Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Grupos de Isometrias

por

Luis Filipe Ramos Campos da Silva

sob orientação de

Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB
2021

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Luis Filipe Ramos Campos da Silva

Grupos de Isometrias

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em Matemática.

Orientador: Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB
2021

Grupos de Isometrias

Luis Filipe Ramos Campos da Silva

Trabalho de conclusão de curso defendido e aprovado em 12 de fevereiro de 2021, pela Comissão Examinadora constituída pelos examinadores:

Prof. Dr. Antônio Pereira Brandão Júnior
Orientador

Prof. Dr. Daniel Cordeiro de Morais Filho
Examinador

Prof. Dr. Claudemir Fidelis Bezerra Júnior
Examinador

Nota: _____.

Dedicatória

Dedico esse trabalho a minha família, em especial a minha avó Edorice Ramos (in memoriam), a minha namorada e a todos que me apoiaram durante a graduação.

Agradecimentos

Agradeço a Deus pela minha saúde e por ter me ajudado em todos os momentos difíceis que passei ao longo desta graduação.

Sou grato aos meus pais, Luis Rangel e Jâmise Ramos, pois sempre me apoiaram e me incentivaram nos momentos difíceis. Quero dizer que amo vocês.

Agradeço aos meus irmãos, Luis Henrique e Jamille Ramos, pois sempre me ajudaram e sempre estiveram presentes nos melhores momentos da minha vida.

Sou grato a minha namorada, Ana Thayse, que me incentivou e me apoiou nos momentos em que mais precisei e que compreendeu, na maioria das vezes, a minha ausência enquanto eu me dedicava aos estudos.

Agradeço a todas as pessoas da minha família: avós, tios e primos que sempre me incentivaram. Em especial, sou muito grato a minha avó, Edorice Ramos, que me fez crescer como pessoa e foi a pessoa que mais me apoiou em toda minha vida. Também agradeço ao meu tio, Jamilson Ramos, que além de amigo sempre me incentivou, esteve presente e me deu suporte a partir do momento que decidi cursar Matemática.

Serei eternamente grato ao professor Daniel Cordeiro, que sempre se mostrou disponível, sempre me incentivou e me ajudou quando passei por momentos difíceis durante a graduação, me passou muito conhecimento, experiência e acabou se tornando um amigo. Certamente não acabaria o curso bem, se não fosse por ele. Muito obrigado por me apresentar o PET-Matemática-UFCG, o senhor será meu eterno tutor.

Agradeço ao meu orientador, Antônio Brandão, que me acompanha desde quando entrei na graduação por causa da iniciação científica. Agradeço também por ter me passado todo o conhecimento que o senhor passou e pela paciência que o senhor teve comigo quando cheguei, pois não tinha experiência e sempre fui bem tratado. Muito obrigado por tudo.

Agradeço a todos os integrantes e petianos egressos do PET-Matemática-UFCG que pude conviver diariamente, pois foi com vocês que dividi momentos difíceis na graduação mas também compartilhei momentos felizes. Todos vocês já fizeram algo por mim em algum momento. Sou grato também a todos meus colegas de turma durante o curso, esses também já me ajudaram bastante.

Em especial, agradeço a Ismael Sandro, Rodrigo Marques e Lucas Siebra por serem tão presentes como amigos e por todas as dúvidas tiradas durante a graduação. Agradeço também a Fábio Lima e José Marcos, pois sempre

me ajudaram quando pagamos disciplinas juntos e se tornaram meus amigos. Sou grato também a Leticia e Otacilia, pois pagamos muitas cadeiras juntos, me ajudaram bastante e se tornaram amigas. Agradeço ao casal Lucas Silva e Daniela Enéas pela amizade e por estarem sempre presentes no meu cotidiano na universidade.

Agradeço também a todas as pessoas da Pós-Graduação com quem tive contato e já me ajudaram em algum momento. Em especial, sou muito grato a Pedro Fellype e a Geisa Gama, que além de amigos sempre estavam disponíveis para me ajudar nas disciplinas que paguei e dispostos a rir por besteira.

Agradeço ao professor, Claudemir Fideles, por ter aceito participar da banca avaliativa deste trabalho e por ter repassado o seu conhecimento quando tive oportunidade de ser seu aluno em uma disciplina da graduação.

Por fim, sou muito grato a todos os professores da UAMat que contribuíram para minha formação acadêmica e sempre estiveram disponíveis quando precisei. Agradeço também a todos os coordenadores que já tive durante a graduação e funcionários da UAMat, por sempre estarem disponíveis, agradeço a Claudiana Albuquerque(Aninha), pela amizade e por sempre me ajudar quando precisei.

Resumo

Uma isometria num espaço métrico M é uma aplicação bijetora de M em M que preserva distâncias. Sabe-se que o conjunto das isometrias de um espaço métrico qualquer M, munido da composição de funções, é um grupo. No presente trabalho será feito um estudo sobre grupos de isometrias, onde veremos algumas propriedades básicas e exemplos. Ademais, mostraremos que no caso em que um grupo G é finito de ordem n, existe um subconjunto finito W do $\mathbb{R}^n$ tal que o grupo de isometrias de W é isomorfo a G. Por fim, será feito um estudo sobre isometrias de espaços vetoriais reais normados, no qual o principal resultado apresentado será o Teorema de Mazur-Ulam, o qual fornece uma condição para que uma isometria seja uma transformação linear.

Abstract

An isometry on a metric space M is a bijection from M to M that preserves distances. It is well-known that a set of isometries of any metric space M, equipped with the composition of functions, is a group. In the present work a study about isometries groups will be done, in which we will see some basic properties and examples. Furthermore, we will prove that in the case wherein a group G is finite of order n, there is a finite subset W of $\mathbb{R}^n$ such that the group of isometries of W is isomorphic to G. Ultimately, a study about real normed vector spaces will be done in which the main result presented will be the Mazur-Ulam Theorem, which provides a condition in order for a isometry to be a linear mapping.

Sumário

Introdução

Quando estudamos Álgebra Abstrata e iniciamos o estudo sobre estruturas algébricas, ou seja, iniciamos um estudo sobre conjuntos dotados de uma ou mais operações binárias, temos como uma das principais estruturas algébricas a estrutura de Grupo. Um Grupo é um conjunto não vazio munido de uma operação que é associativa, possui elemento neutro e todo elemento desse conjunto possui um inverso.

Na Teoria de Grupos, nos deparamos com vários exemplos clássicos como: o conjunto dos números inteiros munido da adição usual, assim como o conjunto dos números reais munido da adição usual e o conjunto das matrizes quadradas, com entradas reais, que possuem determinante diferente de zero munido da multiplicação usual de matrizes. A medida que nos familiarizamos com estes e diversos outros exemplos de Grupos, fica evidente que os elementos de um grupo podem ser de qualquer natureza, inclusive funções. O que iremos enfocar neste trabalho é que, ainda mais do que funções, os elementos de um Grupo também podem ser isometrias.

Em todo o trabalho, estaremos utilizando conceitos e propriedades básicas de Álgebra Linear como por exemplo: espaços vetoriais, produto interno, transformações lineares, caso o leitor queira rever estes conceitos, assim como ver resultados aqui não demonstrados, recomendamos as referências [4] e [9].

Inicialmente, faremos um capítulo com alguns conceitos prévios que serão importantes para o entendimento dos capítulos subsequentes. Neste primeiro capítulo, estudaremos as definições e propriedades básicas de Grupos, Subgrupos, Homomorfismos de Grupos, Produto Semidireto, Espaços Métricos e Isometrias. Além disso, com o intuito de proporcionar um melhor entendimento ao leitor, ainda no primeiro capítulo, discutiremos um pouco sobre aplicações contínuas, sequências em um espaço métrico qualquer e enunciaremos o Teorema da Função Implícita, para esse momento, caso o leitor esteja interessado em maiores detalhes, recomendamos as referências [3],[8] e [11].

Uma *isometria* num espaço métrico M é uma aplicação bijetora de M em M que preserva distâncias. Mostraremos no segundo capítulo que de fato o conjunto $Isom(M)$, conjunto das aplicações de M em M que são isometrias,

munido da composição de funções, é um grupo: *o grupo das isometrias do espaço métrico* M. O estudo sobre Grupos de Isometrias, motivo da escolha do título deste trabalho, será feito a partir deste capítulo, onde serão vistos a definição e vários exemplos interessantes de Grupos de Isometrias. Ademais, será mostrado que se G é um grupo finito de ordem n, então G é isomorfo a um subgrupo de $Isom(\mathbb{R}^n)$ e existe algum subconjunto finito W de $\mathbb{R}^n$ tal que $Isom(W)$ é isomorfo a G. Para isso, utilizaremos as ideias do artigo [1]. Recomendamos também ao leitor interessado, a leitura do artigo [2], o qual também mostra a realização de grupos finitos como grupos de isometrias.

No terceiro e último capítulo, mencionaremos as isometrias de Espaços Vetoriais Reais Normados. Sendo assim, veremos o conjunto das translações como um subgrupo do grupo das isometrias de um espaço vetorial real E. Falaremos um pouco também sobre as isometrias lineares da reta e sobre as isometrias lineares do plano. No caso das isometrias lineares do plano, mostraremos que, com a norma euclidiana, o grupo das isometrias lineares do plano é isomorfo ao grupo ortogonal de grau 2, mas se mudarmos a norma, passando a considerar a norma da soma, o grupo das isometrias será isomorfo ao grupo D_4 (o grupo diedral 4). Além disso, provaremos que se V é um espaço vetorial com produto interno e $T : V \longrightarrow V$ é uma isometria tal que $T(0) = 0$, então T é uma transformação linear. Apresentaremos ainda uma generalização desse resultado que é o Teorema de Mazur-Ulam, onde substituímos a hipótese de espaço vetorial com produto interno, pela hipótese mais fraca de espaço vetorial normado. A demonstração desse resultado é belíssima, pois temos que utilizar outros artifícios interessantes para contornar a ausência da hipótese de produto interno. Por fim, veremos que, através do Teorema de Mazur-Ulam, podemos enxergar um grupo de isometrias como um produto semidireto de grupos.

Capítulo 1

Resultados Prévios

Neste primeiro capítulo serão apresentados alguns conceitos e resultados de Álgebra Abstrata. Para maiores detalhes dos resultados de Álgebra Abstrata apresentados, assim como para acesso a mais exemplos, indicamos [5], [6], [7] e [12].

Além das referências supracitadas, sugerimos as referências [4] e [9], uma vez que utilizaremos não somente neste capítulo, mas em todo o texto, os conceitos e propriedades básicas de produto interno, de transformação linear e de espaços vetoriais.

Além disso, como também falaremos um pouco neste capítulo sobre diferenciabilidade, sobre o Teorema da Função Implícita e sobre topologia do $\mathbb{R}^n$ indicamos as referências [3] e [11].

Por fim, para os resultados e exemplos envolvendo espaços métricos e isometrias, recomendamos [8].

1.1 Grupos e subgrupos

1.1.1 Grupos

Definição 1.1. Sejam G um conjunto não vazio e $* : G \times G \longrightarrow G$ uma operação binária. Dizemos que o par $(G, *)$ é um *grupo* se são satisfeitas:

i) A associatividade da operação $*$, isto é, $x * (y * z) = (x * y) * z$, para quaisquer $x, y, z \in G$;

ii) Existe elemento neutro para $*$, ou seja, existe $e \in G$ tal que $x * e = e * x = x$, para todo $x \in G$;

iii) Para todo $x \in G$, existe um inverso (ou simétrico) $y \in G$, ou seja, $x * y = y * x = e$.

