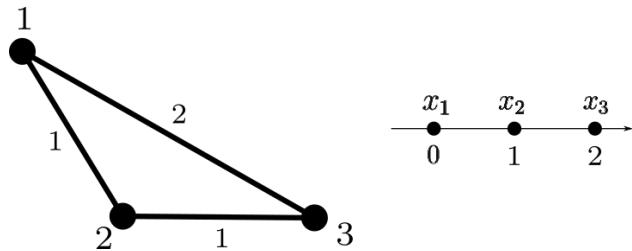


Figura 2.14: Representação do Grafo (esquerda) e sua realização na reta (direita).

## Trilateração

Vamos desenvolver este conceito a partir do exemplo mencionado acima. Se deseja encontrar as posições  $x_1, x_2$  e  $x_3$  de modo que satisfaçam as condições do DGP  $d_{13} = \|x_3 - x_1\| = 2$  e  $d_{23} = \|x_3 - x_2\| = 1$ . Usando a norma Euclidiana,  $\|u - v\|^2 = (u - v)^2 = u^2 - 2uv + v^2$ , tem-se

$$x_3^2 - 2x_1x_3 + x_1^2 = 4 \quad \text{e} \quad (2.17)$$

$$x_3^2 - 2x_2x_3 + x_2^2 = 1. \quad (2.18)$$

Subtraindo a equação 2.18 da 2.17, obtém-se

$$2(x_1 - x_2)x_3 = x_1^2 - x_2^2 - 3 \Rightarrow 2x_3 = 4 \Rightarrow x_3 = 2.$$

Pode-se generalizar esse exemplo facilmente para  $(K + 2)$ -cliques em  $\mathbb{R}^K$ :

Seja um DGP definido a partir de um  $(K + 2)$ -clique  $G$ . Conhece-se previamente as posições  $x_1, \dots, x_{k+1} \in \mathbb{R}^K$  de  $K + 1$  vértices de  $G$  e deseja-se descobrir a posição  $y \in \mathbb{R}^K$  do  $(K + 2)$ -ésimo vértice de  $G$ . Pela definição do DGP,  $y$  deve respeitar as  $K + 1$  equações quadráticas  $\|x_j - y\|^2 = d_{j,K+2}^2$ ,  $1 \leq j \leq K + 1$ , com as  $K$  componentes vetoriais de  $y$  como incógnitas:

$$\begin{cases} \|y\|^2 - 2x_1y + \|x_1\|^2 = d_{1,K+2}^2 \\ \vdots \\ \|y\|^2 - 2x_{K+1}y + \|x_{K+1}\|^2 = d_{K+1,K+2}^2 \end{cases} \quad (2.19)$$

Subtraindo as  $K$  primeiras equações do sistema de equações 2.19 pela  $(K+1)$ -ésima equação

$$\begin{cases} \|y\|^2 - 2x_1y + \|x_1\|^2 - (\|y\|^2 - 2x_{K+1}y + \|x_{K+1}\|^2) = d_{1,K+2}^2 - d_{K+1,K+2}^2 \\ \vdots \\ \|y\|^2 - 2x_Ky + \|x_K\|^2 - (\|y\|^2 - 2x_{K+1}y + \|x_{K+1}\|^2) = d_{K,K+2}^2 - d_{K+1,K+2}^2 \end{cases} \quad (2.20)$$

pode-se formar um novo sistema, contendo  $K$  equações com as mesmas  $K$  incógnitas:

$$\begin{cases} 2(x_1 - x_{K+1}) \cdot y = \|x_1\|^2 - \|x_{K+1}\|^2 - d_{1,K+2}^2 + d_{K+1,K+2}^2 \\ \vdots \\ 2(x_K - x_{K+1}) \cdot y = \|x_K\|^2 - \|x_{K+1}\|^2 - d_{K,K+2}^2 + d_{K+1,K+2}^2 \end{cases} \quad (2.21)$$

Seja a matriz quadrada  $A = (2(x_{ij} - x_{K+1j}))$ , com  $i, j \leq K$  como índices de linha e coluna (componentes vetoriais), respectivamente. Seja também o vetor coluna  $b = (\|x_i\|^2 - \|x_{K+1}\|^2 - d_{i,K+2}^2 + d_{K+1,K+2}^2)^T$ , onde  $1 \leq i \leq K$ . Então, pode-se reescrever o sistema de equações 2.21 como o sistema linear

$$Ay = b. \quad (2.22)$$

Diferentes métodos para solução de sistemas lineares como a equação 2.22 são encontrados na bibliografia [40] — no geral, a escolha do melhor depende de propriedades da matriz  $A$ , como sobre sua singularidade, esparsidão, entre outros. Em particular, se  $A$  não é uma matriz singular, então ela possui uma inversa  $A^{-1}$ . Pode-se, portanto, obter a posição do  $(K+2)$ -ésimo vértice fazendo

$$Ay = b \Rightarrow A^{-1}Ay = A^{-1}b \Rightarrow y = A^{-1}b = x_{K+2}. \quad (2.23)$$

No entanto, se  $A$  é singular, isso quer dizer que as linhas  $a_i = x_i - x_{K+1}$  (para  $i \leq K$ ) não são todas linearmente independentes [40]. Essa situação mostra algumas propriedades geométricas interessantes. Por exemplo, se  $K = 1$ , significa que  $x_1 - x_2 = 0 \Rightarrow x_1 = x_2$ , ou seja, que o segmento entre  $x_1$  e  $x_2$  é um simples ponto. Como estamos imersos no  $\mathbb{R}^K = \mathbb{R}$  (i.e., a reta real), geometricamente, a situação é que ou  $x_3$  está posicionado a direita ou a esquerda de  $x_1 = x_2$ , mas não se pode escolher (veja a Figura 2.15). Numericamente, é possível obter tais soluções ao utilizar a pseudoinversa de  $A$  [41].

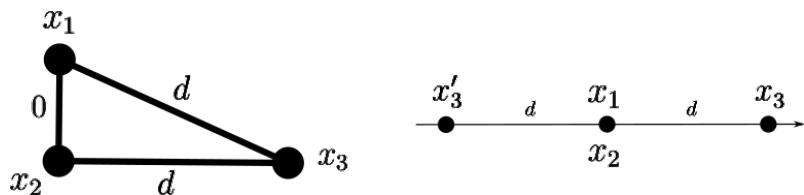


Figura 2.15: Representação da singularidade da matriz  $A$  em  $\mathbb{R}$ .

Não obstante, se  $K = 2$ , a singularidade de  $A$  implica que o triângulo definido por  $x_1$ ,  $x_2$  e  $x_3$  é apenas um segmento no plano (caso o rank de  $A$  é 1) ou um simples ponto (caso o rank for 0). No primeiro caso,  $x_4$  pode estar posicionado em ambos os lados da linha que contém o segmento e, no segundo caso,  $x_4$  pode estar em qualquer um dos pontos formados pela circunferência com centro  $x_1 = x_2 = x_3$  e raio  $d_{14} = d_{24} = d_{34}$ , conforme ilustra a Figura 2.16. Essa característica geométrica vale para valores maiores de  $K$ : a singularidade de  $A$  está relacionada a existência de vértices coincidentes e implica que há sempre múltiplas soluções para  $x_{K+2}$ .

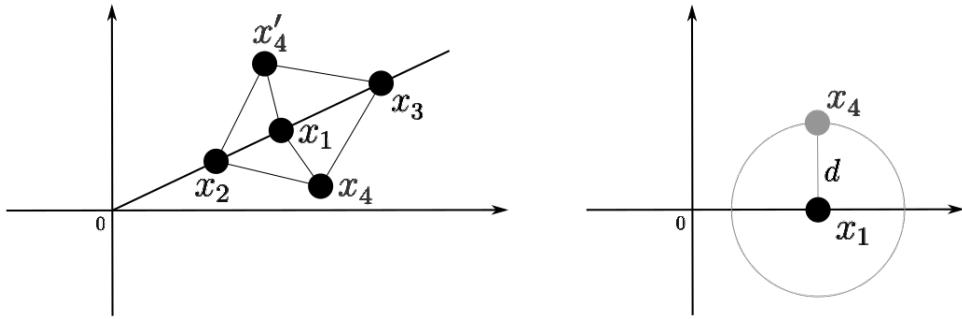


Figura 2.16: Representação da singularidade da matriz  $A$  em  $\mathbb{R}^2$ . A esquerda, caso o rank de  $A$  for 1 e, a direita, caso for 0.

Por fim, é importante mencionar que a partir da equação 2.19 podemos chegar no sistema linear 2.22, mas a recíproca não é verdadeira. Em particular, se o sistema 2.19 tem uma solução, então o sistema 2.22 tem a mesma solução. Porém, mesmo que o sistema 2.19 não tenha solução, o sistema 2.22 sempre terá uma solução — desde que  $A$  não seja singular. Sendo assim, para verificar a factibilidade de uma solução  $x_{K+2}$  advinda do sistema linear 2.22, deve-se verificar se as distâncias aos  $K + 1$  vértices foram respeitadas — ou seja, se

$$\|x_i - x_{K+2}\| = d_{i,K+2},$$

para todo  $i \leq K + 1$ .

**Conclusão:** Dado um  $(K + 2)$ -clique, sabe-se que *se ele possuir* uma realização em  $\mathbb{R}^K$  e não possui vértices coincidentes, no geral, *ela é única* a menos de rotações e translações [42, 43].

### Devagar e Sempre

Utilizando o método da trilateração apresentado, é possível descobrir a posição de apenas um vértice de um grafo completo, dado que se conhece as realizações de outros pontos. No entanto, como o objetivo é uma realização total do grafo, a seguir relembrar-se uma característica dos grafos completos que contorna essa limitação de uma forma engenhosa.

Relembre o grafo completo da Figura 2.17(a), formado pelo conjunto de vértices  $\{v_1, v_2, v_3, v_4\}$  e arestas  $\{\{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_4\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_3, v_4\}\}$ . Perceba que esse é um 4-clique e, ao removermos o vértice  $v_4$ , obtemos um 3-clique

formado pelos vértices restantes  $\{v_1, v_2, v_3\}$  e arestas  $\{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}\}$  (Figura 2.17(b)). Caso for retirado o vértice  $v_3$  desse 3-clique, obtemos o 2-clique  $(\{v_1, v_2\}, \{\{v_1, v_2\}\})$  (Figura 2.17(c)).

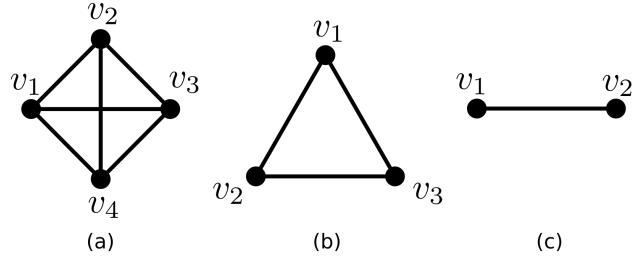


Figura 2.17: Em ordem: (a) 4-clique; (b) 3-clique; (c) 2-clique.

Perceba a existência de uma estrutura recursiva nos grafos completos, que se mantém para o caso geral: sendo  $G_{K+1} = \{V_G, E_G\}$  um  $(K+1)$ -clique e  $v \in V_G$  um vértice qualquer de  $G_{K+1}$ , sempre pode-se obter um  $K$ -clique como o subgrafo induzido  $\{V_G \setminus \{v\}\}$ . Por conta disso, podemos utilizar essas estruturas como “blocos básicos de construção” para planejar uma realização iterativa do grafo como um todo, usando a trilateração para realizar um novo vértice em cada iteração.

### Realização Iterativa de Grafos Completos

A seguir, apresenta-se um algorítimo para realizar em  $\mathbb{R}^K$  todos os  $n$  vértices de um  $(n, \frac{n^2-n}{2})$ -grafo completo  $G$ , com  $n > K$ , tendo como entrada a posição dos  $(K+1)$  primeiros vértices também em  $\mathbb{R}^K$ .

Primeiro, assume-se que existe um  $(K+1)$ -clique  $G_o \subset G$ , chamado clique inicial, que conhecemos a realização — em WSNL, por exemplo, comumente se utiliza nós ancoras como clique inicial [37, 29]. Sem perda de generalidade, seja  $\{1, \dots, K+1\}$  o conjunto dos vértices que formam a clique inicial  $G_o$ , com realizações  $\{x_1, \dots, x_{K+1}\}$ . Seja, também,  $N(i)$  o conjunto de vértices adjacentes ao  $i$ -ésimo vértice. Então, pode-se encontrar uma realização total de  $G$  através do Algorítimo 1.

---

**Algorithm 1:**  $x = \text{RealizacaoIterativa}(G, d, K, x)$  [11]

---

```
// Realize os próximos vértices iterativamente
1 for  $i \in \{K+2, \dots, n\}$  do
    /* Utilize o  $(K+1)$ -clique dos  $(K+1)$  antecessores imediatos
       de  $i$  para calcular a realização  $x_i$ . Caso não haja
       solução, atribuir  $\emptyset$  */  

2      $x_i = \text{Trilateracao}(x_{i-K-1}, \dots, x_{i-1})$ ;
    // verifique se  $x_i$  é factível com relação as demais
    // distâncias
3     for  $\{j \in N(i) ; j < i\}$  do
4         if  $\|x_i - x_j\| \neq d_{ij}$  then
            // Sinalizar como não factível e sair do loop
5              $x_i = \emptyset$ ;
6             break;
7         end
8     end
9     if  $x_i = \emptyset$  then
    // Retornar que a realização não é factível
10    return  $\emptyset$ ;
11 end
12 end
// Retornar a realização factível
13 return  $x$ ;
```

---

Note que o Algorítimo 1 tem a complexidade de seu pior caso como  $\mathcal{O}(K^3n)$ , i.e., para todos os  $n$  vértices, deve-se resolver um sistema linear  $K \times K$  (trilateração). Se não existir realização factível para  $G$  em  $\mathbb{R}^K$ , Algorítimo 1 retorna  $\emptyset$ .

**Definição([37]):** Esse processo de trilateração iterativa em  $\mathbb{R}^K$ , descrita pelo Algorítimo 1, é chamado *K-Lateração*.

### Sobre o clique inicial $G_o$ e unicidade

O Sistema de Posicionamento Global (GPS) é um exemplo de WSNL que pode utilizar da trilateração para descobrir a localização dos aparelhos de GPS (sensores móveis) [44]. Como o objetivo é encontrar posições no  $\mathbb{R}^3$ , precisa-se de 4 vértices âncoras para compor o clique inicial  $G_o$ , que, no caso, é formado por um conjunto de satélites com posições bem conhecidas. Fica claro que, em algumas aplicações, a quantidade de vértices necessários no clique inicial pode significar um projeto de engenharia bastante custoso.

Além disso, em um primeiro momento pode parecer pouco razoável necessitar da realização prévia do clique inicial  $G_o$ . De fato, se o problema possuir apenas  $K+1$  vértices, essa solução não faz sentido. Felizmente, em geral, os problemas de estudo costumam ser maiores [12].

É importante perceber que os  $K+1$  vértices do clique inicial (já realizados), juntamente com o vértice a se realizar, determinam um simplex no espaço  $\mathbb{R}^K$  que, garantida a desigualdade triangular  $d_{i,j} \leq d_{i,u} + d_{u,j}$ , para todo  $i, j, u \leq K+1$ , possui

um volume  $K$ -dimensional  $\geq 0$  (veja a Figura 2.18) diretamente proporcional ao determinante de Cayley-Menger (como mostrado na Equação 2.8). Caso esse volume seja zero, que é o que acontece com  $(K+2)$ -simplex em  $\mathbb{R}^K$ , tem-se o chamado *Simplex Achatado (Flat Simplex)* com no máximo uma realização (como ilustra a Figura 2.18, a direita).

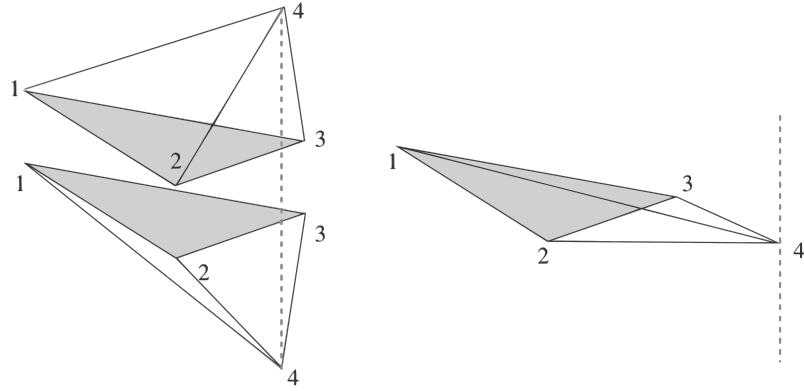


Figura 2.18: Note que as duas realizações de um mesmo 4-clique em  $\mathbb{R}^3$  (esquerda) são possíveis por respeitarem as distâncias entre os vértices, mas somente uma realização é possível em  $\mathbb{R}^2$  (direita) [11].

De fato, através da relação entre o volume de um simplex com a existência de uma realização para um grafo completo (que pode ou não formar um simplex), permite-se estabelecer condições necessárias e suficientes para a realização de cliques:

**Teorema ([45]):** Uma condição necessária e suficiente para que um  $(n+1)$ -clique tenha uma realização em  $\mathbb{R}^K$ , para  $K \leq n$ , é que todos os determinantes de Cayley-Menger, não nulos, de  $m+1$  pontos tenham sinal dado por  $(-1)^{m+1}$ , para todo  $m = 1, 2, \dots, K$ . Além disso, os determinantes de Cayley-Menger de mais de  $K+1$  pontos devem ser nulos.

Uma demonstração detalhada desse resultado pode ser encontrada em [45].

### Realizando grafos $K$ -laterativos em $\mathbb{R}^K$

No Algorítimo 1, fica implícita a existência de uma ordem no conjunto de vértices  $V$  do grafo  $G$ . Se  $G$  é completo, de fato, qualquer ordem  $(v_1, \dots, v_n)$  em  $V$  é tal que  $v_i$  é adjacente a todos os seus antecessores — isto é, para todo  $i > K+1$ , tem-se no mínimo os  $K+1$  antecessores necessários para a  $K$ -lateração. Por outro lado,  $G$  não precisa ser necessariamente completo para garantir isso.

**Definição:** Se  $<$  é uma ordem em  $V$  e  $v \in V$  é um vértice qualquer, então  $\gamma(v) = \{u \in V \mid u < v\}$  é dito conjunto de antecessores de  $v$  em relação a  $<$  e  $\rho(v) = |\gamma(v)| + 1$  é dito posto de  $v$  em  $<$ . Dado um grafo  $G = (V, E)$ , uma ordenação  $<$  sobre  $V$  é chamada *Ordem de  $K$ -Lateração* se:

1. os primeiros  $K+1$  vértices de  $<$  induzirem um  $(K+1)$ -clique  $G_o$  em  $G$ ;
2. todo vértice  $v$ , com  $\rho(v) > K+1$ , tem  $|N_G(v) \cap \gamma(v)| \geq K+1$ .

Um grafo  $G = (V, E)$  é dito *K-Laterativo* se há uma ordem de *K-lateração* sobre  $V$ . Perceba que um grafo *K-laterativo* não precisa ser completo e, mesmo assim, ainda é possível aplicar a *K-lateração* em todo vértice  $v \in V$ , com posto  $\rho(v) > K + 1$ , como é o caso ilustrado da Figura 2.19 para  $K = 2$ . Seguindo a ordenação  $(v_1, v_2, v_3, v_4, v_5)$ , pode-se utilizar a 3-clique  $\{v_1, v_2, v_3\}$  para realizar o vértice  $v_4$  e utilizar a 3-clique  $\{v_2, v_3, v_4\}$  para realizar o vértice  $v_5$ .

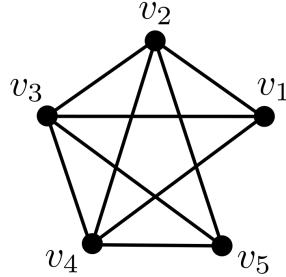


Figura 2.19: Grafo *K-laterativo* não completo, de 5 vértices e  $K = 2$ .

Como a existência de uma ordem de *K-lateração* garante, por definição, que sempre haverá ao menos  $K + 1$  vértices já realizados antecessores a todo vértice  $v \in V$ , com  $\rho(v) > K + 1$ , sempre será possível aplicar a *K-lateração*. Assim, um grafo *K-laterativo* possui no máximo uma solução.

**O Trilaterativo DGP (TDGP):** Um DGP  $(G, d, K)$  é chamado *Trilaterativo* se uma ordem de *K-lateração* sobre  $G$  for dada.

Dado um TDGP  $(G, d, K)$ , seja  $\{x_1, \dots, x_{K+1}\}$  o conjunto de realizações dos primeiros  $K + 1$  vértices em relação a ordem de *K-lateração*. Uma realização  $x$  de  $G$  em  $\mathbb{R}^K$  pode ser encontrada (ou mostrada que não existe) pelo Algorítimo 2.

---

**Algorithm 2:**  $x = \text{RealizacaoTrilaterativa}(G, d, K, x)$ , adaptado de [11]

---

```

1 for  $i \in \{K + 2, \dots, n\}$  do
    // Procure os primeiros  $K + 1$  predecessores adjacentes
    2    sejam  $U \subset |N_G(v) \cap \gamma(v)|$ , com  $|U| = K + 1$ , e  $W = \{x_j \mid j \in U\}$ 
    // Utilize o  $(K + 1)$ -clique definido por  $W$  para realizar  $x_i$ 
    3     $x_i = \text{Trilateracao}(W);$ 
    4    for  $\{j \in \{(N_G(v) \cap \gamma(v)) \setminus U\} ; j < i\}$  do
        5        if  $\|x_i - x_j\| \neq d_{ij}$  then
        6             $x_i = \emptyset;$ 
        7            break;
        8        end
    9    end
    10   if  $x_i = \emptyset$  then
    11       return  $\emptyset;$ 
    12   end
13 end
14 return  $x;$ 
```

---

Há três características que fazem desta uma boa solução para instâncias WSNL: (i) O  $(K + 1)$ -clique inicial necessita de uma realização dada a priori; (ii) sempre possuirá ou nenhuma (se não existe realização em  $\mathbb{R}^K$ ), ou exatamente uma solução; (iii) é resolvido em tempo polinomial.

### Realizando grafos $(K - 1)$ -laterativos em $\mathbb{R}^K$

Agora trataremos dos casos onde o grafo associado ao problema não possui vértices suficientes para a existência de uma ordem  $K$ -laterativa. Em particular, estudaremos o caso da busca de realização de um grafo  $(K - 1)$ -laterativo no espaço  $\mathbb{R}^K$ , que possui uma grande correlação com a classe de problemas moleculares.

Essa correlação vem da estrutura geométrica das proteínas. A cadeia principal de uma proteína é um conjunto  $V = \{v_1, \dots, v_n\}$  de átomos com uma certa ordem conveniente induzida pelas ligações químicas da molécula (veja o Apêndice B). Conhece-se distância de pares consecutivos  $\{v_{i-1}, v_i\}$ , para todo  $i \leq n$ , e também conhece-se o ângulo de ligação entre três átomos consecutivos  $(v_{i-2}, v_{i-1}, v_i)$ . Dessa forma, pode-se calcular a distância entre dois átomos separados por duas ligações, i.e., de pares  $v_{i-2}, v_i$ , ao se construir o triângulo formado pelos dados de distâncias e ângulos. Então, se a distância de pares  $\{v_{i-3}, v_i\}$  separados por três ligações não puderem ser determinadas (usando, por exemplo dados de RMN), então acontece que existe uma ordem alternativa para os vértices de forma que  $v_i$  seja sempre adjacente a pelo menos os últimos três predecessores [11].

Dessa forma, cadeias principais de proteínas podem ser modeladas por grafos 2-laterativos (i.e., cada vértice é adjacente a pelo menos 3 antecessores), que precisam ser realizadas no espaço  $\mathbb{R}^3$ . Porém, encontrar essa ordem nos vértices da molécula pode não ser trivial. O problema de encontrar essa ordem é definido como Problema da Orderm de Discretização (ou DVOP) e está relacionado com encontrar uma ordem de  $(K - 1)$ -lateração. É importante mencionar que o DVOP é um problema NP-Completo [46]. Entretanto, uma ordem pode ser construída manualmente, assim como feito em [47, 48]. Em particular, estudamos a chamada *Hand-crafted vertex order* — ou HC Order — criada por Carlile Lavor e colaboradores, como segue.

### HC Order

Seja  $G = (V, E, d)$  o grafo associado a cadeia principal de uma proteína ( $\{N^k, C_\alpha^k, C^k\}$ , para  $k = 1, \dots, p$ ), incluindo os átomos de oxigênio  $O^k$ , ligados ao  $C^k$ , e átomos de hidrogênio  $H^k$  e  $H_\alpha^k$ , ligados ao  $N^k$  e  $C_\alpha^k$ , respectivamente (conforme Figura 2.20, onde  $p = 3$ ).

Define-se a ordem HC como:

$$\begin{aligned} hc = & \{N^1, H^1, H^{1'}, C_\alpha^1, N^1, H_\alpha^1, C^1, C_\alpha^1, \dots, \\ & H^i, C_\alpha^i, O^{i-1}, N^i, H^i, C_\alpha^i, N^i, H_\alpha^i, C^i, C_\alpha^i, \dots, \\ & H^p, C_\alpha^p, O^{p-1}, N^p, H^p, C_\alpha^p, N^p, H_\alpha^p, C^p, C_\alpha^p, O^p, C^p, O^{p'}\} \end{aligned}$$

Onde, como na Figura 2.20,  $i = 2, \dots, p - 1$ ,  $H^{1'}$  é o segundo hidrogênio ligado ao  $N^1$  e  $O^{p'}$  é o segundo oxigênio ligado ao  $C^p$ .

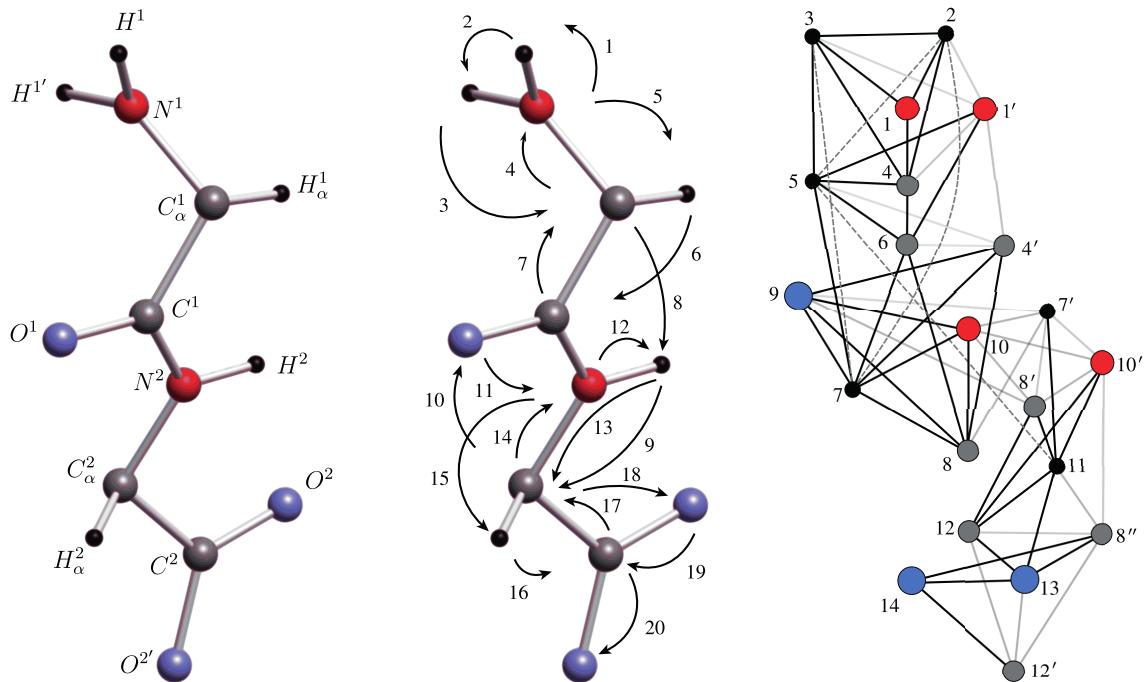


Figura 2.20: A esquerda, o esboço da cadeia principal expandida. No centro, uma representação da ordem HC. A direita, uma representação do grafo associado a ordenação.

Toda distância entre hidrogênios relativamente próximos (representados por vértices tracejados no grafo da Figura 2.20) — inclusive entre  $H_{\alpha}^{i-1}$  e  $H^i$  — são dados pela RMN. Também, para respeitar termos ao menos um grafo 2-laterativo, no átomo  $H^i$ , precisamos ter conhecimento do plano mostrado na Figura B.5 (veja Apêndice B), que diz que os átomos em torno da ligação peptídica são coplanares — e, por tanto, pode-se descobrir a distância entre o  $H^i$  e  $C_{\alpha}^{i-1}$  através das leis de senos e cossenos.

A ordenação HC gera uma estrutura muitíssimo interessante para se trabalhar. De fato, por garantir que sempre tenhamos pelo menos um 3-clique em todo átomo com posto maior que três, ao tentarmos localizar o quarto átomo estamos realizando um 4-clique no  $\mathbb{R}^3$  e, como vimos anteriormente, essa situação pode ter duas soluções (veja Figura 2.18). A interpretação geométrica disso é que estamos calculando a realização do próximo átomo da sequência  $v_i$  com  $i \geq 4$ , utilizando a interseção das 3 esferas centradas nos três átomos anteriores  $v_{i-3}, v_{i-2}$  e  $v_{i-1}$  (já realizados) e com os respectivos raios iguais as distâncias  $d_{i,i-3}, d_{i,i-2}$  e  $d_{i,i-1}$  para o átomo  $i$  que se está tentando localizar. Essas intersecções tem três possibilidades associadas (veja Figura 2.21): Ou não temos nenhum ponto de interseção entre elas — e isso não acontece, pois fere as hipóteses do problema, logo, só ocorre se existe alguma informação incorreta; Ou existe um ponto — donde os átomos são colineares e isso também nunca acontece, devido aos ângulos típicos das ligações; ou existem dois pontos onde as esferas se interceptam — este é o caso geral.