Denotaremos $(G, *)$ simplesmente por G, quando não houver dúvida quanto à operação considerada sobre G. Em um grupo G qualquer é padrão verificar que o elemento neutro é único, assim como o inverso de cada elemento de G. Para maiores detalhes ver *seção 3.4* da referência [12].

Definição 1.2. Um grupo é *comutativo* ou *abeliano* quando

$$x * y = y * x, \forall\, x, y \in G,$$

ou seja, quando a operação em G é comutativa.

Definição 1.3. Se G é um grupo com uma quantidade finita n de elementos, dizemos que G tem *ordem* n, e denotamos por $|G| = n$. Caso G seja infinito, dizemos que G tem *ordem infinita*, e denotamos $|G| = \infty$.

Usaremos as seguintes notações no decorrer do texto:

(I) **Notação aditiva:** usando essa notação, a operação do grupo é denotada por $+$, o elemento neutro é denotado por 0 e o inverso de x é denotado por $-x$.

(II) **Notação multiplicativa:** nessa notação, a operação do grupo é denotada pela justaposição de termos, ou seja, $x * y := xy$. O elemento neutro é denotado por 1 ou e, e o inverso de x é denotado por x^{-1}.

Observação 1.4. *Seja G um grupo. Então, valem as seguintes propriedades:*

(i) Leis do corte, isto é, se $a, x, y \in G$ são tais que $xa = ya$, então $x = y$; e também, se $ax = ay$, então $x = y$.

(ii) Sendo $x, y \in G$, temos $(xy)^{-1} = y^{-1}x^{-1}$. Essa ideia pode ser generalizada para mostrar que se $x_1, x_2, ..., x_n \in G$, então

$$(x_1 x_2 \cdots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1}.$$

As demonstrações dessas propriedades estão feitas na seção 3.4 da referência [12].

Exemplo 1.5. *O conjunto unitário $\{e\}$ é um grupo, munido da única operação binária que pode ser definida nele.*

Exemplo 1.6. *Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, munidos das adições usuais, são exemplos clássicos de grupos aditivos abelianos. Porém, não são grupos munidos da multiplicação usual, pois 0 não possui inverso multiplicativo. Os conjuntos $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, que são respectivamente os conjuntos $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ sem o zero, são grupos, munidos da multiplicação usual.*

Exemplo 1.7. *Seja $G = \{e, a, b, c\}$ munido da operação:*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

O par $(G, *)$ é um grupo, chamado ***grupo de Klein****.*

Exemplo 1.8. *Seja X um conjunto não vazio. Defina S_X como o conjunto de todas as funções $f : X \longrightarrow X$ bijetoras. Esse conjunto, munido da operação de composição de funções, é um grupo, chamado* ***grupo das permutações de*** *X. Em tal grupo, o elemento neutro é a aplicação Id_X, tal que $Id_X(x) = x$, para todo $x \in X$. Caso $X = \{1, 2, ..., n\}$, denotamos S_X por S_n e denominamos este grupo de* ***grupo simétrico de grau n****. Os grupos S_n, para $n \geq 3$, são não abelianos. Mostra-se que $|S_n| = n!$. Representamos uma permutação $\alpha \in S_n$ da seguinte forma:*

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix}.$$

Nesta notação, não importa a ordem das colunas. Dessa forma,

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix} = \begin{pmatrix} 2 & 1 & ... & n \\ \alpha(2) & \alpha(1) & ... & \alpha(n) \end{pmatrix}.$$

Exemplo 1.9. *Sejam G_1 e G_2 grupos. O conjunto $G_1 \times G_2$, munido da operação*

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2),$$

é um grupo, chamado ***produto direto (externo)*** *de G_1 por G_2. Se $|G_1| = n$ e $|G_2| = m$, então $|G_1 \times G_2| = mn$.*

O produto direto pode ser generalizado para n grupos. Dessa forma, se tivermos $G_1, G_2, ..., G_n$ grupos, o conjunto $G_1 \times G_2 \times \cdots \times G_n$, munido da operação

$$(x_1, x_2, ..., x_n)(y_1, y_2, ..., y_n) = (x_1y_1, x_2y_2, ..., x_ny_n)$$

é um grupo, chamado produto direto externo de G_1, ..., G_n.

Exemplo 1.10. *Sendo G um grupo abeliano, considere o conjunto $DG = G \times \{1, -1\}$ e a operação $*$ em DG definida por*

$$(a, n) * (b, m) = (ab^n, nm).$$

Mostra-se que DG, munido desta operação, é um grupo, cujo elemento neutro é $(e, 1)$, onde e denota o elemento neutro de G. Observe que se $(a, n) \in DG$, então $(a, n)^{-1} = (a^{-n}, n)$.

Exemplo 1.11. *Considere $(E, +, \cdot)$ um espaço vetorial, onde "+" é a adição de vetores e " $\cdot$ " é a multiplicação por escalar. Observe que E_+, que é o conjunto E munido apenas da operação de adição de vetores, é um exemplo de grupo aditivo abeliano, pois pela própria definição de espaço vetorial, a operação adição é associativa, possui um único elemento neutro (vetor nulo), para cada vetor $v \in E$ existe um único vetor $-v \in E$ (chamado o inverso aditivo) tal que $-v + v = 0_E$, e além disso a operação adição é comutativa. Denotaremos 0_E como sendo o elemento neutro do grupo aditivo E_+.*

Definição 1.12. Sejam $a, x \in G$, onde G é um grupo. Definimos o *conjugado de a por x*, denotado por a^x, como sendo o elemento $xax^{-1} \in G$.

Definição 1.13. Sejam G um grupo, $x \in G$ e $n \in \mathbb{Z}$. Definimos

$$x^n = \begin{cases} e & , \text{se } n = 0. \\ \underbrace{xx \cdots x}_{n \text{ vezes}} & , \text{se } n > 0. \\ (x^{-1})^{|n|} & , \text{se } n < 0. \end{cases}$$

E em notação aditiva:

$$nx = \begin{cases} 0 & , \text{se } n = 0. \\ \underbrace{x + x + ... + x}_{n \text{ vezes}} & , \text{se } n > 0. \\ |n|(-x) & , \text{se } n < 0. \end{cases}$$

Observação 1.14. *Sejam G um grupo, $x \in G$ e $n, m \in \mathbb{Z}$. Seguem abaixo algumas propriedades que provêm da definição acima. São elas:*

(i) $(x^n)^m = x^{nm}$;

(ii) $x^{n+m} = x^n x^m$;

(iii) $(x^{-1})^n = (x^n)^{-1} = x^{-n}$.

As demonstrações dessas propriedades estão na seção 3.4 da referência [12].

1.1.2 Subgrupos

Definição 1.15. Seja G um grupo. Um subconjunto $H \subseteq G$ não vazio é dito um *subgrupo* de G, e denotado por $H \leq G$, se valem:

(i) $xy \in H$;

(ii) $x^{-1} \in H$;

para quaisquer $x, y \in H$.

Observação 1.16. *Podemos definir um subgrupo de G como um subconjunto $H \subseteq G$ não vazio tal que vale*

(i') $xy^{-1} \in H$, para quaisquer $x, y \in H$.

Essa definição é equivalente à dada anteriormente.

Observação 1.17. *Sejam G um grupo e H um subgrupo de G. Então,*

1) $e \in H$ e H é por si um grupo, cuja operação é a mesma de G.

2) O elemento neutro de H é igual ao elemento neutro de G.

3) Dado $h \in H$, o inverso de h em H coincide com o inverso de h em G.

A verificação da Observação 1.17 pode ser encontrada na seção 3.8 da referência [12].

Exemplo 1.18. *Seja G um grupo. Os conjuntos $\{e\}$ e G são subgrupos de G, chamados subgrupos triviais.*

Exemplo 1.19. *Se G é um grupo e $x \in G$, então o conjunto $\langle x \rangle = \{x^n; n \in \mathbb{Z}\}$ (em notação aditiva, $\langle x \rangle = \{nx; n \in \mathbb{Z}\}$) é um subgrupo, chamado **subgrupo gerado por** x. Dizemos que um grupo G é **cíclico** se existe $x \in G$ tal que $G = \langle x \rangle$.*

Definição 1.20. Sejam G um grupo e $x \in G$. Se existe $n \in \mathbb{N}$ tal que $x^n = e$, dizemos que x tem *ordem finita*, e definimos a *ordem de x*, denotada por $\circ(x)$, como

$$\circ(x) = \min\{n \in \mathbb{N}; x^n = e\}.$$

Caso não exista $n \in \mathbb{N}$ tal que $x^n = e$, dizemos que x tem *ordem infinta*, e denotamos $\circ(x) = \infty$.

Proposição 1.21. *Sejam G um grupo, $x \in G$ um elemento de ordem finita e $m \in \mathbb{Z}$. Nessas condições, temos:*

(i) $x^m = e$ se, e somente se, $\circ(x)$ divide m;

(ii) $|\langle x \rangle| = \circ(x)$.

Demonstração. (i) Sejam $\circ(x) = n$ e $m \in \mathbb{Z}$. Pelo Algorítmo da Divisão, existem $q, r \in \mathbb{Z}$, com $0 \leq r < n$ tais que $m = nq + r$. Assim, temos:

$$x^m = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = x^r$$

de onde $x^m = e$ se, e somente se, $x^r = e$. Como $r < n$, pela definição de $\circ(x)$, vale $x^r = e$ se, e somente se, $r = 0$, ou seja, $m = qn$. Concluímos então que $x^m = e$ se, e somente se, $\circ(x) = n$ divide m.

(ii) Como x é um elemento de ordem finita, digamos $\circ(x) = n$, então os elementos $e, x, x^2, \ldots, x^{n-1}$ são todos distintos. De fato, suponha que $x^i = x^j$ para $0 \leq i < j \leq n-1$, então $x^{j-i} = e$ com $0 < j - i < n$, o que é um absurdo, visto que $\circ(x) = n$. Observe também que para cada $k \in \mathbb{Z}$ tem-se $k = nq + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < n$. Logo, como $\circ(x) = n$, temos

$$x^k = x^{nq+r} = x^{nq}x^r = x^r.$$

Daí,

$$\langle x \rangle = \{x^k; k \in \mathbb{Z}\} = \{x^r; r = 0, 1, ..., n-1\}$$

tem ordem n.

Suponhamos agora que $\langle x \rangle$ tem ordem finita. Logo, as potências x^i, com $i \in \mathbb{Z}$, não podem ser todas distintas. Assim, existem $i, j \in \mathbb{Z}$, com $i < j$, de maneira que $x^j = x^i$, ou seja, $x^{j-i} = e$. Portanto, x tem ordem finita, digamos $\circ(x) = n$. Daí, os elementos $e, x, x^2, \ldots, x^{n-1}$ são todos distintos. Dessa forma,

$$\langle x \rangle = \{x^r; r = 0, 1, ..., n-1\} = \{e, x, x^2, ..., x^{n-1}\}$$

isto é, $|\langle x \rangle| = n = \circ(x)$.

□

Exemplo 1.22. *Considere o grupo $\mathbb{Z}$ (o grupo aditivo dos inteiros). Fixado $n \in \mathbb{Z}$, o subgrupo $\langle n \rangle$ de $\mathbb{Z}$ é o conjunto dos múltiplos de n em $\mathbb{Z}$, que será denotado por $n\mathbb{Z}$.*

Exemplo 1.23. *Seja $\mathbb{C}^*$ o grupo multiplicativo dos complexos. Fixado $n \in \mathbb{N}$, o conjunto $C_n = \{z \in \mathbb{C}^*; z^n = 1\}$ é um subgrupo de $\mathbb{C}^*$. O subgrupo C_n é cíclico, pois sendo $z = \cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)$, temos $C_n = \langle z \rangle$.*

Observação 1.24. *Mostra-se que a interseção de uma família qualquer de subgrupos é um subgrupo. A demonstração desse fato pode ser feita repetindo os procedimentos da Proposição 3.12 encontrada na Seção 3.8 da referência [12].*

Definição 1.25. Sendo G um grupo e $S \subseteq G$ um subconjunto, denotamos por $\langle S \rangle$ a interseção de todos os subgrupos de G que contém S. Logo, pela Observação 1.24, $\langle S \rangle$ é um subgrupo, chamado de **subgrupo gerado por** S.