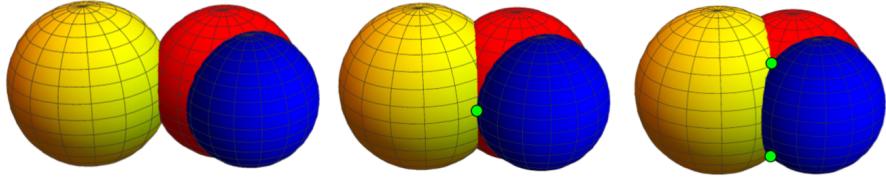


Figura 2.21: Interseção de três esferas [30].

Perceba, então, que além da ordenação dos vértices garantir a finitude do conjunto solução do problema, ela também organiza o espaço onde devemos fazer a busca por uma solução. Na verdade, a ordem induz uma estrutura de *árvore binária* no espaço de busca [10]. De fato, sempre temos duas possibilidades para posicionar o próximo átomo da molécula [12]. Com isso, ganhamos uma discretização do problema (pois saímos espaço contínuo de soluções), nos permitindo definir uma nova variante para ele.

### 2.3.5 *MDGP Discretizável*

Esse é o problema central desse texto. Trata-se do MDGP monido de uma ordenação conveniente que permite sua discretização, como segue formalmente definido.

**MDGP Discretizável (DMDGP):** Dados um grafo ponderado e não-direcionado  $G = (V, E, d)$  associado a um MDGP, onde  $d : E \rightarrow \mathbb{R}_+$ , o subconjunto de vértices iniciais  $U_0 = \{v_1, v_2, v_3\}$  e uma relação de ordem total em  $V$  que satisfaça a seguinte relação de axiomas:

1.  $G[U_0]$  é um clique em três vértices (iniciando a configuração);
2. para todo vértice  $v_i$  com posto  $i = \rho(v_i) > 3$  nesta ordem,  $G[U_i]$  é uma clique com quatro vértices (ordem de discretização, dada anteriormente) e
3. para cada vértice  $v_i$ , com posto  $i = \rho(v_i) > 3$ , juntamente com  $\{v_{i-3}, v_{i-2}, v_{i-1}\}$ , vale a desigualdade

$$d_{i-3,i-1} < d_{i-3,i-2} + d_{i-2,i-1}, \quad (\text{Desigualdade Triangular Estrita})$$

### Representações de Átomos em Coordenadas Internas

As coordenadas internas de uma proteína são definidas pela distância entre os átomos  $d_{1,2}, \dots, d_{n-1,n}$ , pelo ângulo planar  $\theta_{1,3}, \dots, \theta_{n-2,n}$  (formados por 3 átomos consecutivos) e pelos ângulos de torção  $\omega_{1,4}, \dots, \omega_{n-3,n}$  (formado por 4 átomos consecutivos), conforme ilustrado na Figura 2.22. O ângulo de torção é definido entre os planos formados pelos átomos  $i-3, i-2, i-1$  e  $i-2, i-1, i$ , respectivamente. Assim, temos que  $\omega$  varia no intervalo  $[0, 2\pi]$  e  $\theta$  de  $[0, \pi]$  — assim como em um sistema de coordenadas esféricas. As distâncias entre os átomos unidos por ligações covalentes são da ordem de  $1,5\text{\AA}$ .

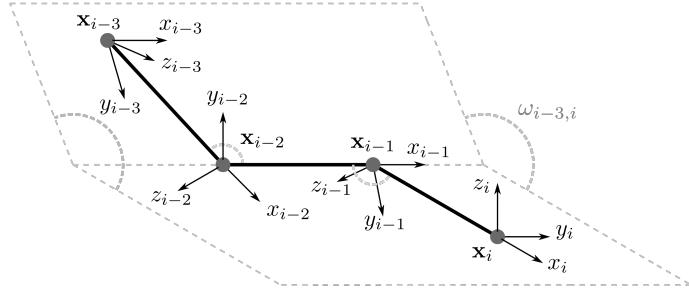


Figura 2.22: Ângulos planos e de torção

Pode-se obter facilmente os ângulos planos pela *Lei dos Cossenos*, tendo em vista que conhece-se todas as distâncias que, por construção, representam os lados do triângulo. Porém, descobrir o ângulo de torção associado (também chamado de ângulo diedral) merece um pouco mais de atenção.

O cosseno de um ângulo diedral pode ser dado em função de distâncias euclidianas e ângulos planos [27]. Sejam  $x_i, x_j, x_k, x_l \in \mathbb{R}^3$  quaisquer quatro átomos consecutivos com coordenadas  $(x_{i_1}, x_{i_2}, x_{i_3})$ ,  $(x_{j_1}, x_{j_2}, x_{j_3})$ ,  $(x_{k_1}, x_{k_2}, x_{k_3})$  e  $(x_{l_1}, x_{l_2}, x_{l_3})$ , respectivamente; Também  $r_{ab}$ , com  $a, b \in \{i, j, k, l\}$  as distâncias entre os átomos  $x_a$  e  $x_b$ ; e por último  $\theta_{ijk}$ , o ângulo definido pelos átomos  $x_i, x_j, x_k$  e  $\theta_{kji}$ , o ângulo definido pelos átomos  $x_k, x_j, x_i$ . Então, o cosseno do ângulo diedral  $\omega_{ijkl}$  é dado por:

$$\cos(\omega_{ijkl}) = \frac{r_{ij}^2 + r_{jl}^2 - 2r_{ij}r_{jl}\cos(\theta_{ijk})\cos(\theta_{kjl} - r_{il}^2)}{2r_{ij}r_{jl}\sin(\theta_{ijk})\sin(\theta_{kjl})}. \quad (2.24)$$

Porém, não temos como definir exatamente o seno desse ângulo. Só podemos fazer  $\sin(\omega_{ijkl}) = \pm\sqrt{1 - \cos(\omega_{ijkl})^2}$ . Mas vamos deixar esse problema do ângulo de torção para depois — por enquanto supomos que temos os valores exatos de  $\omega_{ijkl}$ .

Por tanto, conseguimos definir todo o problema a partir das coordenadas internas. Como nosso objetivo é obter as posições tridimensionais de cada átomo, nosso problema se restringiu em transformar as coordenadas internas em cartesianas. Para isso, utiliza-se uma série de operações lineares que estão descritas pelas matrizes abaixo.

Consideremos que as coordenadas do ponto  $x_i \in \mathbb{R}^3, i = 1, \dots, n$  são dadas por  $(x_{i1}, x_{i2}, x_{i3})$ , temos:

$$\begin{bmatrix} x_{i1} \\ x_{i2} \\ x_{i3} \\ 1 \end{bmatrix} = B_1 B_2 \cdots B_i \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

onde

$$B_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B_2 = \begin{bmatrix} -1 & 0 & 0 & -d_{1,2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$B_3 = \begin{bmatrix} -\cos\theta_{1,3} & -\sin\theta_{1,3} & 0 & -d_{2,3}\cos\theta_{1,3} \\ \sin\theta_{1,3} & -\cos\theta_{1,3} & 0 & d_{2,3}\sin\theta_{1,3} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

e

$$B_i = \begin{bmatrix} -c_{\theta_i} & -s_{\theta_i} & 0 & -d_{i-1,i}c_{\theta_i} \\ s_{\theta_i}c_{\omega_i} & -c_{\theta_i}c_{\omega_i} & -s_{\omega_i} & d_{i-1,i}s_{\theta_i}c_{\omega_i} \\ s_{\theta_i}s_{\omega_i} & -c_{\theta_i}s_{\omega_i} & c_{\omega_i} & d_{i-1,i}s_{\theta_i}s_{\omega_i} \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

dado  $s_{\theta_i} = \sin(\theta_{i-2,i})$ ,  $c_{\theta_i} = \cos(\theta_{i-2,i})$ ,  $s_{\omega_i} = \sin(\omega_{i-3,i})$ ,  $c_{\omega_i} = \cos(\omega_{i-3,i})$ . Em  $B_i$ ,  $i = 4, \dots, n$ .

Perceba que  $B_i$  (chamada *Matriz de Torção*) é a matriz que engloba todas as operações necessárias para encontrar a  $i$ -ésima realização do  $i$ -ésimo átomo da molécula, tendo conhecimento de todas as matrizes  $B_j \forall j < i$ . Como é de grande importância o entendimento de tais operações que formam a  $B_i$ , segue a separação das suas transformações em termos de matrizes de rotação e uma matriz de translação no espaço homogêneo:

$$B_i = R_x(w_{i-3,i}) \cdot R_x(\pi) \cdot R_z(\theta_{i-2,i}) \cdot R_y(\pi) \cdot T_x(d_{i-1,i}),$$

Note também que fixando os comprimentos das ligações covalentes  $d_{1,2}, d_{2,3}$  e o valor do ângulo plano  $\theta_{1,3}$ , os três primeiros átomos terão as coordenadas dadas por

$$x_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad x_2 = \begin{bmatrix} -d_{1,2} \\ 0 \\ 0 \end{bmatrix}, \quad x_3 = \begin{bmatrix} -d_{1,2} + d_{2,3} \cos \theta_{1,3} \\ d_{2,3} \sin \theta_{1,3} \\ 0 \end{bmatrix}.$$

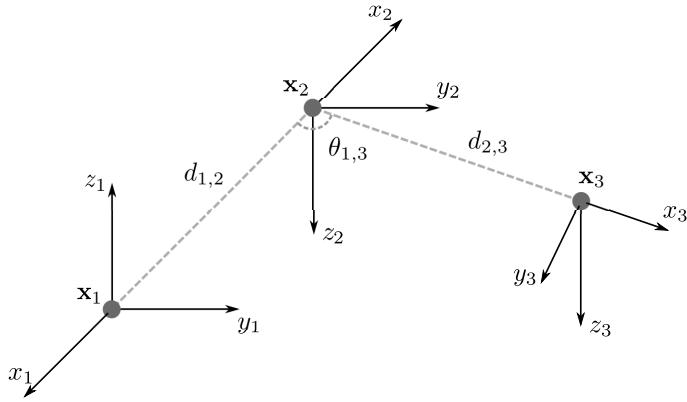


Figura 2.23: Inicialização do BP

Dadas essas três realizações dos primeiros átomos, fixamos a base do sistema, evitando estruturas obtidas por meio de rotações e translações a partir de uma mesma estrutura.

### Espaço de Busca por Soluções

Note que, usando os valores de distâncias das cliques  $\{v_{i-3}, v_{i-2}, v_{i-1}, v_i\}$  garantidas pelo DMDGP, temos gratuitamente todas as distâncias entre átomos consecutivos  $d_{1,2}, \dots, d_{n-1,n}$ , donde podemos obter facilmente os ângulos planos  $\theta_{1,3}, \dots, \theta_{n-2,n}$ .

Logo, sabendo que só precisamos das coordenadas internas para definir a estrutura 3D das proteínas — visto que podemos aplicar o conjunto de matrizes  $B_i$  para

realizar a conversão dos sistemas de coordenadas — como temos todas as distâncias e ângulos planos, só nos falta verificar os ângulos de torção  $\omega_{1,4}, \dots, \omega_{n-3,n}$ , que, como vimos, sempre possuímos dois possíveis ângulos associados ( $\omega_{i-3,i}^1$  e  $\omega_{i-3,i}^2$ ). Isso induz uma estrutura binária de decisão que é ilustrado na Figura 2.24, onde temos as duas posições possíveis ( $i$  e  $i'$ ) para o último vértice.

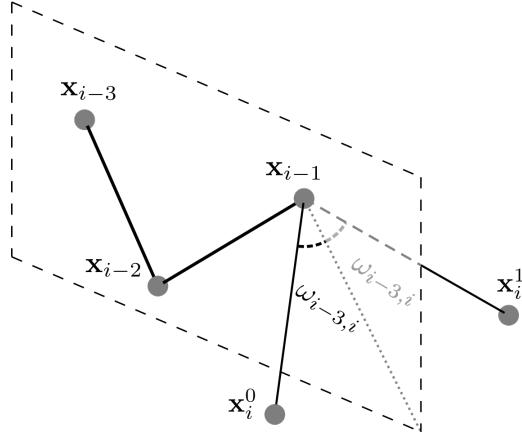


Figura 2.24: Duas possibilidades para o ângulo de torção.

### 2.3.6 Branch-and-Prune

Apresentado em 2007 [50], por Leo Liberti, Carlile Lavor e Nelson Maculan, este algorítimo (também chamado BP) consiste em uma estratégia numérica recursiva, que resolve o DMDGP eficientemente utilizando uma busca combinatória no espaço de busca de soluções, onde realiza-se vértice por vértice do sistema, seguindo a ordem dada, “podando” — isto é, descartando — todo sub-conjunto solução do sistema que não esteja de acordo com as informações pré-estabelecidas. Desde que ele foi publicado, tem se verificado tanto sua beleza matemática, quanto a sua eficiência numérica-computacional para resolver problemas em Geometria de Distâncias.

Como todo algorítimo, esse possui um conjunto de entradas e saídas.

**Entradas:** O grafo  $G(V, E, d)$  que define o DMDGP — onde possuímos uma ordenação para  $V$  — e mais um escalar  $\varepsilon \in \mathbb{R}$  que da a tolerância aceita no algoritmo (pois o BP não é um método exato, encontrando apenas soluções distantes a menos de  $\varepsilon$  das reais).

Para facilitar a utilização do algorítimo, também faremos uma distinção dos vértices que compõem o conjunto  $E$ : Sejam os subconjuntos  $E_d, E_p \subset E$ , tal que  $E = E_d \cup E_p$  — denominados como, respectivamente, *arestas de discretização* e *arestas de poda* —, onde

$$E_d = \{\{v_i, v_j\} \in E : |i - j| \leq 3\} \text{ e } E_p = E - E_d.$$

**Saídas:** Uma árvore binária  $T$ , onde cada nó de nível  $i$  da árvore é uma realização possível do vértice  $v_i \in V$ , de tal forma que o caminho  $C \subset T$  partindo da raiz (primeiro nó) até uma folha de nível  $n = |V|$  da árvore seja uma solução para o problema, isto é, um conjunto de realizações de todos os átomos da molécula.

São três fases que definem o algoritmo: Inicialização, *Branching* e *Pruning* [10].

## Inicialização

Esta etapa se preocupa com a inicialização da estrutura. Ela define a realização dos três primeiros átomos  $v_1, v_2$  e  $v_3 \in V$  da sequência, que são posicionados nas respectivas posições  $x_1, x_2$  e  $x_3 \in \mathbb{R}^3$ , utilizando as operações contidas nas matrizes  $B_1, B_2$  e  $B_3$ .

Essas três primeiras posições estão associados biunivocamente com os três primeiros nós da arvore de busca  $T$  (representada por um grafo), que também é iniciada, conforme Figura 2.25



Figura 2.25: Inicialização de  $T$  [10].

## Branching

Essa etapa está associada com o processo de “ramificação” de  $T$  [10]. Ou seja, supondo que já foram realizados os vértices  $v_1, \dots, v_{i-1}$  (onde  $3 < i < |V|$ ), repetindo a ordenação em  $V$ , nosso objetivo é obter a realização  $x_i = (x_{i1}, x_{i2}, x_{i3}) \in \mathbb{R}^3$  do vértice  $v_i \in V$ .

Para isso, basta calcularmos o produto matricial

$$\begin{bmatrix} x_{i1} \\ x_{i2} \\ x_{i3} \\ 1 \end{bmatrix} = C_i \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

onde  $C_i = C_{i-1}B_i = \prod_{j=1}^i B_j$  é dita o *produto acumulado* das matrizes de torção  $B_j$ . O conceito de ramificação vem do fato de sempre temos duas matrizes de torção  $B_j^1$  e  $B_j^2$  associadas a cada vértice  $v_j$  (por conta dos diferentes ângulos diedrais). A cada matriz de torção temos como resultado um novo conjunto de realizações, que se visualiza como um novo ramo de  $T$ .

Ilustramos esse processo na Figura 2.26, que presume um DMDGP com  $|V| = 6$ . Ou seja, obtemos  $2^{6-3} = 2^3 = 8$  possíveis soluções, dadas pelas suas 6 ramificações.

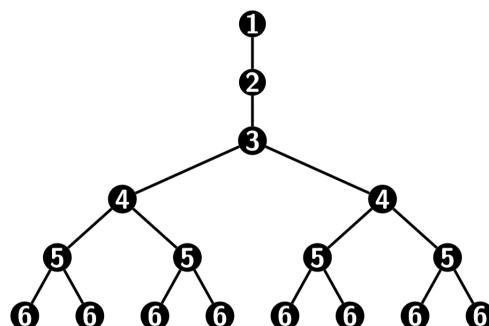


Figura 2.26: Árvore  $T$  completa de uma instância DMDGP com 6 vértices [10].

Fica claro aqui que o processo de ramificação garante que, no máximo, existem  $2^{n-3}$  soluções possíveis para o problema. Isso colabora com a enumerabilidade e finitude do conjunto solução do problema, porém, também mostra que o número de soluções cresce de uma forma exponencial com o crescimento da molécula.

### ***Pruning***

Essa etapa tem como função diminuir drasticamente o conjunto solução do problema. Conseguimos isso ao classificar os diferentes ramos de  $T$  (gerados pelos diferentes ângulos de torção  $\omega_{i-3,i}^1$  e  $\omega_{i-3,i}^2$ ) como factíveis ou não e, então, “podando” os infactíveis.

Como já discutimos antes, para calcular as matrizes de torção da etapa anterior só precisamos dos dados do 3-clique garantido pelas hipóteses do DMDGP, ou seja, das distâncias  $d_{i,i-3}$ ,  $d_{i,i-2}$  e  $d_{i,i-1}$  associadas aos elementos de  $E_d$ . Com isso, todas as distâncias associadas aos elementos de  $E_p$  podem ser consideradas como dados adicionais para o problema.

Perceba que, para todo  $v_j$  tal que  $\{v_i, v_j\} \in E_p$ , se conhecemos a realização de  $v_j$ , a distância extra  $d_{i,j}$  pode ser enxergada, do ponto de vista geométrico, como uma esfera extra àquelas outras três dadas pelo 3-clique. Isso gera a interseção de quatro esferas no  $\mathbb{R}^3$ , donde podemos ter apenas uma das duas possibilidades: Ou elas se interceptam em um único ponto (veja Figura 2.27) ou em nenhum.

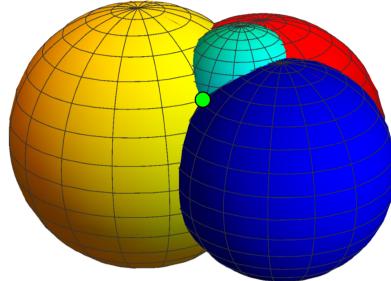


Figura 2.27: Interseção de quatro esferas no  $\mathbb{R}^3$  [30].

E é este o princípio da factibilidade de um ramo: Sempre que estamos na etapa de *Branching* — ou seja, calculando uma realização  $x_i$  de  $v_i$  a partir de uma matriz de torção —, podemos verificar se existe uma distância extra, associada a algum elemento  $\{v_i, v_j\} \in E_p$  tal que  $j < i$  e, caso exista, podemos verificar se  $|x_i - x_j| < \varepsilon$ . Caso for, significa que o ramo é factível e, caso não for, podemos descartar (“podar”) todas as soluções associadas a sub-árvore definida por aquele ramo.

A etapa de *pruning* é ilustrada na Figura 2.28 (adaptada de [10]). Dando continuidade ao exemplo da Figura 2.26, agora temos  $E_p = \{\{v_1, v_5\}, \{v_2, v_6\}\}$ , o que nos permitiu testar a factibilidade dos ramos associados ao  $v_5$  e ao  $v_6$  e podar os infactíveis, diminuindo consideravelmente o conjunto solução.

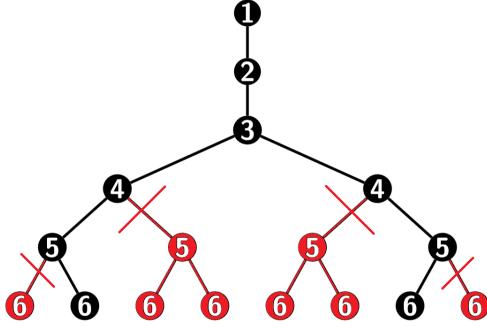


Figura 2.28: Árvore  $T$  de um DMDGP de 6 vértices com a poda evidenciada.

Perceba que o crescimento exponencial de soluções ( $2^{n-3}$ ) da etapa de *branching* está associado com o DMDGP ser um problema NP-Difícil. Por conta disso é que esse algorítimo tem tanta beleza associada, isto é, apesar da grande complexidade de se resolver o problema original, o BP pode encontrar rapidamente essas soluções.

Mas uma dúvida ainda é importante: O conjunto  $E_p = \emptyset$ ? Neste caso,  $E = E_d$  e, portanto, todas as posições finais são factíveis trivialmente. Dessa forma, todas as  $2^{n-3}$  realizações encontradas durante a etapa de *branching* representam soluções possíveis para o DMDGP, o que, é claro, é o nosso pior caso, pois o BP precisa continuar a exploração de todos os  $2^{n-3}$  nós de  $T$ .

Por outro lado, se utilizarmos a ordenação hc como ordem que define o DMDGP, nós garantimos que  $E_p \neq \emptyset$ . Essa é uma das vantagens dessa ordenação. Na verdade, muito mais do que não vazio, graças as propriedades geométricas das proteínas estudadas em [47] nós podemos enunciar o seguinte resultado (extraído de [47]):

**Teorema 2.3.1.** *Usando a ordenação hc, considerando que todos os ângulos e distâncias das ligações atômica estão fixadas nos seus valores de equilíbrio energético (essa é conhecida como hipótese de geometria rígida), que os átomos ao redor das ligações peptídicas formam um plano, que as posições possíveis para  $C_\alpha^1$  e  $C^j$  (com  $j = 1, \dots, p$ ) são únicas — devido a propriedade quiral do tetraedro formado por  $\{N^1, H^1, H^1, C_\alpha^1\}$  e  $\{C_\alpha^j, N^j, H^j, C^j\}$  — e, dado o conjunto de distâncias entre os pares de átomos de hidrogênio*

$$\{H^{1'}, H_\alpha^1\}, \dots, \{H_\alpha^{i-1}, H^i\}, \{H^i, H_\alpha^i\}, \{H_\alpha^i, H^{i+1}\}, \dots, \{H^p, H_\alpha^p\}$$

(onde  $i = 2, \dots, p - 1$  e  $p$  é o número de aminoácidos que compõem a proteína), as ramificações na árvore de busca só ocorrem em átomos de hidrogênio dados por

$$\{H_\alpha^1, \dots, H^i, H_\alpha^i, \dots, H^p, H_\alpha^p\}.$$

## Algorítimo

Agora que a ideia por trás do BP está desenvolvida nos três passos anteriores (inicialização, *branching* e *pruning*) podemos apresentá-lo formalmente como um algorítimo de uma função recursiva, como segue.

---

**Algorithm 3:** Algoritmo BP [10] [50]

```
1 BranchAndPrune( $T, v, i$ )
2 if  $i \leq n - 1$  then
3   Calcule as matrizes de torção  $B_i^1$  e  $B_i^2$ ;
4   Recupere a matriz de torção acumulada  $C_{i-1}$  referente ao nó-pai  $P(v)$ ;
5   Calcule as próximas matrizes de torção acumuladas  $C_i = C_{i-1}B_i^1$  e
6      $C'_i = C_{i-1}B_i^2$ ;
7   Utilize-as para calcular as posições  $x_i = C_iy$  e  $x'_i = C'_i y$ ;
8   Seja  $\lambda = 1, \rho = 1$ ;
9   foreach  $\{v_j, v_i\} \in E_p$  com  $j < i$  do
10    if  $(\|x_j - x_i\|^2 - d_{ij}^2)^2 > \varepsilon$  then
11       $\lambda = 0$ ;
12    end
13    if  $(\|x_j - x'_i\|^2 - d_{ij}^2)^2 > \varepsilon$  then
14       $\rho = 0$ ;
15    end
16  end
17  if  $\lambda = 1$  then
18    Crie um nó  $z$ , armazenando  $C_i$  e  $x_i$  e fazendo  $P(z) = v$  e  $L(v) = z$ ;
19    Faça  $T \leftarrow T \cup \{z\}$ ;
20    BranchAndPrune( $T, z, i + 1$ );
21  else
22    Faça  $L(v) = \text{PRUNED}$ ;
23  end
24  if  $\rho = 1$  then
25    Crie um nó  $z'$ , armazenando  $C'_i$  e  $x'_i$  e fazendo  $P(z') = v$  e  $R(v) = z'$ ;
26    Faça  $T \leftarrow T \cup \{z'\}$ ;
27    BranchAndPrune( $T, z', i + 1$ );
28  else
29    Faça  $R(v) = \text{PRUNED}$ ;
30  end
31  | Solução está armazenada nos nós-pais de  $n$  a 1, em busca retrocedida.
32 end
```

---

# 3

## Materiais e Métodos

### 3.1 BP com Quaternios

# **4**

## **Resultados e Discussão**

### **4.1 Contando Operações**

### **4.2 Pré-processamento Molecular**

### **4.3 Resultados Computacionais**

### **4.4 Publicações Relacionadas**

O Relatório Final e Parcial (quando necessário) deve relacionar, quando for o caso, as eventuais participações do bolsista nos principais congressos da área e publicações com o orientador em periódicos indexados e/ou com corpo editorial. Deve relacionar os títulos/autores e nome dos periódicos com referência bibliográfica completa.

este trabalho é um desdobramento de uma pesquisa em andamento do prof f f e cita os artigos publicados em congresso e diz que é coautor de um artigo submetido em revista tal

# 5

## Considerações Finais

O Relatório Final e Parcial (quando for o caso) precisa conter, ainda, nas conclusões, uma avaliação do aluno em relação aos benefícios da IC no seu aprendizado e formação científica.

# Referências Bibliográficas

- [1] Gerald Sommer. *Geometric computing with Clifford algebras: theoretical foundations and applications in computer vision and robotics*. Springer Science & Business Media, 2013.
- [2] Hermann Grassmann. *Die lineale Ausdehnungslehre ein neuer Zweig der Mathematik: dargestellt und durch Anwendungen auf die übrigen Zweige der Mathematik, wie auch auf die Statik, Mechanik, die Lehre vom Magnetismus und die Krystallonomie erläutert*, volume 1. O. Wigand, 1844.
- [3] Professor Clifford. Applications of grassmann's extensive algebra. *American Journal of Mathematics*, 1(4):350–358, 1878.
- [4] Pertti Lounesto. *Clifford algebras and spinors*, volume 286. Cambridge university press, 2001.
- [5] Douglas Lundholm and Lars Svensson. Clifford algebra, geometric algebra, and applications. *arXiv preprint arXiv:0907.5356*, 2009.
- [6] Carl Benjamin Boyer. *História da matemática*. Edgard Blücher/EDUSP, São Paulo, 3 edition, 1974.
- [7] César Polcino Milies. *Breve história da álgebra abstrata*. USP, São Paulo, 2014.
- [8] J. B. Kuipers. *Quaternions and Rotation Sequences*. Princeton University Press, Princeton, New Jersey, 1999.
- [9] William Rowan Hamilton. *Elements of Quaternions*. London: Longmans, Green and Co, Dublin, first edition, 1866. Book II pag 156.
- [10] Felipe Delfini Caetano Fidalgo. *Dividindo e conquistando com simetrias em geometria de distâncias*. PhD thesis, UNICAMP, Campinas, SP, Fevereiro 2015.
- [11] Leo Liberti and Carlile Lavor. *Euclidean Distance Geometry*. Springer, 2017.
- [12] Leo Liberti, Carlile Lavor, Nelson Maculan, and Antonio Mucherino. Euclidean distance geometry and applications. *Society for Industrial and Applied Mathematics*, 56(1):3–69, February 2014.
- [13] Irineu Bicudo et al. *Os elementos*. Unesp, 2009.
- [14] Leo Liberti and Carlile Lavor. Six mathematical gems from the history of distance geometry. *International Transactions in Operational Research*, 23(5):897–920, 2016.

- [15] Arthur Cayley. A theorem in the geometry of position. *Cambridge Mathematical Journal*, 2:267–271, 1841.
- [16] Douglas S Gonçalves. *Geometria de Distâncias: aspectos teóricos e computacionais*, volume 91. São Carlos, SP : SBMAC, Notas em Matemática Aplicada, 2020.
- [17] Karl Menger. Untersuchungen über allgemeine metrik. *Mathematische Annalen*, 100(1):75–163, 1928.
- [18] Andrew J Hanson. Geometry for n-dimensional graphics., 1994.
- [19] Leonard M Blumenthal. *Theory and applications of distance geometry*. Oxford University Press, Oxford, 1953.
- [20] Manfred J Sippl and Harold A Scheraga. Cayley-menger coordinates. *Proceedings of the National Academy of Sciences*, 83(8):2283–2287, 1986.
- [21] Yechiam Yemini. Some theoretical aspects of position-location problems. In *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)*, pages 1–8. IEEE, 1979.
- [22] Gordon M Crippen, Timothy F Havel, et al. *Distance geometry and molecular conformation*, volume 74. Research Studies Press Taunton, 1988.
- [23] Yechiam Yemini. The positioning problem-a draft of an intermediate summary. Technical report, UNIVERSITY OF SOUTHERN CALIFORNIA MARINA DEL REY INFORMATION SCIENCES INST, 1978.
- [24] Deepak Tolani, Ambarish Goswami, and Norman I Badler. Real-time inverse kinematics techniques for anthropomorphic limbs. *Graphical models*, 62(5):353–388, 2000.
- [25] Jan de Leeuw and Willem Heiser. 13 theory of multidimensional scaling. *Handbook of statistics*, 2:285–316, 1982.
- [26] David L Nelson and Michael M Cox. *Lehninger principles of biochemistry*. W.H.Freeman and Company, 2013.
- [27] Carlile Lavor. *Uma abordagem determinística para minimização global da energia potencial de moléculas*. PhD thesis, PhD thesis, COPPE/UFRJ, Rio de Janeiro, 2001.
- [28] GN Ramachandran, AS Kolaskar, C Ramakrishnan, and V Sasisekharan. The mean geometry of the peptide unit from crystal structure data. *Biochimica et Biophysica Acta (BBA)-Protein Structure*, 359(2):298–302, 1974.
- [29] Andreas Savvides, Chih-Chieh Han, and Mani B Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, pages 166–179. ACM, 2001.