Se existe um conjunto S finito tal que $G = \langle S \rangle$, então dizemos que G é um grupo finitamente gerado.

Exemplo 1.26. *Sejam G um grupo, $H \leq G$ e $x \in G$. O conjunto $H^x = \{xhx^{-1};\ h \in H\}$ é um subgrupo, chamado* ***conjugado de H por x.***

Definição 1.27. Sejam G um grupo e N um subgrupo de G. Dizemos que N é um **subgrupo normal**, e denotamos $N \trianglelefteq G$, se $N^x \subseteq N$ para todo $x \in G$, ou seja, N é um subgrupo normal quando o conjugado de N por x estiver contido em N, para todo $x \in G$.

Na realidade temos o seguinte resultado:

Proposição 1.28. *Seja $N \leq G$. São equivalentes:*
(i) N é normal;
(ii) $N^x = N$, para todo $x \in G$;

Demonstração. (ii) $\Rightarrow$ (i)
Essa implicação é imediata, visto que se $N^x = N$, para todo $x \in G$, em particular $N^x \subseteq N$, para todo $x \in G$. Logo, N é normal.
(i) $\Rightarrow$ (ii)
Supondo *(i)*, temos $N^x \subseteq N$, para todo $x \in G$. Mostremos agora que $N \subseteq N^x$, para todo $x \in G$. De fato, seja $n \in N$. Daí, como $n^{x^{-1}} \in N^{x^{-1}}$ e $N^{x^{-1}} \subseteq N$, visto que $N^x \subseteq N$ para todo $x \in G$, por hipótese, então $n^{x^{-1}} \in N$. Logo, $n = (n^{x^{-1}})^x \in N^x$, onde $x^{-1} \in G$ visto que $x \in G$, e portanto $N \subseteq N^x$, para todo $x \in G$. Assim, $N^x = N$, para todo $x \in G$.

□

Seguem alguns exemplos de subgrupos normais:

Exemplo 1.29. *Sendo G um grupo arbitrário, os subgrupos $\{e\}$ e G são normais em G.*

Exemplo 1.30. *Em um grupo G abeliano, todo subgrupo N é normal. Com efeito, temos*

$$N^x = \{xnx^{-1};\ n \in N\} = \{nxx^{-1};\ n \in N\} = \{ne;\ n \in N\} = N.$$

Exemplo 1.31. *Dados G_1 e G_2 grupos, os subgrupos $H_1 = G_1 \times \{e_2\}$ e $H_2 = \{e_1\} \times G_2$ de $G_1 \times G_2$ são normais. Com efeito, dados $(g_1, e_2) \in H_1$ e $(x_1, x_2) \in G_1 \times G_2$, temos*

$$(x_1, x_2)(g_1, e_2)(x_1, x_2)^{-1} = (x_1 g_1 x_1^{-1}, x_2 x_2^{-1}) = (g_1', e_2)$$

onde $g_1' = x_1 g_1 x_1^{-1} \in G_1$. Isto mostra que $H_1^x \subseteq H_1$, para todo $x \in G_1 \times G_2$, e portanto $H_1 \trianglelefteq G_1 \times G_2$. A demonstração para $H_2 \trianglelefteq G_1 \times G_2$ é análoga.

Sejam G um grupo e H e N subgrupos de G. Definimos

$$HN = \{hn \,|\, h \in H, n \in N\}.$$

Observe que H e N são subconjuntos de HN. Mostremos agora que HN é subgrupo de G se, e somente se, $HN = NH$. De fato, supondo HN subgrupo de G, temos $HN = (HN)^{-1} = \{n^{-1}h^{-1} \,|\, h \in H, n \in N\} = NH$. Suponhamos agora que $HN = NH$ e sejam $x, y \in HN$. Daí, $x = h_1n_1$ e $y = h_2n_2$, onde $h_1, h_2 \in H$ e $n_1, n_2 \in N$. Logo, $xy = h_1n_1h_2n_2$ e $x^{-1} = n_1^{-1}h_1^{-1}$. Como $x^{-1} \in NH$, temos $x^{-1} \in HN$, visto que $HN = NH$. Ademais, $n_1h_2 \in NH$ e como $HN = NH$, temos $n_1h_2 = h_3n_3$, onde $h_3 \in H$ e $n_3 \in N$. Portanto, $xy = h_1h_3n_3n_2 \in HN$.

Sendo H e N subgrupos finitos de G, o subconjunto HN de G é também finito e, sendo ou não subgrupo, mostra-se que sua ordem é dada por

$$|HN| = \frac{|H||N|}{|H \cap N|}.$$

A demonstração da igualdade acima pode ser encontrada em [6].

Definição 1.32. Sejam H um subgrupo de G e $x \in G$. Definimos a **classe lateral à esquerda de H contendo** x como sendo o conjunto $xH = \{xh; h \in H\}$. Analogamente, definimos a **classe lateral à direita de H contendo** x como sendo o conjunto $Hx = \{hx; h \in H\}$.

Sejam G um grupo e H um subgrupo de G. A relação "$\sim_H$" em G definida da seguinte forma:

$$x \sim_H y, \textit{ se } xy^{-1} \in H$$

é chamada *relação de congruência módulo H à direita*. Mostra-se que essa relação é uma relação de equivalência. Além disso, denotando por $\overline{g}$ a classe de equivalência do elemento $g \in G$ com respeito a essa relação, temos $\overline{g} = Hg$. Daí,

i) $G = \bigcup_{g \in G} Hg$;

ii) Se $x, y \in G$ e $Hx \neq Hy$, então $Hx \cap Hy = \emptyset$;

iii) Para $x, y \in G$, tem-se:

$$Hx = Hy \iff xy^{-1} \in H \iff x \in Hy \iff y \in Hx.$$

Analogamente, definimos em G a *relação de congruência módulo H à esquerda*, denotada por "$_H \sim$", da seguinte forma:

$$x \ {}_H\sim \ y \ , \text{ se } x^{-1}y \in H.$$

Neste caso, também temos uma relação de equivalência e denotando por $\overline{g}$ a classe de equivalência do elemento $g \in G$ com respeito a essa relação, temos $\overline{g} = gH$. Logo,

iv) $G = \bigcup_{g \in G} gH$;
v) Se $x, y \in G$ e $xH \neq yH$, então $xH \cap yH = \emptyset$;
vi) Para $x, y \in G$, tem-se:

$$xH = yH \Longleftrightarrow x^{-1}y \in H \Longleftrightarrow x \in yH \Longleftrightarrow y \in xH.$$

Sejam G um grupo e H um subgrupo de G. Denotamos por $D_{G:H}$ o conjunto de todas as classes laterais à direita de H em G e por $E_{G:H}$ o conjunto de todas as classes laterais à esquerda de H em G. Consideremos a seguinte aplicação:

$$\begin{array}{rccc} f: & E_{G:H} & \longrightarrow & D_{G:H} \\ & xH & \longmapsto & f(xH) = Hx^{-1}. \end{array}$$

Mostra-se que esta aplicação está bem definida e que é uma bijeção. Dessa forma, os conjuntos $E_{G:H}$ e $D_{G:H}$ têm a mesma cardinalidade, a qual denominamos *índice de H em G* e denotamos por $|G : H|$.

Teorema 1.33. *(Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então, $|G| = |G : H||H|$ e consequentemente $|H|$ divide $|G|$.*

O leitor encontrará a demonstração do Teorema 1.33 na *Seção 3.14* da referência [12].

Corolário 1.34. *Sejam G um grupo finito, $x \in G$, e H e N subgrupos de G. Então*

a) $\circ(x)$ divide $|G|$
b) $|H \cap N|$ divide $|H|$ e $|N|$.

Demonstração. a) Segue da Proposição 1.21 que $\circ(x) = |\langle x \rangle|$ e como $\langle x \rangle$ é um subgrupo de G, utilizando o Teorema 1.33, concluímos que $|\langle x \rangle|$ divide $|G|$, ou seja, $\circ(x)$ divide $|G|$.

b) Segue da Observação 1.24 que $H \cap N$ é um subgrupo de H e de N. Dessa forma, utilizando o Teorema 1.33, temos que $|H \cap N|$ divide $|H|$ e $|N|$. □

Outra definição para um **subgrupo normal** de um grupo é a seguinte:

Definição 1.35. Sejam G um grupo e N um subgrupo de G. Dizemos que N é um **subgrupo normal**, e denotamos $N \trianglelefteq G$, se $xN = Nx$, para todo $x \in G$.

Observe que as Definições 1.27 e 1.35 são equivalentes. De fato, suponha $xN = Nx$, para todo $x \in G$ e seja $a \in N^x$. Daí, $a = xn_1x^{-1}$, onde $n_1 \in N$. Logo, como $xN = Nx$, temos $xn_1 = n_2x$ para algum $n_2 \in N$ e daí $a = n_2xx^{-1}$, ou seja, $a = n_2 \in N$.

Suponhamos agora que $N^x \subseteq N$, para todo $x \in G$. Já foi visto na Proposição 1.28 que $N^x = N$, para todo $x \in G$. Logo, dados $x \in G$ e $n_1 \in N$, temos $xn_1x^{-1} = n_2 \in N$, donde $xn_1 = n_2x$. Portanto, $xN \subseteq Nx$. A inclusão contrária se mostra de forma análoga.

Exemplo 1.36. *Sejam G um grupo e suponha H um subgrupo de $|G : H| = 2$. Dado $g \in G$, temos que se $g \in H$, então $gH = H = Hg$. Se $g \notin H$, então $E_{G:H} = \{H, gH\}$ e $D_{G:H} = \{H, Hg\}$. Assim, devemos ter $gH = G - H = Hg$ e portanto concluímos que $H \trianglelefteq G$.*

Sejam G um grupo e $N \trianglelefteq G$. Pela Definição 1.35, $xN = Nx$, para todo $x \in G$ e portanto podemos mencionar, sob a hipótese de normalidade, simplesmente classes laterais de N em G, ao invés de especificarmos classes laterais à direita ou à esquerda. Denotemos por G/N o conjunto de todas as classes laterais de N em G, ou seja, $G/N = \{xN;\ x \in G\}$.

Definamos a seguinte operação:

$$\begin{array}{rccc} \cdot : & G/N \times G/N & \longrightarrow & G/N \\ & (xN, yN) & \longmapsto & (xN) \cdot (yN) = xyN. \end{array}$$

Utilizando o fato de que N é normal em G, mostra-se que esta operação está bem definida e que o conjunto G/N, munido dela, é um grupo, chamado de **grupo quociente de G por N**. Note que o elemento neutro de G/N é a classe $eN = N$ e que se $x \in G$, então o inverso de xN em G/N é $x^{-1}N$. Por simplicidade de notação, às vezes denotaremos xN por $\overline{x}$.