- [30] C. Lavor, N. Maculan, M. Souza, and R. Alves. *Álgebra e Geometria no Cálculo de Estrutura Molecular*. IMPA, Rio de Janeiro, RJ, 31º colóquio brasileiro de matemática edition, 2017.
- [31] Agner Fog et al. Instruction tables: Lists of instruction latencies, throughputs and micro-operation breakdowns for intel, amd and via cpus. *Copenhagen University College of Engineering*, 93:110, 2011.
- [32] Leo Liberti, Carlile Lavor, Antonio Mucherino, and Nelson Maculan. Molecular distance geometry methods: from continuous to discrete. *International Transactions in Operational Research*, 18(1):33–51, 2011.
- [33] Carlile Lavor, Leo Liberti, Nelson Maculan, and Antonio Mucherino. Recent advances on the discretizable molecular distance geometry problem. *European Journal of Operational Research*, 219(3):698–706, 2012.
- [34] James B Saxe. Embeddability of weighted graphs in k-space is strongly np-hard. In *Proc. of 17th Allerton Conference in Communications, Control and Computing, Monticello, IL*, pages 480–489, 1979.
- [35] Carlile Lavor, Leo Liberti, Weldon A Lodwick, and Tiago Mendonça da Costa. *An Introduction to Distance Geometry applied to Molecular Geometry*. Springer, 2017.
- [36] Riccardo Benedetti and Jean-Jacques Risler. In real algebraic and semi-algebraic sets. *Berlin, Hermann, Paris*, 1990.
- [37] Tolga Eren, OK Goldenberg, Walter Whiteley, Yang Richard Yang, A Stephen Morse, Brian DO Anderson, and Peter N Belhumeur. Rigidity, computation, and randomization in network localization. In *IEEE INFOCOM 2004*, volume 4, pages 2673–2684. IEEE, 2004.
- [38] Ana Flávia da Cunha Lima. Rigidez de grafos e aplicações. Master’s thesis, UNICAMP, IMECC, Campinas, SP, 2015.
- [39] Qunfeng Dong and Zhijun Wu. A linear-time algorithm for solving the molecular distance geometry problem with exact inter-atomic distances. *Journal of Global Optimization*, 22(1-4):365–375, 2002.
- [40] Elon Lages Lima. *Álgebra Linear*. SBM, Rio de Janeiro : IMPA, 1a edition, 2014.
- [41] Lloyd N Trefethen and David Bau III. *Numerical linear algebra*, volume 50. Siam, 1997.
- [42] Bruce Hendrickson. Conditions for unique graph realizations. *SIAM journal on computing*, 21(1):65–84, 1992.
- [43] Robert Connelly. On generic global rigidity, applied geometry and discrete mathematics, 147–155. *DIMACS Ser. Discrete Math. Theoret. Comput. Sci*, 4, 1991.

- [44] Bernhard Hofmann-Wellenhof, Herbert Lichtenegger, and James Collins. *Global positioning system: theory and practice*. Springer Science & Business Media, 2012.
- [45] Fernando Correia et al. Condições necessárias e suficientes para a realização de um conjunto de distâncias através de determinantes de cayley-menger. 2016.
- [46] Andrea Cassioli, Oktay Günlük, Carlile Lavor, and Leo Liberti. Discretization vertex orders in distance geometry. *Discrete Applied Mathematics*, 197:27–41, 2015.
- [47] Carlile Lavor, Leo Liberti, Bruce Donald, Bradley Worley, Benjamin Bardiaux, Thérèse E Malliavin, and Michael Nilges. Minimal nmr distance information for rigidity of protein graphs. *Discrete Applied Mathematics*, 256:91–104, 2019.
- [48] Virginia Costa, Antonio Mucherino, Carlile Lavor, Andrea Cassioli, Luiz M Carvalho, and Nelson Maculan. Discretization orders for protein side chains. *Journal of Global Optimization*, 60(2):333–349, 2014.
- [49] Carlile Lavor, Leo Liberti, Nelson Maculan, and Antonio Mucherino. The discretizable molecular distance geometry problem. *Computational Optimization and Applications*, 52(1):115–146, 2012.
- [50] Leo Liberti, Carlile Lavor, and Nelson Maculan. A branch-and-prune algorithm for the molecular distance geometry problem. *International Transactions in Operational Research*, 15(1):1–17, 2008.
- [51] J. A. Bondy and U. S. R. Murty. *Graph Theory With Applications*. Elsevier Science Publishing, New York, 5 edition, 1982.
- [52] Leonhard Euler. Leonhard euler and the königsberg bridges. *Scientific American*, 189(1):66–72, 1953.
- [53] W.W. Rouse Ball. Hsm coxeter mathematical recreations and essays, 1956.
- [54] Frank Harary. *Graph Theory*. Westview Press, 1969.
- [55] Gustav Kirchhoff. Ueber die auflösung der gleichungen, auf welche man bei der untersuchung der linearen vertheilung galvanischer ströme geführt wird. *Annalen der Physik*, 148(12):497–508, 1847.
- [56] A Cayley. On the theory of the analytical forms called trees, math, 1897.
- [57] Jayme Luiz Szwarcfiter. *Teoria computacional de grafos: Os algoritmos*. Elsevier Brasil, 2018.
- [58] wwPDB.org. Worldwide protein data bank.
- [59] Emerson Castelani; Repositório da MolecularConformation.jl; Acesso em 11/08/2019. Url = “<https://github.com/evcastelani/molecularconformation.jl>”.

# Apêndice A

## Teoria de Grafos

Esta seção tem como objetivo apresentar um breve resumo da *Teoria de Grafos*, tema amplamente estudado por diversos matemáticos e aplicado em diversas áreas do conhecimento como computação, engenharia e matemática [51].

### Descoberta (Eureka!)

Costuma-se dizer que a teoria se iniciou em 1736, com base no artigo publicado por Leonhard Euler (1707 a 1783) sobre as 7 pontes de Königsberg [52], representada na Figura A.1. Conta a história que os moradores daquela região perguntavam-se sobre a possibilidade de atravessar todas as sete pontes do local sem ter que repetir alguma delas. Esse é um problema muito usado para introduzir o tema [53] — propõe-se o desafio de ligar todos os pontos de um desenho sem tirar o lápis do papel e sem passar duas vezes no mesmo ponto. Para o caso das pontes de Königsberg, Euler provou que era impossível fazer isso ao formular matematicamente o problema, dando origem a esta teoria.

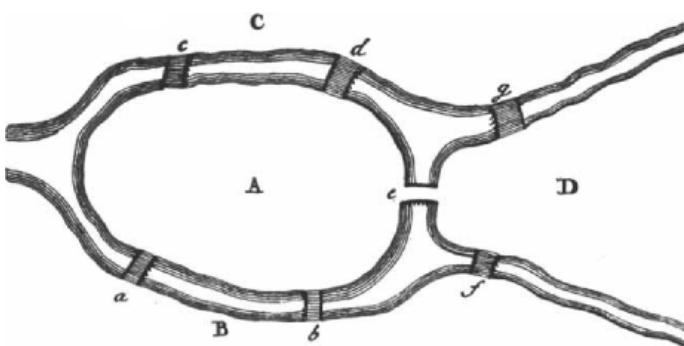


Figura A.1: Ilustração original do problema [52].



Figura A.2: Euler.

A grande ideia de Euler foi abstrair o problema:vê-lo de uma forma elementar, como um conjunto de pontos conectados por curvas. Isso pode ser representado por um “gráfico”, conforme a Figura A.3 — é daí a origem do termo em inglês “Graph”, que é tradução literal de “Gráfico”. Essa representação facilita a análise e a busca por uma solução. Com isso, Euler percebeu que só seria possível solucionar o problema se houvesse exatamente nenhum ou apenas dois pontos conectados por um número ímpar de curvas (ou pontes) — o par de caminhos está associado com o ato de entrar

e sair de um ponto [52]. Note que o caso de Koenigsberg, não possui solução.

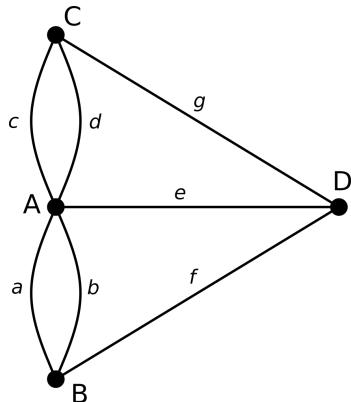


Figura A.3: Grafo representando o caso da ponte de Koenigsberg.

Mas não se pode deixar todo o mérito com Euler. O conceito de grafo é muito intuitivo e foi proposto por diversas mentes brilhantes como forma de solucionar problemas que, em essência, são muito parecidos. Após Euler, a teoria foi redescoberta por Gustav Kirchhoff (1824 a 1887) e Arthur Cayley (1821 a 1895) [54]. Kirchhoff desenvolveu esse conceito por volta de 1847, enquanto solucionava sistemas de equações lineares que relacionavam as correntes que percorriam as malhas de um circuito elétrico [55]. Dez anos depois, em 1857, foi a vez de Cayley, que estudava diferentes estruturas em bioquímica formadas por carbonos (com quatro ligações químicas) e hidrogênios (com apenas uma ligação), onde conseguiu formular seu problema introduzindo o conceito de árvore em grafos [56].

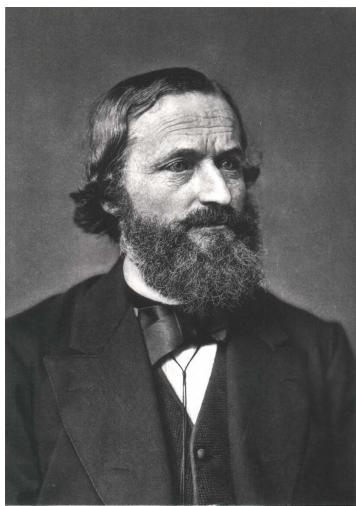


Figura A.4: Gustav Kirchhoff.

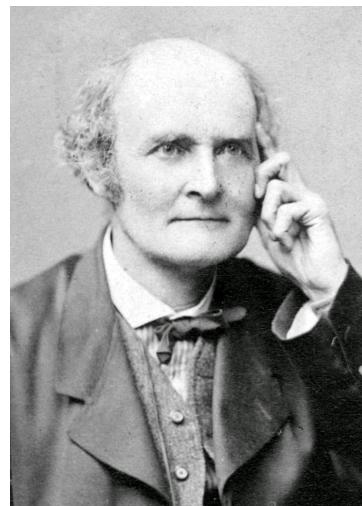


Figura A.5: Arthur Cayley.

Além dessas, muitas outras situações reais podem ser convenientemente representadas por simples diagramas contendo um conjunto de pontos e um conjunto de relações entre pares desses pontos. Por exemplo, pode-se definir o conjunto  $P = \{a, b, c\}$  das pessoas  $a, b$  e  $c$  e um conjunto  $A = \{\{a, b\}, \{b, c\}\}$  como o conjunto de amizades entre essas pessoas — no caso,  $a$  é amigo de  $b$ , que é amigo de  $c$ , porém

$a$  não é amigo de  $c$ . Esta análise se torna muitíssimo útil quando se deseja estudar como uma informação se propaga em redes sociais.

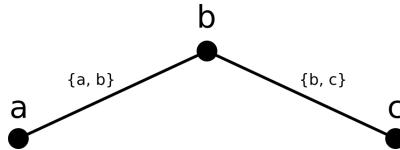


Figura A.6: Grafo representando a relação entre as pessoas  $\{a, b, c\}$ .

## Algumas definições importantes

Não há um forte consenso sobre as terminologias usadas pelos autores sobre grafos. Essa confusão se deve tanto pela sua vasta disseminação em diversas áreas como pela enorme abstração que ela carrega. Cayley poderia chamar as relações entre pontos de ligações químicas enquanto Kirchhoff chamaria de curto-circuitos. No que se segue, há aqui um apanhado de definições sobre a Teoria de Grafos fortemente baseado em [54] e [51]. Mas não sobre toda ela. Essa é uma grande área da matemática e não cabe abordá-la completamente nesse texto. Trata-se apenas do essencial para que o leitor possa progredir sem ter que consultar uma bibliografia complementar sobre grafos.

**Definição:** Um *Grafo*  $G$  é uma tripla ordenada da forma  $(V_G, E_G, \psi_G)$ , composta por um *Conjunto de Vértices*  $V_G$ , um *Conjunto de Arestas*  $E_G$  e uma *Função de Incidência*  $\psi_G$  que, por sua vez, associa a cada elemento de  $E_G$  um par não ordenado de elementos (nem sempre distintos) de  $V_G$ .

Nesse texto, porém, abstraiu-se a função de incidência  $\psi_G$  pois entende-se que o conjunto de arestas  $E_G$  é tal que, se  $e \in E_G$ , então  $e = \{a, b\}$  onde  $a, b \in V_G$ . Fica implícita, portanto, a associação dos elementos de  $V_G$  e  $E_G$ .

Aos elementos dos conjuntos  $V_G$  e  $E_G$ , refere-se-os por *Vértices* e *Arestas*, respectivamente. Também, para uma aresta  $e \in E_G$ , onde  $e = \{u, v\}$ , diz-se que  $u$  e  $v$  são *Vértices Adjacentes*. Chama-se  $u$  e  $v$  de *Incidentes*, assim como  $v$  e  $e$ . À quantidade de vértices adjacentes a  $v$  dá-se o nome *Grau* de  $v$ . Para um vértice  $v \in V_G$ , define-se o *Conjunto Vizinhança*  $N_G(v)$  como o conjunto de todos os vértices  $u \in V_G$  adjacentes a  $v$ . Também, se duas arestas distintas  $e_1$  e  $e_2$  são incidentes com um vértice em comum, diz-se que  $e_1$  e  $e_2$  são *Arestas Adjacentes*.

Seja um grafo com  $m$  vértices e  $n$  arestas, dizer-se-á que este é um  $(m, n)$  *grafo*. Isto é, a Figura A.6, para ilustrar, contém um  $(3, 2)$  grafo onde os vértices  $a$  e  $b$  são adjacentes, assim como as arestas  $\{a, b\}$  e  $\{b, c\}$ , porém, os vértices  $a$  e  $c$  não são. Define-se o  $(1, 0)$  Grafo como *Trivial*.

Existem muitas variações de grafos. A definição de grafo permite *Loops* (também chamado de *Laço*, uma aresta da forma  $e = \{v, v\}$ , ou seja,  $v$  é adjacente a si mesmo) e *Múltiplas Arestas* (mais do que uma aresta ligando os mesmos dois vértices). Grafos que não permitem múltiplas arestas ou loops são ditos *Simples*. Grafos que

permitem múltiplas arestas, mas não loops, são chamados de *Multigrafos*. Caso também permitam os loops, os chamamos de *Pseudografos*. Na Figura A.3 (do problema das pontes de Koenigsberg) temos um multigrafo e na Figura A.7 um pseudografo.

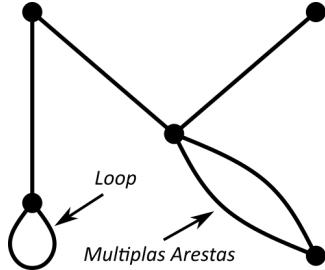


Figura A.7: Exemplo de pseudografo contendo 5 vértices e 6 arestas.

Porém, para esse trabalho não interessa o estudo de multigrafos ou pseudografos. Por isso, adotou-se uma definição alternativa para grafos, visando restringir sua aplicação, como segue:

**Definição:** Um *Grafo Simples*  $G$  é uma dupla ordenada da forma  $(V_G, E_G)$ , composta por um conjunto não nulo e finito  $V_G$  e outro conjunto finito  $E_G$  de pares não ordenados de elementos **distintos** pertencentes a  $V_G$ .

Diz-se que um  $(m, n)$  grafo  $G$  é *Rotulado* quando pode-se distinguir seus  $m$  vértices ao nomeá-los — algo como  $v_1, v_2, \dots, v_m$ . Por exemplo, os grafos da Figura A.8 são rotulados, enquanto o grafo da Figura A.7 não é. Quando não é dito o contrário, considera-se todo grafo como rotulado.

Dois grafos  $G = (V_G, E_G)$  e  $H = (V_H, E_H)$  são ditos *Isomorfos* (escreve-se  $G \cong H$ ) quando existe uma correspondência biunívoca entre os conjuntos de vértices  $V_G$  e  $V_H$  que preserve suas adjacências. A Figura A.8 ilustra essa situação, com a correspondência  $v_i \longleftrightarrow v_i$ .

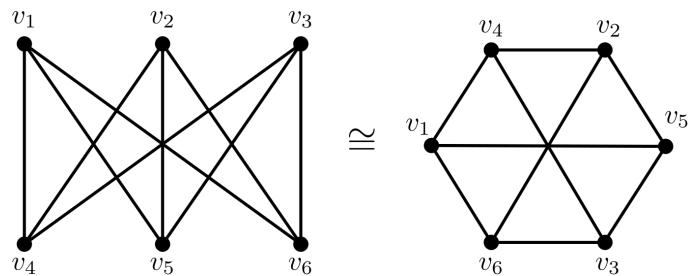


Figura A.8: Diferentes representações isomórficas de um  $(6, 9)$  grafo.

O isomorfismo é uma relação de equivalência. Fica claro que, por mais que seja útil, a representação gráfica de um grafo existe apenas como um apelo intuitivo. A forma geométrica formada pelos vértices é escolha de quem desenha. Vários são os casos em que problemas envolvendo grafos são facilmente solucionáveis apenas rearranjando a forma como se desenha — como o caso das pontes de Koenigsberg. A resposta salta aos olhos.

## Subgrafos

Diz-se que o grafo  $G_1 = (V_{G_1}, E_{G_1})$  é *Subgrafo* de  $G = (V_G, E_G)$  se  $V_{G_1} \subset V_G$  e  $E_{G_1} \subset E_G$ . Se  $G_1$  é subgrafo de  $G$ , então  $G$  é *Supergrafo* de  $G_1$ . Para qualquer  $V \subset V_G$ , existe um *Subgrafo Induzido*  $\langle V \rangle$  definido por  $(V, E)$ , onde  $E \subset E_G$  contém todas as arestas  $(v_1, v_2) \in E_G$  tal que  $v_1, v_2 \in V$ . Fica claro que dois vértices em  $\langle V \rangle$  são adjacentes se, e somente se, forem também adjacentes em  $G$ .

Pode-se *remover* um vértice  $v$  de um grafo  $G = (V_G, E_G)$ , que resulta no subgrafo induzido  $G - v = \langle V_G \setminus \{v\} \rangle$ . Da mesma forma, pode-se *remover* uma aresta  $e$  de um grafo  $G = (V_G, E_G)$ , resultando no grafo  $G - e = (V_G, E_G \setminus \{e\})$ .

## Caminhos

Um *Passeio* em  $G$  é uma sequência finita não nula  $W = v_0e_1v_1e_2v_2\dots e_kv_k$ , onde seus termos são alternados entre vértices e arestas, tal que, para  $1 \leq i \leq k$ , antes e depois de  $e_i$  vem  $v_{i-1}$  e  $v_i$ , respectivamente. Diz-se que  $W$  é um passeio de  $v_0$  para  $v_k$ , ou um  $(v_0, v_k)$ -passeio. Os vértices  $v_0$  e  $v_k$  são chamados origem e fim do passeio, respectivamente, e  $v_1, v_2, \dots, v_{k-1}$  são os vértices internos. O número  $k$  é o comprimento de  $W$ . Em um grafo simples, um passeio  $v_0e_1v_1e_2v_2\dots e_kv_k$  é determinado suficientemente pela sequência dos vértices que o constitui  $v_0v_1v_2\dots v_k$ .

Se  $W = v_0v_1\dots v_k$  e  $W' = v_kv_{k+1}\dots v_l$  são passeios, o passeio  $W^{-1} = v_kv_{k-1}\dots v_0$  é dito *Passeio Reverso* de  $W$  e o passeio  $WW' = v_0v_1\dots v_l$  é dito *Concatenação* de  $W$  com  $W'$ . Chama-se *Seção* do passeio  $W$  uma subsequência  $(v_i, v_j)$ -seção  $= v_iv_{i+1}\dots v_j$  de termos consecutivos de  $W$ .

Se as arestas  $e_1, e_2, \dots, e_k$  de um passeio  $W$  são todas distintas — o que sempre ocorre em grafos simples — chama-se  $W$  de *Trilha*. Se, adicionalmente, os vértices da trilha  $W$  forem todos distintos, chama-se  $W$  de *Caminho* (também conhecido como *Caminho Simples*).

## Conectividade

Dois vértices  $u$  e  $v$  de  $G$  são ditos *Conectados* se existe um  $(u, v)$ -passeio em  $G$ . A conectividade induz uma relação de equivalência sobre o conjunto de vértices  $V$ : Há uma partição de  $V$  em subconjuntos não vazios  $V_1, V_2, \dots, V_\omega$  tal que dois vértices  $u$  e  $v$  são conectados se, e somente se,  $u$  e  $v$  pertencem ambos ao mesmo subconjunto  $V_i$ . Os subgrafos induzidos  $\langle V_1 \rangle, \langle V_2 \rangle, \dots, \langle V_\omega \rangle$  são chamados *Componentes de  $G$* . Se  $G$  tem exatamente uma única componente, então  $G$  é dito *Conectado*; e, do contrário,  $G$  é dito *Desconectado*.

A Figura A.9 mostra dois grafos: O grafo da esquerda é conectado — possui uma única componente  $\langle \{v_1, v_2, v_3, v_4\} \rangle$ ; porém, o da direita não é — pois possui duas componentes  $\langle \{v_1, v_2, v_3\} \rangle, \langle \{v_4\} \rangle$ .

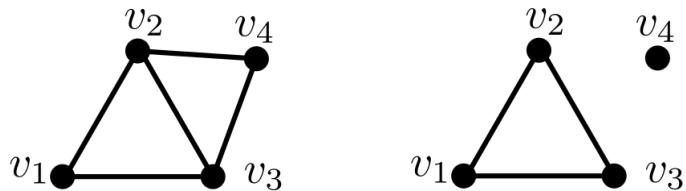


Figura A.9: A esquerda um grafo conectado e, a direita, um grafo desconectado

## Grafos Completos

Introduze-se agora uma classe especial de grafos: Um grafo é dito *Completo* se possui todas as suas arestas possíveis, i.e., para cada par de vértices distintos  $u, v \in V_G$ ,  $u$  é adjacente a  $v$  (vide Figura A.10).

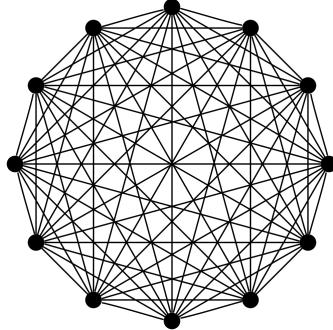


Figura A.10: Diagrama de um grafo completo com 12 vértices ( $|V| = 12$ ).

Usando combinatória, sabe-se que todo grafo completo com  $n$  vértices possui  $\binom{n}{2} = \frac{n(n-1)}{2}$  arestas.

Em particular, chama-se de  $k$ -*Clique* um subgrafo  $G'$  de  $G$ , com  $k$  vértices, tal que  $G'$  é completo, independente se seu supergrafo  $G$  é ou não completo. Por exemplo, selecionando arbitrariamente quaisquer dois vértices do grafo da Figura A.10, pode-se gerar um 2-clique induzido por estes e, caso toma-se 3 vértices, pode-se gerar um 3-clique (veja a Figura A.11).

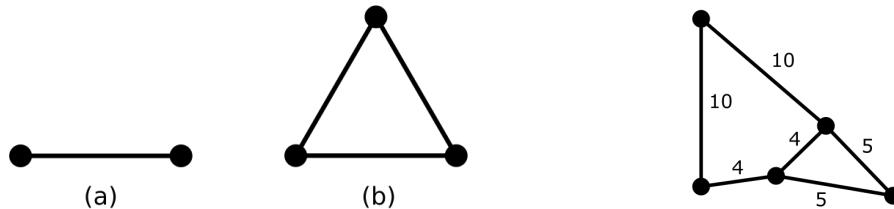


Figura A.11: (a) 2-clique e (b) 3-clique.

Figura A.12: Grafo ponderado.

## Grafos Ponderados

As arestas  $e \in E$  de um grafo  $G$  pode estar associadas com um número real  $d(e)$ , chamado de *Peso da Aresta*  $e$  (veja a Figura A.12). Quando  $G$  tem todas as suas arestas associadas com pesos, define-se  $G$  como um *Grafo Ponderado*. Grafos ponderados são frequentemente associados com aplicações em teoria de grafos [57].

Costuma-se definir uma *Função Ponderação*  $d : E \rightarrow \mathbb{R}$  para mapear o conjunto de arestas  $E$  no conjunto dos números reais  $\mathbb{R}$  [11]. Escreve-se  $G = (V_G, E_G, d)$  como um grafo ponderado ( $V_G, E_G$ ) e função ponderação  $d$ .

## Apêndice B

# Um Passeio pela Bioquímica

A bioquímica é a ciência que estuda as formas e funções biológicas em termos químicos. Já no século XVIII, os químicos percebiam a grande diferença entre o mundo inanimado e o mundo vivo: Antoine-Laurent Lavoisier (1743-1794) constatou a relativa simplicidade do “mundo mineral” — não orgânico — comparada a complexidade dos “mundos animal e vegetal” [26]. Ele sabia que esses últimos eram constituídos de moléculas ricas nos elementos carbono, oxigênio, nitrogênio e fósforo, que, devido sua abundância na natureza somada com as suas características químicas, são ótimos para constituírem a complexidade da vida.

## Carbono

A química dos organismos vivos está organizada em torno do carbono, pois este é muito comum na natureza e possui uma ótima propriedade estrutural: O carbono pode formar ligações simples estáveis com até quatro outros átomos. De fato, o carbono constitui mais da metade do peso seco das células.

Sabe-se, através de experimentos de cristalografia [28], muito sobre a geometria das ligações dos átomos de uma proteína. Em particular, as quatro ligações simples do carbono formam um tetraedro (vide Figura B.1, retirada de [26]) com ângulos de 109,5° entre duas ligações quaisquer e comprimento médio de ligação de 1,54Å<sup>1</sup>. Existe também uma outra característica muito importante para nós nas ligações do carbono: Sabe-se que as ligações simples podem rotacionar livremente (a menos que grupos muito grandes ou altamente carregados estejam ligados aos átomos de carbono, onde, neste caso — e, na verdade, esse é o caso comum —, a rotação é regida pelo equilíbrio de forças na molécula [27], que pode ser limitada), enquanto que as ligações duplas são mais curtas (em torno de 1,34Å) e não permitem rotação. Perceba também o plano formado pelos átomos A, B, X e Y na Figura B.1.

---

<sup>1</sup>Unidade física para distâncias atômicas é o Ångstron (Å), onde equivale a 1Å = 10<sup>-10</sup> m.

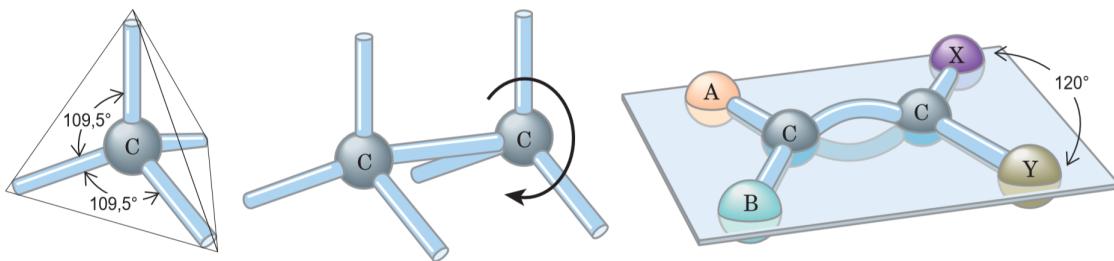


Figura B.1: Geometria da ligação do carbono.

A versatilidade das ligações covalentes do carbono podem formar cadeias lineares, ramificadas e estruturas cílicas. Nenhum outro elemento químico consegue formar moléculas com tanta diversidade de tamanhos, formas e composição.

## Classificação Macromolecular

As células contém um conjunto universal de moléculas pequenas. Mas como podemos discutir sobre o que é uma molécula pequena? Devemos definir uma forma de comparar os tamanhos moleculares. Na literatura existem duas medidas principais para esse fim, com uma relação bem definida entre si, tratam-se do *peso molecular* (ou *massa molecular relativa*), denominado  $M_r$  e da *massa molecular*, denotada simplesmente por  $m$ .