Exemplo 1.37. *Seja $n \in \mathbb{N}$. Como $\mathbb{Z}$ é um grupo abeliano, então $n\mathbb{Z}$ é normal em $\mathbb{Z}$. Daí, podemos falar do quociente $\mathbb{Z}/n\mathbb{Z}$, o qual denotaremos por $\mathbb{Z}_n$. Pelo Algoritmo da Divisão de Euclides, dado $m \in \mathbb{Z}$, existem $r, q \in \mathbb{Z}$, com $0 \leq r \leq n-1$ tais que $m = nq + r$. Logo, $m - r = nq \in n\mathbb{Z}$ e portanto $\overline{m} = \overline{r}$. Assim, temos $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$, $|\mathbb{Z}_n| = n$ e*

$$\overline{x} + \overline{y} = \overline{x + y} = \overline{r},$$

onde $r \in \{0, 1, ..., n-1\}$ é o resto da divisão euclidiana de $x + y$ por n. Tem-se que $\langle\overline{1}\rangle = \{k\overline{1};\ k \in \mathbb{Z}\} = \mathbb{Z}_n$.

1.2 Homomorfismos de grupos

Definição 1.38. Sejam $(G, *)$ e $(G_1, \cdot)$ grupos. Dizemos que uma aplicação $\varphi : G \longrightarrow G_1$ é um homomorfismo de grupos se $\varphi(x * y) = \varphi(x) \cdot \varphi(y)$ para quaisquer $x, y \in G$.

Definição 1.39. Definimos um isomorfismo entre dois grupos como sendo um homomorfismo de grupos bijetivo.

Sejam G e G_1 grupos. Se existe um isomorfismo de $\varphi : G \longrightarrow G_1$, dizemos que G é *isomorfo* a G_1, e denotamos $G \simeq G_1$. Note que, dados $y_1, y_2 \in G_1$, existem $x_1, x_2 \in G$ tais que $\varphi(x_1) = y_1$ e $\varphi(x_2) = y_2$. Portanto,

$$\varphi^{-1}(y_1y_2) = \varphi^{-1}(\varphi(x_1)\varphi(x_2)) = \varphi^{-1}(\varphi(x_1x_2)) = x_1x_2 = \varphi^{-1}(y_1)\varphi^{-1}(y_2).$$

Logo, $\varphi^{-1} : G_1 \longrightarrow G$ também é um isomorfismo, e assim G_1 é isomorfo a G, daí podemos dizer que G e G_1 são *grupos isomorfos*.

Se dois grupos são isomorfos, eles têm exatamente a mesma "estrutura" e gozam das mesmas propriedades algébricas. Para maiores detalhes, indicamos as referências [12] e [6].

Exemplo 1.40. *Sejam G e G_1 grupos e e_1 o elemento neutro de G_1. A aplicação $\varphi_0 : G \longrightarrow G_1$, definida por $\varphi_0(x) = e_1$ para todo $x \in G$, é um homomorfismo de grupos, chamado de* ***homomorfismo nulo ou trivial****.*

Exemplo 1.41. *Seja G um grupo arbitrário. Considere a aplicação identidade de G, definida por:*

$$\begin{array}{rccc} Id_G : & G & \longrightarrow & G \\ & g & \longmapsto & Id_G(g) = g. \end{array}$$

Esta aplicação é um isomorfismo de G em G. De fato, a aplicação identidade é uma bijeção e, sendo $x, y \in G$ temos:

$$Id_G(xy) = xy = Id_G(x)Id_G(y).$$

Em virtude deste exemplo, concluímos que todo grupo é isomorfo a si próprio.

Exemplo 1.42. *Seja V um espaço vetorial sobre o corpo K. Os conjuntos $GL(V) = \{T : V \longrightarrow V \,;\, T$ é um isomorfismo linear$\}$, munido da composição de funções, e $GL_n(K) = \{(a_{ij})_{n\times n} \,;\, a_{ij} \in K$ e $(a_{ij})_{n\times n}$ é invertível$\}$, munido do produto usual de matrizes, são exemplos de grupos e, ainda mais, mostra-se que esses grupos são isomorfos no caso em que $\dim V = n$, mais especificamente, sendo $\beta = \{v_1, v_2, ..., v_n\}$ uma base de V e $T : V \longrightarrow V$ um elemento de $GL(V)$, a aplicação*

$$\begin{array}{rccl} \varphi: & GL(V) & \longrightarrow & GL_n(K) \\ & T & \longmapsto & \varphi(T) = (a_{ij})_{n\times n}, \end{array}$$

é um isomorfismo, com $T(v_j) = a_{1j}v_1 + a_{2j}v_2 + ... + a_{nj}v_n$ *e* $1 \leq j \leq n$*, onde os coeficientes* a_{ij} *são obtidos a partir desta última igualdade citada.*

1.3 Produto semidireto

Definição 1.43. Sejam G um grupo e H e N subgrupos de G . Dizemos que G é o **produto semidireto** (interno) de N por H se $G = HN$, $H \cap N = \{e\}$ e $N \trianglelefteq G$.

Notações: $G = N \rtimes H$ ou $G = H \rtimes N$.

Agora apresentaremos alguns exemplos de produtos semidiretos.

Exemplo 1.44. *Todo grupo* G *é o produto semidireto de* G *por* $\{e\}$ *(produto semidireto trivial). De fato, bastar notar que* $G = \{e\}G$, $G \cap \{e\} = \{e\}$ *e* $G \trianglelefteq G$.

Exemplo 1.45. *Considerando* $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$*,* $H = \langle\sigma\rangle$ *e* $N = \langle\gamma\rangle$*, temos que* $S_3 = N \rtimes H$*. Com efeito, como* $|H| = |\langle\sigma\rangle| = \circ(\sigma) = 2$, $|N| = |\langle\gamma\rangle| = \circ(\gamma) = 3$ *e* $|S_3| = 3! = 6$ *temos* $|S_3 : N| = \frac{|S_3|}{|N|} = 2$*, ou seja,* $N \trianglelefteq S_3$ *(veja Exemplo 1.36). Ademais, como* $mdc(|H|, |N|) = 1$*, segue do Corolário 1.34 que* $|H \cap N| = 1$ *e daí temos:*

$$|HN| = \frac{|H||N|}{|H \cap N|} = \frac{|H||N|}{1} = 6 = |S_3|.$$

Assim, $HN = S_3$.

Exemplo 1.46. *Considere o grupo diedral infinito* $D_\infty = \mathbb{Z} \times \{-1, 1\}$*, cuja operação é a seguinte:*

$$(a, n) * (b, m) = (a + nb, nm).$$

Temos aqui um caso particular do Exemplo 1.10, onde o grupo G *é o grupo aditivo dos inteiros. Tomando os seguintes subgrupos de* D_∞*:*

$$N = \{(a, 1); a \in \mathbb{Z}\} \quad e \quad H = \{(0, 1), (0, -1)\},$$

temos que $D_\infty = N \rtimes H$*. De fato, sendo* $(a, n) \in D_\infty$*, ou* $(a, n) = (a, 1)$ *ou* $(a, n) = (a, -1)$*, com* $a \in \mathbb{Z}$*. No primeiro caso,* $(a, 1) = (0, 1) * (a, 1)$*, onde*

$(0,1) \in H$ *e* $(a,1) \in N$. *Já no segundo caso,* $(a,-1) = (0,-1) * (-a,1)$, *onde* $(0,-1) \in H$ *e* $(-a,1) \in N$, *e portanto* $(a,n) \in HN$. *Logo,* $D_\infty = HN$. *Ademais, seja* $(a,n) \in H \cap N$. *Dessa forma,* $(a,n) = (0,1)$ *e portanto* $H \cap N = \{(0,1)\}$.

Por fim, queremos mostrar que $N^g \subseteq N$, *para todo* $g \in D_\infty$. *Neste caso,* $g = (a,1)$ *ou* $g = (a,-1)$, *com* $a \in \mathbb{Z}$. *Sendo* $(x,y) \in N^g$ *e* $g = (a,1)$, *temos:*

$$(x,y) = (a,1)^{-1} * (b,1) * (a,1)$$
$$\Rightarrow (x,y) = (-a,1) * (b,1) * (a,1)$$
$$\Rightarrow (x,y) = (b,1),$$

com $b \in \mathbb{Z}$. *Logo,* $(x,y) \in N$. *Sendo* $(x,y) \in N^g$ *e* $g = (a,-1)$, *temos:*

$$(x,y) = (a,-1)^{-1} * (b,1) * (a,-1)$$
$$\Rightarrow (x,y) = (a,-1) * (b,1) * (a,-1)$$
$$\Rightarrow (x,y) = (-b,1),$$

com $b \in \mathbb{Z}$. *Portanto,* $(x,y) \in N$ *e* $N \trianglelefteq D_\infty$. *Assim,* $D_\infty = N \rtimes H$.

1.4 Espaços métricos e isometrias

Nesta seção, faremos uma discussão introdutória sobre Espaços Métricos e Isometrias que será essencial para o entendimento dos principais resultados deste trabalho.

1.4.1 Espaços Métricos

Definição 1.47. Uma *métrica* num conjunto M não vazio é uma função $d : M \times M \longrightarrow \mathbb{R}$ que associa a cada par ordenado de elementos $x, y \in M$ um número real $d(x,y)$, chamado a *distância* de x a y, de modo que sejam satisfeitas as seguintes condições para quaisquer $x, y, z \in M$:

1. $d(x,x) = 0$;
2. Se $x \neq y$, então $d(x,y) > 0$;
3. $d(x,y) = d(y,x)$;
4. $d(x,z) \leq d(x,y) + d(y,z)$ *(Desigualdade Triangular).*

Definição 1.48. Um *Espaço Métrico* é um par (M,d), onde M é um conjunto não vazio e d é uma métrica em M.

Observação 1.49. *Os elementos de um Espaço Métrico podem ser de natureza bastante arbitrária: números, pontos, vetores, matrizes, funções, entre outras coisas.*

São exemplos de Espaços Métricos:

Exemplo 1.50. *(A métrica "zero-um"). Qualquer conjunto M pode tornar-se um espaço métrico de maneira muito simples. Basta definir a métrica $d : M \times M \longrightarrow \mathbb{R}$ pondo $d(x, x) = 0$ e $d(x, y) = 1$ se $x \neq y$. De fato, d é uma métrica pois, sendo $x, y, z \in M$, tem-se:*

1. $d(x, x) = 0$;
2. *Se $x \neq y$, então $d(x, y) = 1 > 0$;*
3. $d(x, y) = d(y, x) = 1$, *se $x \neq y$, e $d(x, y) = d(y, x) = 0$, se $x = y$;*
4. *Analisaremos dois casos:*
   - Se $x = y$, tem-se $d(x, y) = 0$ e assim é imediato que

$$d(x, y) \leq d(x, z) + d(z, y).$$

   - Se $x \neq y$, tem-se $z \neq x$ ou $z \neq y$, e assim

$$d(x, y) = 1 \qquad e \qquad 1 \leq d(x, z) + d(z, y).$$

Este é um dos exemplos mais simples, porém útil para contraexemplos.

Exemplo 1.51. *Se (M, d) é um espaço métrico, todo subconjunto não vazio $S \subseteq M$ pode ser considerado como espaço métrico. Para isso, basta considerarmos a restrição de d a $S \times S$. Quando isto é feito, S chama-se um* ***subespaço de M*** *e a métrica de S diz-se* ***induzida*** *pela de M.*

Exemplo 1.52. *O conjunto $\mathbb{R}$ dos números reais é um dos exemplos mais importantes de espaço métrico. A distância entre dois pontos $x, y \in \mathbb{R}$ é dada por $d(x, y) = |x - y|$(valor absoluto de $x - y$). Note que as condições para termos uma métrica novamente são satisfeitas. Com efeito, sendo $x, y, z \in \mathbb{R}$, tem-se:*

1. $d(x, x) = |x - x| = |0| = 0$;
2. *Se $x \neq y$, então $d(x, y) = |x - y| > 0$;*
3. $d(x, y) = |x - y| = |y - x| = d(y, x)$;
4. *Como $|x - z| \leq |x - y| + |y - z|$, (esta desigualdade pode ser verificada em [10]) temos $d(x, z) \leq d(x, y) + d(y, z)$.*

Essa é a chamada "métrica usual da reta". De agora em diante, quando citarmos a "reta", estaremos nos referindo ao conjunto $\mathbb{R}$ munido desta métrica.

Exemplo 1.53. *(Espaços Vetoriais Normados). Seja E um espaço vetorial real. Uma* ***norma*** *em E é uma função real $|\cdot| : E \longrightarrow \mathbb{R}_+$, que associa a cada vetor $x \in E$ o número real não negativo $|x|$, chamado a* ***norma*** *de x, de modo a serem cumpridas as condições abaixo para quaisquer $x, y \in E$ e $\lambda \in \mathbb{R}$:*

1. *Se $x \neq 0$, então $|x| > 0$*
2. *$|\lambda x| = |\lambda||x|$*
3. *$|x + y| \leq |x| + |y|$.*

Considerando a condição 2 anterior, obtem-se $|0_E| = 0$, tomando $\lambda = 0$, e $|-x| = |x|$ para todo $x \in E$, tomando $\lambda = -1$.

Um ***Espaço Vetorial Normado*** *é um par $(E, |\cdot|)$ onde E é um espaço vetorial real e $|\cdot|$ é uma norma em E. Todo espaço vetorial normado $(E, |\cdot|)$ torna-se um espaço métrico por meio da definição $d(x, y) = |x - y|$. De fato, sendo $x, y, z \in E$ segue da definição de norma:*

1. *$d(x, x) = |x - x| = |0_E| = 0$*
2. *Se $x \neq y$, então $x - y \neq 0_E$ e portanto $|x - y| > 0$*
3. *$d(x, y) = |x - y| = |-(y - x)| = |y - x| = d(y, x)$*
4. *$d(x, z) = |x - z| = |x - y + y - z| \leq |x - y| + |y - z| = d(x, y) + d(y, z)$.*

Exemplo 1.54. *(Espaços Vetoriais com Produto Interno).*

Seja E um espaço vetorial real. Um ***produto interno*** *em E é uma função $\langle , \rangle : E \times E \longrightarrow \mathbb{R}$ que associa a cada par ordenado de vetores $x, y \in E$ um número real $\langle x, y \rangle$, chamado o produto interno de x por y , de modo a serem cumpridas as condições abaixo, para $x, x', y \in E$ e $\lambda \in \mathbb{R}$ arbitrários:*

1. *$\langle x + x', y \rangle = \langle x, y \rangle + \langle x', y \rangle$;*
2. *$\langle \lambda x, y \rangle = \lambda \cdot \langle x, y \rangle$;*
3. *$\langle x, y \rangle = \langle y, x \rangle$;*
4. *$x \neq 0 \Rightarrow \langle x, x \rangle > 0$.*

Usando a condição 1, mostra-se facilmente que $\langle 0_E, y \rangle = \langle x, 0_E \rangle = 0$.

Definição 1.55. Num espaço com produto interno $(E, \langle , \rangle)$, define-se a norma de um vetor $x \in E$ pondo $|x| = \sqrt{\langle x, x \rangle}$, ou seja, $|x|^2 = \langle x, x \rangle$.

Sendo $(E, \langle , \rangle)$ um espaço com produto interno, a aplicação $|\cdot| : E \longrightarrow \mathbb{R}_+$, dada pela definição acima, é de fato uma norma (a demonstração pode ser encontrada em [8], na *Seção 1.1*).

Exemplo 1.56. *O exemplo mais natural de espaço vetorial com produto interno é o* $\mathbb{R}^n$ *, com* $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$*, onde* $x = (x_1, \ldots, x_n)$*,* $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$*. Não é difícil verificar que esta aplicação é de fato um produto interno, o qual é chamado de produto interno canônico do* $\mathbb{R}^n$*.*

Observe que a norma proveniente deste produto interno é dada por

$$|x| = \sqrt{x_1^2 + \ldots + x_n^2},$$

onde $x = (x_1, \ldots, x_n)$*. Esta norma é chamada de norma usual ou norma euclidiana do* $\mathbb{R}^n$*, e proveniente dela temos a métrica usual ou euclidiana do* $\mathbb{R}^n$*, a qual é dada por*

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + \ldots + (x_n - y_n)^2}$$

para $x = (x_1, \ldots, x_n)$*,* $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$*.*

Definição 1.57. Um subconjunto X de um espaço métrico M chama-se *limitado* quando existe uma constante $c > 0$ tal que $d(x, y) \leq c$, para quaisquer $x, y \in X$.

Definição 1.58. Definimos o *diâmetro* de um conjunto limitado $X \subseteq M$ como sendo o número real

$$diam(X) = sup\{d(x, y)\,;\, x, y \in X\}.$$

1.4.2 Aplicações contínuas e sequências

O resultado a seguir nos dá uma importante caracterização de continuidade do ponto de vista técnico.

Definição 1.59. Sejam M e N espaços métricos. Diz-se que a aplicação $f : M \longrightarrow N$ é *contínua no ponto* $a \in M$ quando, para todo $\epsilon > 0$ dado, é possível obter $\delta > 0$ tal que $d(x, a) < \delta$ implica $d(f(x), f(a)) < \epsilon$. Diz-se que $f : M \longrightarrow N$ é *contínua* quando ela é contínua em todos os pontos $a \in M$.

Exemplo 1.60. *Seja E um espaço vetorial real normado. Fixado $x \in E$, a aplicação*

$$\begin{array}{rccc} f_x: & \mathbb{R} & \longrightarrow & E \\ & a & \longmapsto & f_x(a) = ax \end{array}$$

é contínua. Primeiramente, se $x = 0_E$, a aplicação f_x é uma função constante, e portanto f_x é contínua.

No caso em que se $x \neq 0_E$, provaremos que f_x é contínua em $a \in \mathbb{R}$. De fato, dado $\epsilon > 0$, considere $\delta = \dfrac{\epsilon}{||x||}$. Logo,

$$|a-b| < \delta \Rightarrow ||f_x(a) - f_x(b)|| = ||(a-b)x|| = |(a-b)|||x|| < ||x||\frac{\epsilon}{||x||} = \epsilon.$$

Da arbitrariedade de a, segue que f_x é contínua.

Outra definição importante que faremos uso no *Capítulo 3* é a seguinte:

Definição 1.61. Seja $(x_n)_{n\in\mathbb{N}}$ uma sequência num espaço métrico M. Diz-se que o ponto $a \in M$ é *limite* da sequência $(x_n)_{n\in\mathbb{N}}$ quando, para todo $\epsilon > 0$ dado, pode-se obter $n_0 \in \mathbb{N}$ tal que:

$$n > n_0 \Rightarrow d(x_n, a) < \epsilon.$$

Escreve-se então $a = limx_n$. Diz-se também que x_n tende para a e escreve-se $x_n \longrightarrow a$. Quando existe $a = limx_n \in M$, diz-se que a sequência de pontos $x_n \in M$ é convergente em M, e converge para a. Se não existe $limx_n$ em M, dizemos que a sequência é divergente em M.

Outro resultado quando estudamos a teoria de Espaços Métricos é o seguinte:

Proposição 1.62. *Sejam M e N espaços métricos. A fim de que a aplicação $f : M \longrightarrow N$ seja contínua no ponto $a \in M$ é necessário e suficiente que $x_n \longrightarrow a$ em M implique $f(x_n) \longrightarrow f(a)$ em N.*

A demonstração deste resultado pode ser encontrada na *seção 4 do capítulo 5* da referência [8].

1.4.3 Isometrias

Definição 1.63. Sejam M e N espaços métricos. Então $f : M \longrightarrow N$ chama-se uma **imersão isométrica** quando $d(f(x), f(y)) = d(x, y)$, para quaisquer $x, y \in M$.

Intuitivamente, costumamos dizer que uma imersão isométrica é uma aplicação que preserva distâncias.

Observação 1.64. *Uma imersão isométrica é sempre injetora. Com efeito, sejam $x, y \in M$ tais que $f(x) = f(y)$. Como $f(x) = f(y)$, então*

$$d(f(x), f(y)) = 0.$$

Mas $d(f(x), f(y)) = d(x, y)$, pois temos uma imersão isométrica, logo $d(x, y) = 0$ e portanto $x = y$.

Ademais, toda imersão isométrica é contínua. Mostremos que uma imersão isométrica f qualquer é contínua em a. De fato, dado $\epsilon > 0$, considere $\delta = \epsilon$. Logo,

$$d(a, y) < \delta \Rightarrow d(f(a), f(y)) = d(a, y) < \delta = \epsilon.$$

Definição 1.65. Uma **isometria** é uma imersão isométrica sobrejetiva.

Seguem abaixo alguns exemplos de imersões isométricas e isometrias.

Exemplo 1.66. *Seja $\mathbb{R}^n$ com a métrica induzida por uma norma qualquer. Tomemos $a, u \in \mathbb{R}^n$, com $|u| = 1$. A aplicação $f : \mathbb{R} \longrightarrow \mathbb{R}^n$, definida por $f(t) = a + t \cdot u$, é uma imersão isométrica da reta em $\mathbb{R}^n$. De fato, para $s, t \in \mathbb{R}$ arbitrários, temos:*

$$\begin{aligned} d(f(s), f(t)) &= |f(s) - f(t)| = |a + s \cdot u - (a + t \cdot u)| \\ &= |s \cdot u - t \cdot u| = |(s - t)u| \\ &= |(s - t)||u| = |(t - s)||u| \\ &= |(t - s)| = d(s, t). \end{aligned}$$

Exemplo 1.67. *Seja M um espaço métrico. A aplicação identidade*

$$\begin{array}{rccc} Id: & M & \longrightarrow & M \\ & x & \longmapsto & Id(x) = x \end{array}$$

é uma isometria. De fato, para quaisquer $x, y \in M$ temos $d(Id(x), Id(y)) = d(x, y)$, logo Id preserva distâncias e consequentemente é injetiva. Ademais, dado $y \in M$, tem-se $y = Id(y)$, ou seja, a aplicação Id é sobrejetiva. Logo, a aplicação Id é uma isometria.

Exemplo 1.68. *Seja E um espaço vetorial real normado qualquer. Fixado $a \in E$, a aplicação $g : E \longrightarrow E$, dada por $g(x) = x + a$, é uma isometria chamada **translação pelo vetor a**. Com efeito, esta aplicação é uma imersão isométrica pois sendo $x, y \in E$ tem-se:*

$$\begin{aligned} d(g(x), g(y)) &= d(x + a, y + a) = |x + a - y - a| \\ &= |x - y| = d(x, y). \end{aligned}$$

Ademais, g também é sobrejetiva, pois sendo $y \in E$ note que

$$y = y - a + a = g(y - a)$$

com $y - a \in E$, visto que $a, y \in E$.

Exemplo 1.69. *Considere M, N e S espaços métricos e sejam $f : M \longrightarrow N$ e $g : N \longrightarrow S$ isometrias. Então a função composta $g \circ f : M \longrightarrow S$ e a aplicação inversa $f^{-1} : N \longrightarrow M$ também são isometrias.*

Com efeito, dados $x, y \in M$ temos

$$d((g \circ f)(x), (g \circ f)(y)) = d(g(f(x)), g(f(y))) = d(f(x), f(y)) = d(x, y),$$

onde a segunda igualdade segue do fato que a aplicação g é uma isometria (logo preserva distâncias), e a última igualdade é válida pois f também é uma isometria (e portanto também preserva distâncias). Assim, $g \circ f$ preserva distâncias. Além disso, $g \circ f$ é uma aplicação sobrejetiva, visto que é uma composição de aplicações sobrejetivas. Portanto, $g \circ f$ é uma isometria.