O peso molecular é definido como uma relação direta da massa da molécula da substância estudada com um duodécimo da massa do carbono-12 ( $^{12}C$ , em torno de  $1,9926 \times 10^{-23}$  gramas), note que, como  $M_r$  é uma razão, não possui dimensão associada. Já a massa molecular é apenas a massa da molécula (ou massa molar) sobre o número de Avogadro — que é definida como sendo o número de átomos por mol de uma determinada substância. Esta, diferente da massa molecular relativa, possui dimensão e é expressa em dáltons (abreviado Da) e um dálton equivale a um duodécimo da massa do carbono-12 — donde deduze-se facilmente a relação entre massa molecular e peso molecular.

Os organismos vivos são constituídos por moléculas de características muito diversas. Existe uma coleção de aproximadamente mil moléculas consideradas pequenas ( $M_r \sim 100$  a  $\sim 500$ ) diferentes dissolvidas na fase aquosa das células [26]. Nessa coleção está contido os aminoácidos comuns, nucleotídeos, açúcares e seus derivados fosforilados e ácidos mono, di e tricarboxílicos. Porém, neste estudo, estaremos mais preocupados com moléculas significativamente maiores, chamadas *macromoléculas*.

## Macromoléculas

As macromoléculas são as principais constituintes das células. São polímeros<sup>1</sup> com peso molecular acima de  $\sim 5.000$ . Polímeros menores são chamados de *oligômeros* — do grego, “oligos” significa “pouco”. Proteínas (principal molécula do nosso estudo), ácidos nucleicos (DNA, RNA) e polissacarídeos são macromoléculas feitas

<sup>1</sup>Polímeros são moléculas formadas a partir de repetições de unidades estruturais menores, chamadas *meros* ou *monômeros*. Daí o nome, poli-meros  $\approx$  vários-meros.

de monômeros cujos pesos moleculares são de 500 ou menos, porém, como apresentam um grande número dessas subunidades, possuem um alto peso molecular — até 1 milhão para proteínas e até vários bilhões para ácidos nucleicos. A síntese de macromoléculas é a atividade mais custosa energeticamente das células.

Tanto as proteínas quanto os ácidos nucleicos são polímeros lineares (isto é, que não possuem ramos ligados às suas cadeias principais, agindo como um longo fio contínuo) feitos de subunidades monoméricas bem mais simples, donde esta sequência específica de meros é que dá as informações sobre a sua estrutura tridimensional e suas funções biológicas associadas [26].

Em especial, as proteínas são constituídas por um conjunto de monômeros muito bem conhecidos e catalogados, chamados *aminoácidos*. As proteínas constituem a segunda maior fração da célula, só perdendo para a água. Provavelmente são as mais versáteis de todas as biomoléculas: Algumas têm atividade catalítica e funcionam como enzimas, outras servem como elementos estruturais, receptoras de sinais, ou transportadoras que carregam substâncias específicas para dentro ou fora das células.

## Configuração Molecular

No mundo biomolecular, toda a informação sobre uma molécula é dada pela sua estrutura (também chamada de *estereoquímica*), logo, suas ligações covalentes e seus grupos funcionais (subestruturas padrões associadas) são trivialmente importantes para definir seu bom funcionamento. Devido à característica rotacional das ligações simples do carbono, existem muitas moléculas (chamadas *estereoisômeros*) com a mesma fórmula molecular e ligações químicas, mas com diferentes configurações espaciais, o que pode mudar completamente suas funções.

De maneira simples, podemos identificar estereoisômeros pelo fato de que eles possuem as mesmas propriedades químicas, porém, não podem ser convertidos entre si sem que haja a quebra de uma ou mais ligações covalentes. Isto se dá pela presença de ligações duplas (devido à limitação na sua rotação) ou pela presença de *centros quirais*, onde a molécula rotacionada não pode corresponder à sua imagem especular (conforme Figura B.2, extraída de [26]). Um átomo de carbono com quatro ligações diferentes é considerado assimétrico e é chamado de centro quiral — do grego, *chiros* quer dizer "mão", parafraseando estas estruturas com a relação da mão direita com a esquerda. Logo, se existir um centro quiral, sempre haverá pelo menos duas possibilidades para configuração.

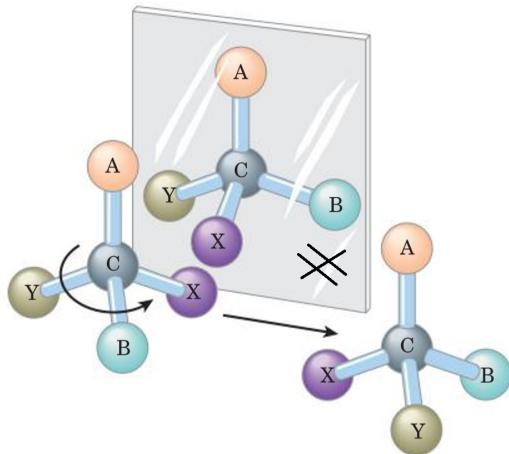


Figura B.2: Ilustração de uma molécula quiral.

Outro conceito que nos será importante no futuro, a *conformação molecular* é a disposição dos átomos no espaço que pode ser mudada por rotação em torno de ligações simples, sem quebrar ligações covalentes. Estes ângulos possíveis tem posições mais estáveis e instáveis do ponto de vista energético, conforme mostra o gráfico da Figura B.3. Podemos tentar descobrir a conformação mais provável de uma molécula minimizando a somatória de todas as forças atuantes na molécula [27].

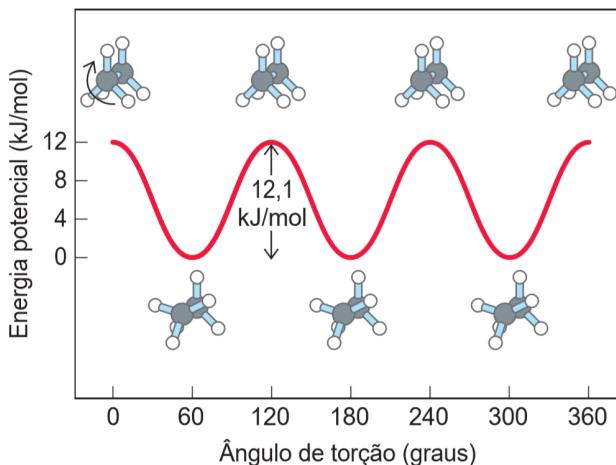


Figura B.3: Conformações e Equilíbrio de Energia [26].

Para compreender melhor como serão as configurações das moléculas que trataremos nesse texto (proteínas), vale nos preocuparmos com as subestruturas do qual eles são formados.

## Aminoácidos

As proteínas são longas cadeias lineares de aminoácidos ligados por um tipo específico de ligação (chamada *peptídica*), a qual é característica por ter como resíduo

uma molécula de água. São vinte tipos diferentes de aminoácidos encontrados normalmente na natureza, sendo esses muito bem conhecidos e catalogados. O primeiro a ser descoberto foi a asparagina, em 1806; o ultimo foi a treonina, descoberto em 1938 [26]. Vale mencionar que, além destes vinte aminoácidos mais comuns, há vários outros menos frequentes, porém não constituem as proteínas.

Destes vinte aminoácidos comuns (disponíveis no Apêndice C), dezenove compartilham da mesma estrutura principal [10] — estes são chamados  $\alpha$ -aminoácidos. Eles tem um grupo carboxílico e um grupo amina ligados ao mesmo átomo de carbono (o carbono  $\alpha$ ), além de mais um hidrogênio (chamado hidrogênio  $\alpha$ ) e, em sua última ligação, uma cadeia R que é o que diferencia cada aminoácido. Essa estrutura é ilustrada na Figura B.4. O único aminoácido que difere disso é a Prolina, que possui como cadeia R um anel aromático que se fecha no nitrogênio (que no padrão mencionado há um grupo amina).

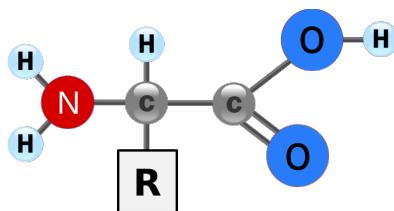


Figura B.4: Estrutura padrão de um  $\alpha$ -aminoácido.

Portanto, há uma noção prévia de qual tipo de estrutura esperar ao analisar uma molécula de proteína. Existe uma estrutura conhecida e repetitiva para os átomos.

Para todos os aminoácidos comuns, exceto a glicina, o carbono  $\alpha$  está ligado com quatro outros átomos diferentes entre si (na glicina temos R como apenas mais um hidrogênio, sendo o aminoácido mais simples), o que transforma o carbono  $\alpha$  em um centro quiral. Logo, cada aminoácido (menos glicina) tem sempre dois estereoisômeros possíveis. Porém, na verdade, apenas um destes ocorre naturalmente nas proteínas [26].

## Ligaçāo Peptídica

A ligação entre dois aminoácidos é feita de modo covalente por meio de desidratação do grupo  $\alpha$ -carboxílico de um com o grupo  $\alpha$ -amina do outro — ou seja, ligar o carbono final de um no nitrogênio inicial do outro, liberando um oxigênio e dois hidrogênios, que formam uma molécula de água. Essa ligação, também chamada de resíduo (devido a liberação da água), forma um dipeptídeo.

Quando muitos aminoácidos se juntam, o produto é chamado de polipeptídeo. Perceba que os termos “polipeptídeo” e “proteína” parecem dirigir-se as mesmas moléculas, porém, a diferença está na massa molecular: As moléculas com massa abaixo de 10.000 são ditas polipeptídeos, enquanto as maiores que essas são consideradas proteínas. Os comprimentos dessas cadeias variam significativamente. O citocromo c humano tem apenas 104 aminoácidos, enquanto, no outro extremo, a titina (relacionada ao músculo de vertebrados) possui aproximadamente 27.000 aminoácidos e uma massa molecular de cerca de 3.000.000. No geral, as proteínas naturais contém menos de 2.000 aminoácidos [26].

Outra característica muito importante das ligações peptídicas é de que elas se comportam semelhantemente a ligações covalentes duplas dos carbonos. Estudos envolvendo difração de raios X em cristais de aminoácidos e polipeptídeos descobriram que a ligação peptídica  $C - N$  é de alguma forma mais curta que a ligação de uma amina simples, e que os átomos associados a ligação peptídica estão todos co-planares (conforme Figura B.5). Perceba que também são rígidos, não sendo possível a rotação. Essa é uma propriedade muito útil que também nos será importante, descoberta de 1930 que se deve a Linus Pauling e Robert Corey.

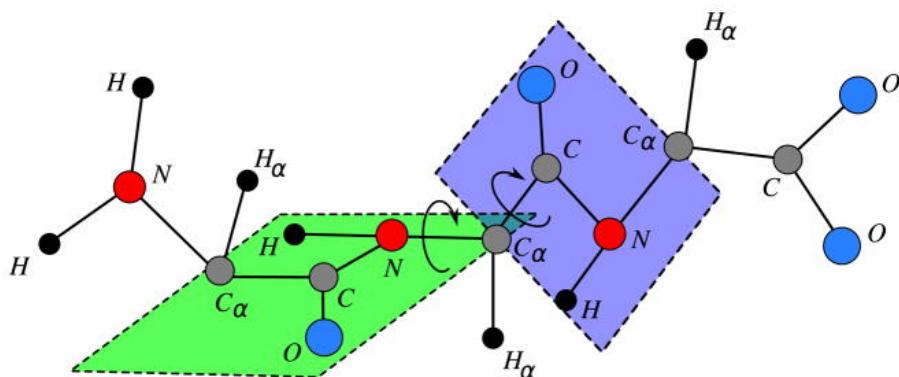


Figura B.5: O grupo peptídico planar [47].

## Estrutura das Proteínas

A estrutura de proteínas pode ser descrita em quatro níveis de importante hierarquia conceitual, conforme pode ser visto na Figura B.6, retirado de [26]. A estrutura primária consiste da mais detalhada, sendo de fato os polímeros de aminoácidos; Estes, por sua vez, formam alguns arranjos particularmente estáveis, que dão origem a padrões estruturais recorrentes, que chamamos de *estruturas secundárias* (como as hélices  $\alpha$ , as duplas hélices etc.). A estrutura terciária descreve todos os aspectos do enovelamento tridimensional de um polipeptídeo, ou seja, define quais serão as forças atuantes na molécula — que da origem a sua conformação estável, que minimiza a energia livre de Gibbs do sistema. Quando existem mais estruturas terciárias em uma proteína, chamamos a junção destas de estrutura quaternária.

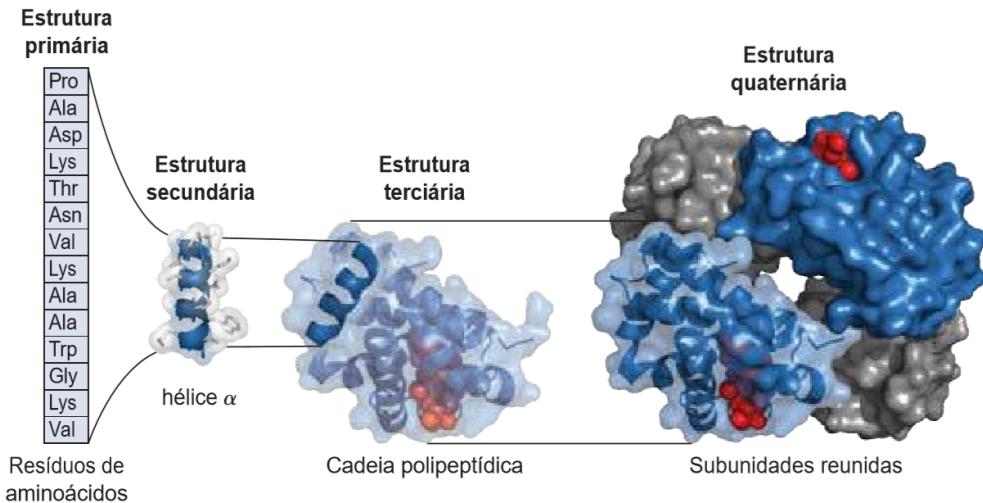


Figura B.6: Níveis de estrutura das proteínas exemplificados na Hemoglobina.

Em especial, as diferentes configurações da estrutura primária — que pode mudar drasticamente entre estruturas primárias diferentes na mesma molécula — nos é mais informativa. A estrutura primária de uma proteína determina como ela se dobra em sua estrutura tridimensional, devido os ângulos e distâncias bem definidos de suas ligações entre átomos, que da a sua estrutura especial; o que, por sua vez, determina a função da proteína — como no exemplo da Figura B.6, onde a estrutura da hemoglobina é que permite que átomos de oxigênio “encaixem” nela, possibilitando o transporte desse átomo pelo organismo, que é sua função (e só o é dado sua estrutura tridimensional).

Por sua relação com a estrutura tridimensional e, logo, função das proteínas, vamos nos concentrar em estudar a subdivisão de estruturas primárias.