Provemos agora que a aplicação f^{-1} é uma isometria. De fato, dados $y_1, y_2 \in N$, temos

$$d(f^{-1}(y_1), f^{-1}(y_2)) = d(f(f^{-1}(y_1)), f(f^{-1}(y_2))) = d(y_1, y_2),$$

onde a primeira igualdade decorre do fato que f é uma isometria. Logo, f^{-1} preserva distâncias. Ademais, f^{-1} é bijetiva. Sendo assim, f^{-1} é uma isometria.

Exemplo 1.70. *Considere o plano, ou seja, o $\mathbb{R}^2$ munido da métrica euclidiana (veja Exemplo 1.56). Identificando o $\mathbb{R}^2$ como o conjunto do números complexos, temos que esta norma é exatamente a função módulo dos números complexos. Fixemos um elemento $u = a + ib$, com $|u|^2 = a^2 + b^2 = 1$. A aplicação $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, definida por $f(z) = u \cdot z$, onde $\cdot$ é a multiplicação de números complexos, é uma isometria. De fato, a aplicação f é uma imersão isométrica, pois sendo $z, w \in \mathbb{R}^2$ tem-se:*

$$\begin{aligned} |f(z) - f(w)| &= |u \cdot z - u \cdot w| = |u(z - w)| \\ &= |u||z - w| = |z - w|. \end{aligned}$$

Além disso, f é sobrejetiva, pois sendo $w \in \mathbb{R}^2$, note que

$$w = (u \cdot u^{-1}) \cdot w = u \cdot (u^{-1} \cdot w) = f(u^{-1} \cdot w),$$

com $u^{-1} \cdot w \in \mathbb{R}^2$.

1.4.4 Teorema da Função Implícita

Para demonstração do principal resultado do Capítulo 2, precisaremos de um Lema que garante a existência de uma base do $\mathbb{R}^n$ sobre certas condições, e na demonstração desse Lema, utilizaremos o Teorema da Função Implícita.

Para o entendimento do resultado que apresentaremos a seguir, *Teorema da Função Implícita*, será necessário que o leitor tenha um conhecimento prévio sobre os conceitos e propriedades básicas de função diferenciável, matriz Jacobiana e topologia do $\mathbb{R}^n$. Para isso, recomendamos as referências [3] e [11].

A seguir, apresentaremos este importante resultado de Análise no $\mathbb{R}^n$. A demonstração do Teorema 1.71 pode ser encontrada na Seção 41 do Capítulo VII, em [3].

Teorema 1.71. *(Teorema da Função Implícita) Sejam Ω um aberto de $\mathbb{R}^p \times \mathbb{R}^q$ e $(a,b) \in \Omega$. Suponha que $F : \Omega \longrightarrow \mathbb{R}^q$ é de classe C^1, $F(a,b) = 0$ e que a aplicação linear definida por*

$$L_2(v) = F'(a,b)(0,v),$$

com $v \in \mathbb{R}^q$, é uma bijeção de $\mathbb{R}^q$ em $\mathbb{R}^q$.

a) Então existe uma vizinhança aberta W de $a \in \mathbb{R}^p$ e uma única função $\varphi : W \longrightarrow \mathbb{R}^q$ de classe C^1 tal que $b = \varphi(a)$ e

$$F(x, \varphi(x)) = 0,$$

para todo $x \in W$.

b) Existe uma vizinhança aberta U de (a,b) em $\mathbb{R}^p \times \mathbb{R}^q$ tal que o par $(x,y) \in U$, satisfaz $F(x,y) = 0$ se, e somente se $y = \varphi(x)$, para todo $x \in W$.

Capítulo 2

Grupos de Isometrias

Neste capítulo será apresentado o assunto que nos motivou a intitular nosso trabalho, Grupos de Isometrias. A demonstração que apresentaremos aqui para este resultado foi baseada na referência [1]. Quando estuda-se Teoria de Grupos, fica notório que os elementos de um grupo podem ser de qualquer natureza, inclusive funções. Estamos interessados na situação onde essas funções são isometrias.

Conforme veremos, o principal resultado deste capítulo diz que todo grupo finito é isomorfo a um grupo de isometrias.

2.1 Grupos de isometrias

Seja M um espaço métrico. O conjunto

$$Isom(M) = \{f : M \longrightarrow M;\ f \text{ é uma isometria}\}$$

munido da composição de funções (denotada por "$\circ$"), é um grupo. De fato, $Isom(M) \neq \emptyset$, pois a aplicação identidade pertence a $Isom(M)$. Além disso, a composição de funções é associativa, ou seja, dadas $f, g, h \in Isom(M)$ temos

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Observe que todas essas composições estão bem definidas, pois todas essas aplicações levam M em M e a composição de isometrias ainda é uma isometria. Tais resultados foram provados no Capítulo 1.

A operação "$\circ$" possui elemento neutro que é exatamente a aplicação Id mencionada anteriormente. De fato, como já foi visto, $Id \in Isom(M)$ e

$$f \circ I_d = I_d \circ f = f,$$

para toda $f \in Isom(M)$.

Por fim, para cada aplicação f em $Isom(M)$, existe g em $Isom(M)$ que cumpre

$$f \circ g = I_d = g \circ f.$$

Neste caso a função g é a inversa da função f, ou seja $g = f^{-1}$, pois

$$f \circ f^{-1} = I_d = f^{-1} \circ f$$

e $f^{-1} \in Isom(M)$, conforme foi visto no Capítulo 1. Portanto, $Isom(M)$ é um grupo como havíamos afirmado anteriormente.

Sejam M um espaço métrico e $(S_M, \circ)$ o grupo das permutações sobre M, ou seja, $S_M = \{f : M \longrightarrow M;\ f \text{ é bijetora}\}$. Observe que $Isom(M) \leq S_M$, pois $Isom(M) \subseteq S_M$ e $Isom(M)$ é fechado à composição e a inversos.

A seguir mostraremos alguns exemplos de grupos de isometrias.

Exemplo 2.1. *Seja M um espaço métrico com apenas um elemento, digamos $M = \{a\}$. O conjunto $G = \{Id_M\}$, onde Id_M é a aplicação identidade de M, é o grupo das isometrias de M. De fato, sendo M unitário, a identidade é a única aplicação de M em M.*

Observemos que este é o grupo de isometrias mais trivial que podemos construir.

O exemplo a seguir é um exemplo de grupo de isometrias com apenas um elemento, como no exemplo 2.1. Porém, neste exemplo, temos um grupo de isometrias de um espaço métrico com três elementos.

Exemplo 2.2. *Considere três pontos distintos do plano, digamos A, B e C, tais que $d(A, B) = 2$, $d(A, C) = 5$ e $d(B, C) = 3$, onde d é a distância entre dois pontos no plano, e seja M o espaço métrico formado por esses três pontos, munido da métrica d, ou seja, (M, d) é um subespaço métrico de $(\mathbb{R}^2, d)$. Observe que este espaço M admite uma única isometria, a identidade.*

Com o intuito de mostrarmos esta última afirmação, observemos que as demais aplicações candidatas a serem isometrias (as cinco permutações de $M = \{A, B, C\}$ além da identidade) serão descritas nas possibilidades abaixo:

1ª Possibilidade: *Considere $f : M \longrightarrow M$ dada por $f(A) = A$, $f(B) = C$ e $f(C) = B$. Temos:*

$$2 = d(A, B) \neq d(f(A), f(B)) = d(A, C) = 5.$$

Logo, a aplicação f não é uma isometria.

2ª Possibilidade: *Considere $f : M \longrightarrow M$ dada por $f(A) = B$, $f(B) = A$ e $f(C) = C$. Temos:*

$$5 = d(A, C) \neq d(f(A), f(C)) = d(B, C) = 3.$$

Logo, a aplicação f não é uma isometria.

3ª Possibilidade: *Considere $f : M \longrightarrow M$ dada por $f(A) = B$, $f(B) = C$ e $f(C) = A$. Temos:*

$$2 = d(A, B) \neq d(f(A), f(B)) = d(B, C) = 3.$$

Logo, a aplicação f não é uma isometria.

4ª Possibilidade: *Considere $f : M \longrightarrow M$ dada por $f(A) = C$, $f(B) = A$ e $f(C) = B$. Temos:*

$$2 = d(A, B) \neq d(f(A), f(B)) = d(C, A) = 5.$$

Logo, a aplicação f não é uma isometria.

5ª Possibilidade: *Considere $f : M \longrightarrow M$ dada por $f(A) = C$, $f(B) = B$ e $f(C) = A$. Temos:*

$$2 = d(A, B) \neq d(f(A), f(B)) = d(C, B) = 3.$$

Logo, a aplicação f não é uma isometria.

Note que em todas essas possibilidades analisadas, a aplicação f não é uma isometria. Assim, concluímos que a única isometria neste caso é a aplicação identidade.

Exemplo 2.3. *(Grupo de isometrias com dois elementos). Seja $M = \{a, b\}$ um espaço métrico. O conjunto $G = \{Id_M, f\}$, onde f é a aplicação $f : M \longrightarrow M$ dada por $f(b) = a$ e $f(a) = b$, é o grupo das isometrias de M. Verifiquemos este fato. Já mencionamos que a aplicação Id_M é uma isometria. Observe que f também é uma isometria, pois f preserva distâncias visto que:*

$$d(a, a) = 0 = d(b, b) = d(f(a), f(a))$$

e

$$d(a, b) = d(f(b), f(a)) = d(f(a), f(b)).$$

As igualdades acima decorrem da definição da aplicação f e do fato que d é uma métrica sobre M. De forma análoga, $d(b, a) = d(f(b), f(a))$ e $d(b, b) = d(f(b), f(b))$. Logo, para quaisquer $x, y \in M$ tem-se $d(x, y) = d(f(x), f(y))$, ou seja, f preserva distâncias. Ademais, f é sobrejetiva.

Assim, temos $G \subseteq Isom(M)$. Além disso, Id_M e f são as únicas funções bijetoras de M em M. Logo, não existem outras isometrias além dessas.

Exemplo 2.4. *No começo deste capítulo foi mencionado que $Isom(M) \leq S_M$, para todo espaço métrico M. Iremos mostrar neste exemplo que dado um conjunto não vazio qualquer, é possível definir neste conjunto*

alguma métrica de modo que o grupo das isometrias do espaço métrico obtido coincide com o grupo das permutações do conjunto. De fato, sendo M um conjunto qualquer, fixemos um número real positivo λ e definamos

$$d_\lambda : M \times M \longrightarrow \mathbb{R} \quad , \quad d_\lambda(x,y) = \begin{cases} 0 & , \text{ se } x = y \\ \lambda & , \text{ se } x \neq y \end{cases}$$

De modo análogo ao que foi feito no Exemplo 1.50, mostra-se que d_λ é uma métrica. Ademais, dada $f \in S_M$, para x, $y \in M$ tem-se que $f(x) = f(y)$ se, e somente se, $x = y$, uma vez que f é injetiva. Logo, $d_\lambda(x,y) = d_\lambda(f(x), f(y))$, para quaisquer x, $y \in M$, e assim $f \in Isom(M, d_\lambda)$. Logo, $Isom(M, d_\lambda) = S_M$.

Por outro lado, seja N um espaço métrico, com pelo menos 2 elementos, tal que $Isom(N) = S_N$. Fixados x_0, $y_0 \in N$, distintos, tomemos $\alpha = d(x_0, y_0)$. Dados x, $y \in N$ quaisquer e distintos, existe $f \in S_N$ tal que $f(x_0) = x$ e $f(y_0) = y$. Como f é uma isometria, devemos ter $d(x,y) = d(x_0, y_0) = \alpha$. Daí, concluímos que $d = d_\alpha$.