## A Cadeia Principal de uma Proteína

Quando se estuda proteínas a nível dos aminoácidos, não tardamos a perceber que elas possuem uma estrutura repetida muito interessante do ponto de vista bioquímico. Trata-se da *cadeia principal* de uma proteína, também chamada de *Backbone* — espinha dorsal, em tradução literal, fazendo alusão a importância desta estrutura. Perceba que os vinte aminoácidos que compõem as proteínas possuem sempre os mesmos três átomos ligados em sequência (Figura B.7):  $N - C_{\alpha} - C$ , através de ligações covalentes em torno do  $C_{\alpha}$  e da ligação peptídica  $C - N$  entre aminoácidos.

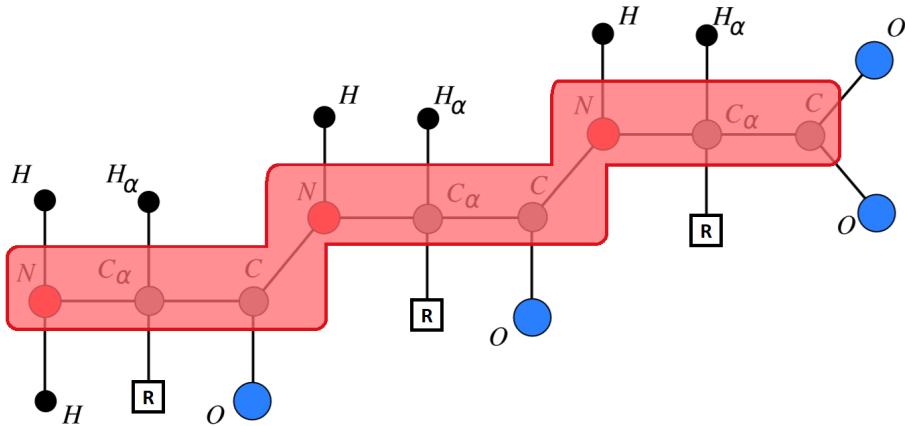


Figura B.7: Representação da cadeia principal da proteína, adaptada de [47]

Outra informação bastante útil sobre esta cadeia principal é que, devido dados experimentais de cristalografia, sabe-se sobre a geometria média dessa subestrutura [28], onde os comprimentos e ângulos entre as ligações dos átomos que a formam são fixas, na média, a menos de erros de medida. Vide Figura B.8, extraída do texto original de Ramachandran *et al.*, um dos precursores deste estudo.

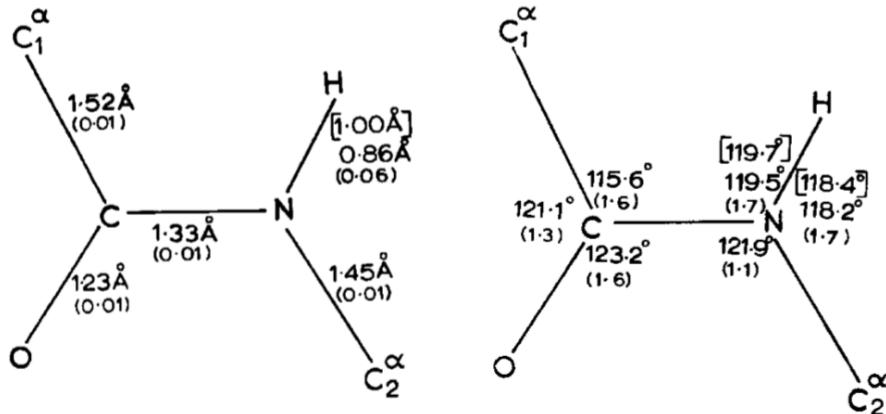


Figura B.8: Dados de ângulos e distâncias médios de ligações em um aminoácido.

## Worldwide Protein Data Bank

Já foi possível perceber a grande variedade de diferentes configurações possíveis para as proteínas. Com isso, há a necessidade de se estudar cada uma explicitamente, através de experimentos, catalogando e guardando essas informações. Esse grande esforço para entender o mundo das macromoléculas se deixa transparecer com o repositório *Worldwide Protein Data Bank* — ou simplesmente wwPDB [58].

Este é um repositório online e público onde estão guardadas todas os dados de proteínas e ácidos nucleicos já catalogados, em especial dados de suas estruturas 3D (posições x, y e z de cada um dos átomos que a constituem). Auxiliando tanto pesquisadores, quanto professores e estudantes, essa base de dados é um grande

esforço em conjunto de físicos, biólogos, bioquímicos e vários outros profissionais de diversas áreas do conhecimento de todo o mundo.

## Arquivo PDB

Quando se quer estudar uma proteína no repositório PDB, base fazer o *download* do arquivo PDB da molécula (extensão “.ent”). Esse é um arquivo de estruturas tridimensionais de macromoléculas biológicas determinadas experimentalmente, que descrevem as coordenadas espaciais de cada átomo cuja posição foi determinada (muitas das estruturas catalogadas não estão completas); também existem dados adicionais sobre informações de como as estruturas foram determinadas, os dados práticos dos experimentos, a precisão associada aos dados e tudo mais que quem estiver criando o documento achar necessário para aquela macromolécula.

Tecnicamente, o arquivo PDB trata-se de uma representação estruturada dos dados moleculares e experimentais da proteína. Ele é separado por seções, onde cada seção pode possuir subseções. São elas:

- **Seção Title** - Contem a descrição da molécula;
- **Seção Remark** - Vários comentários sobre anotações de entrada com mais profundidade que os registros padrões;
- **Seção Primary structure** - Sequências peptídicas ou nucleotídicas especificadas para serem posteriormente utilizadas, diminuindo a repetição do arquivo;
- **Seção Heterogen** - Descrição de grupos presentes não padronizados — Visto que proteínas também podem conter materiais inorgânicos, como o ferro presente na hemoglobina (vide Figura B.6);
- **Seção Secondary structure** - Descrição das estruturas secundárias presentes na molécula;
- **Seção Connectivity annotation** - Descrição das conectividade químicas da molécula;
- **Seção Miscellaneous features** - Descrição dos recursos dentro da macromolécula;
- **Seção Crystallographic** - Descrição de parâmetros da cristalografia, quando o experimento utiliza esta metodologia;
- **Seção Coordinate transformation** - Matrizes como operadores de transformação das coordenadas;
- **Seção Coordinate** - Dados de coordenadas atômicas, a seção que mais vamos utilizar;
- **Seção Connectivity** - Citação das conexões químicas entre os átomos;
- **Seção Bookkeeping** - Resumo das características totais do arquivo e o marcador de fim de arquivo.

Como o arquivo é significativamente extenso, não entraremos em detalhes neste texto sobre as características detalhadas de cada uma das seções apresentadas. No entanto, vale mencionar o tipo de entrada ATOM, presente na seção Coordinate, pois essa é a entrada que compõe a maior parte dos arquivos PDB, além de ser a de nosso interesse principal.

A entrada ATOM tem como objetivo descrever detalhes de cada átomo específico da molécula. Ela segue um padrão indentado, onde cada dado é caracterizado pela

Código serial do átomo	7-11
Nome do átomo	13-16
Nome do resíduo que pertence	18-20
Identificador da cadeia	22
Código serial de dentro do resíduo	23-26
Coordenada x	31-38
Coordenada y	39-46
Coordenada z	47-54
<i>Occupancy</i> do átomo	55-60
Fator de temperatura	61-66
Símbolo do elemento	77-78

Tabela B.1: Principais dados da entrada ATOM.

sua posição na linha (coluna). Segue principais dados da entrada e suas respectivas colunas na Tabela B.1.

Segue exemplo de um conjunto de entradas do tipo ATOM na Figura B.9.

1	2	3	4	5	6	7	8		
12345678901234567890123456789012345678901234567890123456789012345678901234567890									
ATOM	1	N	MET A	1	-10.885	6.773	13.357	1.00 0.00	N
ATOM	2	CA	MET A	1	-12.318	6.914	13.685	1.00 0.00	C
ATOM	3	C	MET A	1	-13.195	6.440	12.525	1.00 0.00	C
ATOM	4	O	MET A	1	-12.738	6.392	11.383	1.00 0.00	O
ATOM	5	CB	MET A	1	-12.654	8.361	14.078	1.00 0.00	C
ATOM	6	CG	MET A	1	-12.548	9.328	12.889	1.00 0.00	C

Figura B.9: Conjunto de entradas do tipo ATOM.

Com esse conjunto de dados, pode-se, por exemplo, esboçar uma representação gráfica de uma molécula. Existem muitos softwares compatíveis com os arquivos PDB para este fim, por exemplo, o autor deste documento implementou uma visualização de uma projeção da molécula 3D no plano  $z = 0$ , como pode-se averiguar na Figura B.10.

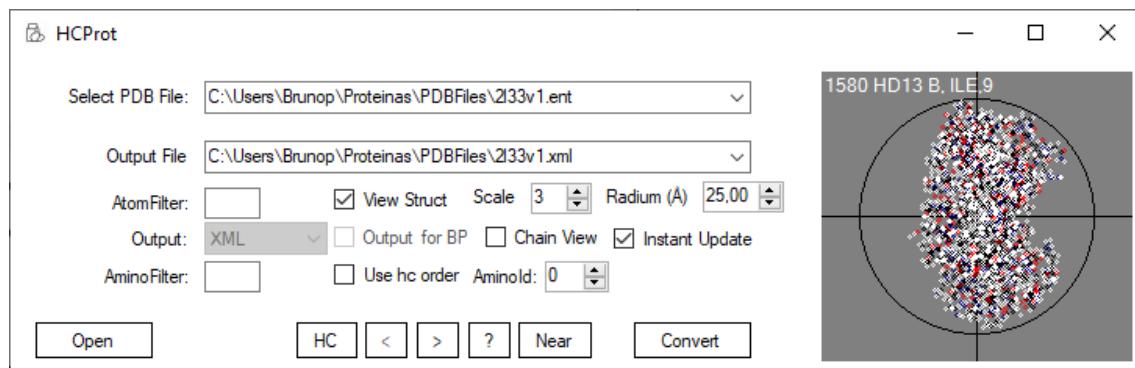


Figura B.10: HCProt com visualização a partir de um aquivo PDB.

# Apêndice C

## Vinte Aminoácidos Naturais

É comum dividirmos os aminoácidos proteicos em cinco classes, como segue.

### Grupos R apolares, alifáticos

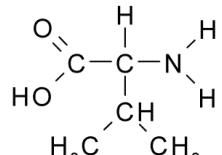
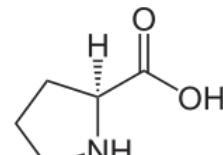
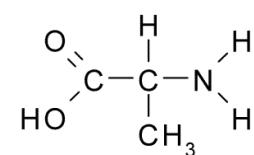
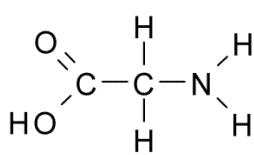


Figura C.1: Glicina Figura C.2: Alanina Figura C.3: Prolina Figura C.4: Valina

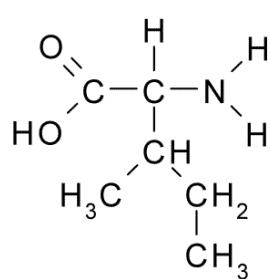
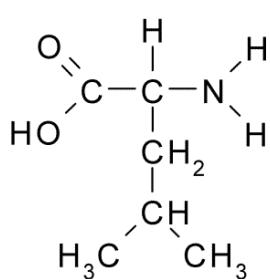
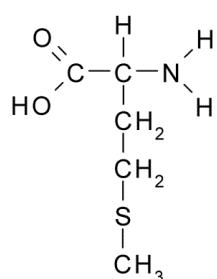


Figura C.5: Metionina

Figura C.6: Leucina

Figura C.7: Isoleucina

### Grupos R polares, não carregados

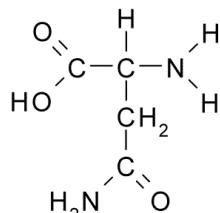
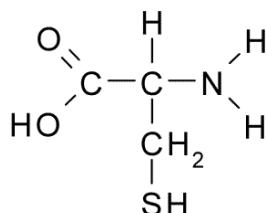


Figura C.8: Cisteína

Figura C.9: Asparagina

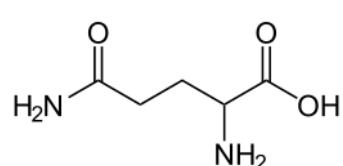


Figura C.10: Glutamina

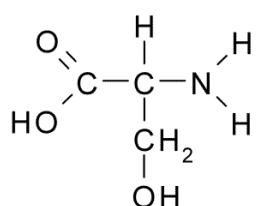


Figura C.11: Serina

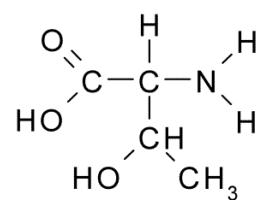


Figura C.12: Treonina

### Grupos R aromáticos

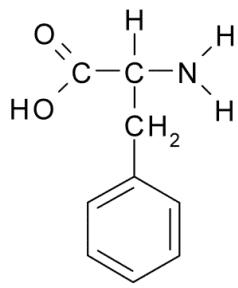


Figura C.13: Fenilalanina

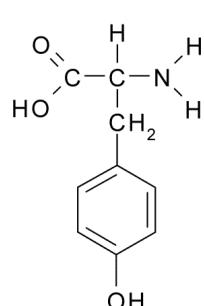


Figura C.14: Tirosina

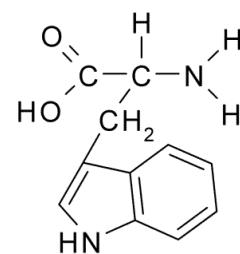


Figura C.15: Triptofano

### Grupos R carregados positivamente

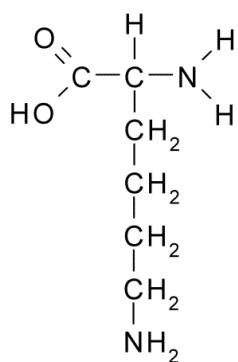


Figura C.16: Lisina

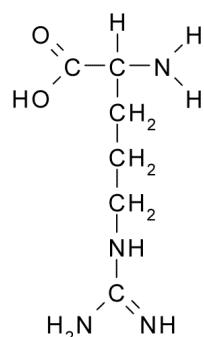


Figura C.17: Arginina

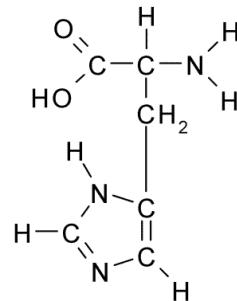


Figura C.18: Histidina

**Grupos R carregados negativamente**

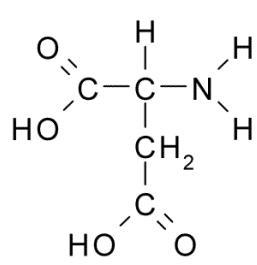


Figura C.19: Aspartato

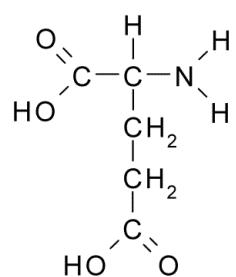


Figura C.20: Glutamato