2.2 Isometrias de alguns subconjuntos da Reta

Nesta seção, estudaremos o grupo de isometrias da reta e o grupo de isometrias dos inteiros. Estudaremos também um subconjunto da reta cujo o grupo de isometrias é o grupo cíclico infinito. No estudo do grupo das isometrias da reta e dos inteiros, aparecerão casos particulares do grupo DG, sendo G um grupo abeliano, descrito no Exemplo 1.10.

Considere X um subespaço métrico da reta, com $0 \in X$, e $f \in Isom(X)$. Temos $f(x) = x + a$, para todo $x \in X$, ou $f(x) = -x + a$, para todo $x \in X$, onde $a \in X$ é fixo e depende de f. Com efeito, sendo $f \in Isom(X)$, considere $f(0) = a$, onde $a \in X$. Daí,

$$|x - 0| = |f(x) - f(0)| = |f(x) - a|, \qquad (I)$$

para todo $x \in X$. Por (I), concluímos que $f(x) - a = x$ ou $f(x) - a = -x$, para cada $x \in X$.

Vamos supor que existam $x_1, x_2 \in X - \{0\}$, tais que

$$f(x_1) = x_1 + a \qquad \text{e} \qquad f(x_2) = -x_2 + a.$$

Daí,

$$|x_1 - x_2| = |f(x_1) - f(x_2)| = |x_1 + a + x_2 - a| = |x_1 + x_2|. \qquad (II)$$

Para que valha a igualdade em (II), devemos ter $x_1 + x_2 = x_1 - x_2$ ou $x_1 + x_2 = -x_1 + x_2$, isto é, $x_2 = 0$ ou $x_1 = 0$, o que é um absurdo, pois fizemos a suposição que $x_1, x_2 \in X - \{0\}$. Dessa forma, temos apenas duas possibilidades: $f(x) = x + a$, para todo $x \in X$, ou $f(x) = -x + a$, para todo $x \in X$.

É importante observar que nem toda aplicação de uma dessas duas formas é bem definida em X. Por exemplo, considere o conjunto $X = \{0, 2\}$, $a = 2$ e a seguinte aplicação

$$\begin{array}{rccc} f: & X & \longrightarrow & X \\ & x & \longmapsto & f(x) = x + 2. \end{array}$$

Observe que $f(2) = 4$ e $4 \notin X$. E mesmo sendo bem definida, não precisa ser sobrejetora. Por exemplo, considere a seguinte aplicação

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & x & \longmapsto & f(x) = x + 1. \end{array}$$

Essa aplicação está bem definida mas não é sobrejetora. No entanto, sendo $h : X \longrightarrow X$ bem definida e sobrejetora, e sendo de uma dessas formas, não é difícil ver que h é uma isometria de X. De fato, se $h(x) = x + a$, então

$$|h(x) - h(y)| = |x + a - (y + a)| = |x - y|$$

e se $h(x) = -x + a$, então

$$|h(x) - h(y)| = | - x + a - (-y + a)| = | - x + y| = |x - y|.$$

Exemplo 2.5. *(Isometrias da Reta). Considere a reta* $\mathbb{R}$*. Dada* $f \in Isom(\mathbb{R})$*, temos apenas duas possibilidades para* f*:* $f(x) = x + a$*, para todo* $x \in \mathbb{R}$*, ou* $f(x) = -x + a$*, para todo* $x \in \mathbb{R}$*, onde* $a = f(0)$*. Para ver isso, utilizamos o que foi comentado anteriormente, pois* $\mathbb{R} \subseteq \mathbb{R}$ *e* $0 \in \mathbb{R}$*. Observe que nas duas possibilidades temos funções bem definidas e bijeções para qualquer valor de* $a \in \mathbb{R}$*. Logo,*

$$Isom(\mathbb{R}) = \{f_{a,n};\ a \in \mathbb{R},\ n = \pm 1\},$$

onde $f_{a,n} : \mathbb{R} \longrightarrow \mathbb{R}$ *é definida por* $f_{a,n}(x) = nx + a$*. A aplicação*

$$\begin{array}{rccc} \varphi: & D\mathbb{R} & \longrightarrow & Isom(\mathbb{R}) \\ & (a, n) & \longmapsto & \varphi(a, n) = f_{a,n} \end{array}$$

é um isomorfismo de grupos, onde $\mathbb{R} = (\mathbb{R}, +)$*, e "+" é a operação de adição usual(O grupo* $D\mathbb{R}$ *é um caso particular do Exemplo 1.10, onde o grupo* G *é o grupo* $(\mathbb{R}, +)$*). Com efeito, sendo* $(a, n_1), (b, n_2) \in D\mathbb{R}$*, temos:*

$$\varphi((a,n_1)*(b,n_2)) = \varphi((a+n_1b, n_1n_2)) = f_{a+n_1b,\, n_1n_2}.$$

Por outro lado,

$$f_{a,n_1}(f_{b,n_2}(x)) = n_1(n_2x+b)+a = n_1n_2x + (n_1b+a) = f_{a+n_1b,\, n_1n_2}(x),$$

para todo $x \in \mathbb{R}$. *Portanto,*

$$\varphi(a,n_1)\circ\varphi(b,n_2) = f_{a,n_1}\circ f_{b,n_2} = f_{a+n_1b,\, n_1n_2} = \varphi((a,n_1)*(b,n_2)).$$

Dessa forma, mostramos que a aplicação φ *é um homomorfismo. Ademais, suponhamos* $\varphi(a,n_1) = \varphi(b,n_2)$, *isto é,* $f_{a,n_1}(x) = f_{b,n_2}(x)$, *para todo* $x \in \mathbb{R}$. *Daí,* $n_1x+a = n_2x+b$, *para todo* $x \in \mathbb{R}$. *Em particular, esta última igualdade vale para* $x = 0$ *e para* $x = 1$, *daí temos* $a = b$ *e* $n_1 = n_2$, *e portanto* $(a,n_1) = (b,n_2)$, *mostrando assim que a aplicação* φ *é injetiva.*

Por fim, seja $f \in Isom(\mathbb{R})$. *Como* $Isom(\mathbb{R}) = \{f_{a,n};\ a \in \mathbb{R},\ n = \pm 1\}$, *existem* $n \in \{-1,1\}$ *e* $a \in \mathbb{R}$ *tal que* $f = f_{a,n}$, *e assim* $f = f_{a,n} = \varphi(a,n)$, *onde* $(a,n) \in D\mathbb{R}$, *mostrando que a aplicação* φ *é sobrejetiva. Portanto, os grupos* $D\mathbb{R}$ *e* $Isom(\mathbb{R})$ *são isomorfos.*

Exemplo 2.6. *(Isometrias dos inteiros). Considere o conjunto* $\mathbb{Z}$ *dos inteiros como subespaço métrico da reta. Dada* $f \in Isom(\mathbb{Z})$, *temos apenas duas possibilidades para* f: $f(x) = x+a$, *para todo* $x \in \mathbb{Z}$, *ou* $f(x) = -x+a$, *para todo* $x \in \mathbb{Z}$, *onde* $a = f(0)$. *Para ver isso, utilizamos novamente o que foi comentado no começo dessa seção, pois* $\mathbb{Z} \subseteq \mathbb{R}$ *e* $0 \in \mathbb{Z}$. *Observe que, como no exemplo anterior, nas duas possibilidades temos funções bem definidas e bijeções para qualquer valor de* $a \in \mathbb{Z}$. *Logo,*

$$Isom(\mathbb{Z}) = \{f_{a,n};\ a \in \mathbb{Z},\ n = \pm 1\},$$

onde $f_{a,n} : \mathbb{Z} \longrightarrow \mathbb{Z}$ *é definida por* $f_{a,n}(x) = nx+a$. *Considere o grupo diedral infinito* D_∞*(Veja Exemplo 1.46). Mostra-se, analogamente ao isomorfismo mostrado no Exemplo 2.5, que o grupo* $Isom(\mathbb{Z})$ *é isomorfo ao grupo diedral infinito.*

Exemplo 2.7. *Considere o seguinte conjunto:*

$$A = \mathbb{Z} + \left\{0, \frac{1}{2}, \frac{1}{3}\right\} = \mathbb{Z} \cup \left\{n + \frac{1}{2};\ n \in \mathbb{Z}\right\} \cup \left\{n + \frac{1}{3};\ n \in \mathbb{Z}\right\}$$

e sobre este conjunto consideremos a métrica usual da reta (A *é um subespaço métrico da reta). Dado* $a \in \mathbb{Z}$, *a aplicação*

$$\begin{array}{rccc} \phi_a : & A & \longrightarrow & A \\ & x & \longmapsto & \phi_a(x) = x + a \end{array}$$

é uma isometria do conjunto A. Ademais, toda isometria do conjunto A é da forma de ϕ_a. De fato, dados $x \in A$ e $a \in \mathbb{Z}$, temos que $x+a \in A$ e assim $\phi_a : A \longrightarrow A$ é bem definida. Além disso, dado $y \in A$, temos $y-a \in A$ e $\phi_a(y-a) = y-a+a = y$, donde ϕ_a é sobrejetiva. Logo, pelo que comentamos no começo dessa seção, temos que $\phi_a \in Isom(A)$.

Por outro lado, como $A \subseteq \mathbb{R}$ e $0 \in A$, dada $F \in Isom(A)$, concluímos que $F(x) = x+a$, para todo $x \in A$, ou $F(x) = -x+a$, para todo $x \in A$, com $a = F(0)$. Além disso, mostraremos que $a \in \mathbb{Z}$, e para isso, como $a \in A$, mostraremos que $a \notin \left\{n + \frac{1}{2};\ n \in \mathbb{Z}\right\}$ e $a \notin \left\{n + \frac{1}{3};\ n \in \mathbb{Z}\right\}$, analisando 4 possibilidades:

1ª Possibilidade($F(x) = x + a$):

Suponha que $a \in \left\{n + \frac{1}{2};\ n \in \mathbb{Z}\right\}$, ou seja,

$$a = n_1 + \frac{1}{2};\ n_1 \in \mathbb{Z}.$$

Como neste caso, $F(x) = x + a$, temos:

$$F(x) = x + n_1 + \frac{1}{2}.$$

Logo,

$$F\left(\frac{1}{3}\right) = \frac{1}{3} + n_1 + \frac{1}{2} = n_1 + \frac{5}{6}.$$

Absurdo, pois por um lado $F\left(\frac{1}{3}\right) \in A$, visto que F é de A em A, e por outro lado $n_1 + \frac{5}{6} \notin A$. Portanto, $a \notin \left\{n + \frac{1}{2};\ n \in \mathbb{Z}\right\}$.

2ª Possibilidade($F(x) = -x + a$):

Suponha novamente que $a \in \left\{n + \frac{1}{2};\ n \in \mathbb{Z}\right\}$, ou seja,

$$a = n_1 + \frac{1}{2};\ n_1 \in \mathbb{Z}.$$

Como neste caso $F(x) = -x + a$, temos:

$$F(x) = -x + n_1 + \frac{1}{2}.$$

Daí,

$$F\left(\frac{1}{3}\right) = -\frac{1}{3} + n_1 + \frac{1}{2} = n_1 + \frac{1}{6}.$$

Absurdo, pois novamente temos $F\left(\frac{1}{3}\right) \in A$ *e* $n_1 + \frac{1}{6} \notin A$. *Assim,* $a \notin \left\{n + \frac{1}{2};\ n \in \mathbb{Z}\right\}$.

3ª Possibilidade$(F(x) = x + a)$*:*

Neste caso, vamos supor que $a \in \left\{n + \frac{1}{3};\ n \in \mathbb{Z}\right\}$, *ou seja,*

$$a = n_1 + \frac{1}{3};\ n_1 \in \mathbb{Z}.$$

Como neste caso, $F(x) = x + a$, *temos:*

$$F(x) = x + n_1 + \frac{1}{3}.$$

Assim,

$$F\left(\frac{1}{2}\right) = \frac{1}{2} + n_1 + \frac{1}{3} = n_1 + \frac{5}{6}.$$

Analogamente às análises realizadas nas possibilidades anteriores, temos um absurdo. Assim, $a \notin \left\{n + \frac{1}{3};\ n \in \mathbb{Z}\right\}$.

4ª Possibilidade$(F(x) = -x + a)$*:*

Suponha que $a \in \left\{n + \frac{1}{3};\ n \in \mathbb{Z}\right\}$, *ou seja,*

$$a = n_1 + \frac{1}{3};\ n_1 \in \mathbb{Z}.$$

Como neste caso, $F(x) = -x + a$, *temos*

$$F(x) = -x + n_1 + \frac{1}{3}.$$

Logo,

$$F\left(-\frac{1}{2}\right) = \frac{1}{2} + n_1 + \frac{1}{3} = n_1 + \frac{5}{6}$$

e novamente temos um absurdo. Sendo assim, $a \notin \left\{ n + \frac{1}{3};\ n \in \mathbb{Z} \right\}$. *Dessa forma, concluímos que* $a \in \mathbb{Z}$, *como queríamos mostrar.*

Sendo assim, suponhamos agora que $F(x) = -x + a$, *com* $a \in \mathbb{Z}$. *Logo,*

$$F\left(\frac{1}{3}\right) = -\frac{1}{3} + a, \text{ com } a \in \mathbb{Z}$$

um absurdo, pois $-\frac{1}{3} + a \notin A$. *Assim,* $F(x) = x + a$ *para todo* $x \in A$, *e portanto toda isometria do conjunto* A *é da forma:*

$$\begin{array}{rccc} \phi_a: & A & \longrightarrow & A \\ & x & \longmapsto & \phi_a(x) = x + a \end{array}$$

com $a \in \mathbb{Z}$.

Por fim, a aplicação

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & Isom(A) \\ & a & \longmapsto & \phi(a) = \phi_a \end{array}$$

é um isomorfismo entre o grupo aditivo dos inteiros e o grupo $Isom(A)$. *De fato, sendo* $a, b \in \mathbb{Z}$, *como*

$$\phi_{a+b}(x) = x + a + b = x + b + a = \phi_a(x + b) = \phi_a(\phi_b(x)),$$

para todo $x \in A$, *então* $\phi(a+b) = \phi(a) \circ \phi(b)$, *e daí concluímos que a aplicação* ϕ *é um homomorfismo. Suponhamos agora* $\phi(a) = \phi(b)$, *ou seja,* $\phi_a = \phi_b$. *Logo,* $\phi_a(x) = \phi_b(x)$, *para todo* $x \in A$. *Sendo assim,* $x + a = x + b$, *para todo* $x \in A$. *Em particular, quando* $x = 0$, *temos* $a = b$ *e portanto a aplicação* ϕ *é injetiva. Para mostrar a sobrejetividade da aplicação* ϕ, *basta observar que dado* $f \in Isom(A)$, *pelo que já foi mostrado anteriormente,* $f = \phi_a$, *onde* $a \in \mathbb{Z}$. *Daí,* $f = \phi_a = \phi(a)$, *com* $a \in \mathbb{Z}$, *e concluímos assim que a aplicação* ϕ *é um isomorfismo.*

2.3 Grupos finitos como grupos de isometrias

Conforme foi visto na Seção 2.1, o conjunto $Isom(M)$ munido da composição de funções é um grupo. Diante disso, é natural surgir o seguinte questionamento: Será que dado um grupo G qualquer, existe algum espaço métrico M, cujo grupo de isometrias de M é isomorfo a G? Nesta seção, mostraremos que a resposta para essa pergunta é positiva para todos os grupos finitos.

Definição 2.8. Diz-se que um conjunto de pontos W em um espaço euclidiano realiza um grupo G se o grupo de isometrias de W é isomorfo a G.

Mostraremos a seguir que todo grupo finito G além de ser isomorfo a um grupo de isometrias, pode ser realizado por um subconjunto finito de algum $\mathbb{R}^n$. Antes disso, vejamos as seguintes observações:

Observação 2.9. *Seja $n \in \mathbb{N}$ e considere*

$$v = (x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, \ldots, x_{n1}, x_{n2}, \ldots, x_{nn}) \in \mathbb{R}^{n^2}.$$

Definimos $\det(v)$ *como sendo o determinante da matriz* $(x_{ij})_{n\times n}$ *. Com isso, temos uma função* $\det : \mathbb{R}^{n^2} \longrightarrow \mathbb{R}$*, a qual é contínua.*

Sendo $v_0 = (a_{11}, a_{12}, \ldots, a_{1n}, a_{21}, a_{22}, \ldots, a_{2n}, \ldots, a_{n1}, a_{n2}, \ldots, a_{nn}) \in \mathbb{R}^{n^2}$ *tal que os vetores*

$$(a_{11}, a_{12}, \ldots, a_{1n}) \ , \ (a_{21}, a_{22}, \ldots, a_{2n}) \ , \ \ldots \ , \ (a_{n1}, a_{n2}, \ldots, a_{nn})$$

de $\mathbb{R}^n$ *são LI, temos que* $\det(v_0) \neq 0$*. Observando que a função* $\det$ *é contínua, concluímos que existe algum aberto* A *de* $\mathbb{R}^{n^2}$*, com* $v_0 \in A$*, tal que para todo*

$$v = (x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, \ldots, x_{n1}, x_{n2}, \ldots, x_{nn}) \in A$$

tem-se $\det(v) \neq 0$ *e portanto os vetores*

$$(x_{11}, x_{12}, \ldots, x_{1n}) \ , \ (x_{21}, x_{22}, \ldots, x_{2n}) \ , \ \ldots \ , \ (x_{n1}, x_{n2}, \ldots, x_{nn})$$

são LI em $\mathbb{R}^n$ *.*

Observação 2.10. *Considere* $a \in \mathbb{R}$*, com* $a \geq 0$*, e* $u_0 = (a, a, \ldots, a) \in \mathbb{R}^n$*. Seja*

$$D_1 \cup D_2 \cup \ldots \cup D_m = \{1, 2, \ldots, n\}$$

uma partição, ou seja, $D_i \cap D_j = \varnothing$*, para* $i \neq j$*. Tomemos* b_1*,* b_2*,* $\ldots$*,* $b_m \in \mathbb{R}$*, todos maiores que* a*, tais que* $b_i = b_j$ *se, e somente se,* i *e* j *pertencem ao mesmo conjunto* D_k *da partição dada de* $\{1, 2, \ldots, n\}$*.*

Considere agora A *um subconjunto aberto de* $\mathbb{R}^n$ *tal que* $u_0 \in A$*. Tomando* $w_0 = (b_1, b_2, \ldots, b_n)$*, considere* $v = w_0 - u_0$ *e* $\lambda > 0$ *tal que a bola fechada* $B[u_0, \lambda]$ *está contida em* A*. Tomando então*

$$v_1 = u_0 + \frac{\lambda}{|v|} v$$

temos que $v_1 \in A$*. Ademais, sendo* $v_1 = (c_1, c_2, \ldots, c_n)$*, temos que todos os* c_i*'s são positivos e* $c_i = c_j$ *se, e somente se,* i *e* j *estão no mesmo conjunto* D_k *da partição dada de* $\{1, 2, \ldots, n\}$*.*

Antes de apresentarmos o resultado principal, o Teorema 2.15, veremos o Lema 2.11 e algumas observações. Ressaltamos que as demonstrações aqui apresentadas, tanto do Teorema 2.15 quanto do Lema 2.11, são baseadas nas demonstrações feitas na referência [1].

Lema 2.11. *Considere o conjunto* $D = \{(i,j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i < j \leq n\}$ *e uma partição* $D_1 \cup D_2 \cup \ldots \cup D_m = D$ *do conjunto* D. *Então existe uma base* $\{X_1, X_2, \ldots, X_n\}$ *do* $\mathbb{R}^n$ *tal que:*
1) A j*-ésima coordenada de* X_i *é zero para* $i < j$.
2) Todos os X_i*'s têm norma 1, considerando a norma euclidiana.*
3) $d(X_i, X_j) = d(X_k, X_l)$ *se, e somente se, os pares* (i,j) *e* (k,l) *estão no mesmo conjunto* D_s *da partição de* D *dada acima, onde* d *é a métrica euclidiana.*

Demonstração. Seja $f : \mathbb{R}^{n^2+q} = \mathbb{R}^{n^2} \times \mathbb{R}^q \longrightarrow \mathbb{R}^{n^2}$, com $q = (n^2 - n)/2$, $f = f(\overline{X}, \overline{\delta})$, onde

$$\overline{X} = (x_{11}, x_{12}, \ldots, x_{1n}, x_{21}, x_{22}, \ldots, x_{2n}, \ldots, x_{n1}, x_{n2}, \ldots, x_{nn}) \qquad e$$

$$\overline{\delta} = (\delta_{12}, \delta_{13}, \ldots, \delta_{1n}, \delta_{23}, \ldots, \delta_{n-1,n}) \ (\delta_{ij} \ , \ i < j).$$

Considere $f = (f_1, f_2, \ldots, f_{n^2})$, tal que:

- Para $s < r$: $f_{(s-1)n+r} = x_{sr}$
- Para $s = r$: $f_{(s-1)n+r} = x_{s1}^2 + \ldots + x_{sn}^2 - 1$
- Para $s > r$: $f_{(s-1)n+r} = (x_{s1} - x_{r1})^2 + \ldots + (x_{sn} - x_{rn})^2 - \delta_{rs}^2$,

onde $s, r \in \{1, 2, \ldots, n\}$. Considere o ponto $(A, B) \in \mathbb{R}^{n^2+q}$ dado por $A = (e_1, e_2, \ldots, e_n) \in \mathbb{R}^{n^2}$, onde $\{e_1, e_2, \ldots, e_n\}$ é a base canônica do $\mathbb{R}^n$, e $B = (\sqrt{2}, \sqrt{2}, \ldots, \sqrt{2}) \in \mathbb{R}^q$. Temos $f(A, B) = (0, 0, \ldots, 0)$. Com efeito, observe que para $s < r$ temos:

$$f_{(s-1)n+r}(A, B) = f_{(s-1)n+r}((e_1, e_2, ..., e_n), (\sqrt{2}, ..., \sqrt{2})) = x_{sr} = 0,$$

pois $s \neq r$. Para $s = r$, temos:

$$f_{(s-1)n+r}((e_1, e_2, ..., e_n), (\sqrt{2}, ..., \sqrt{2})) = x_{s1}^2 + ... + x_{sn}^2 - 1 = 1 - 1 = 0.$$

Por fim, para $s > r$ temos:

$$\begin{aligned} f_{(s-1)n+r}((e_1, e_2, ..., e_n), (\sqrt{2}, ..., \sqrt{2})) &= (x_{s1} - x_{r1})^2 + ... + (x_{sn} - x_{rn})^2 - \delta_{sr}^2 \\ &= 2 - (\sqrt{2})^2 = 0. \end{aligned}$$

Como cada f_i é uma função polinomial, então f é uma função de classe C^1. Seja $M = M(\overline{X}, \overline{\delta})$ a matriz formada pelas n^2 primeiras colunas da matriz jacobiana de f. Assim, M é uma matriz $n \times n$ que tem na k-ésima linha as derivadas parciais de f_k em relação às variáveis:

$$x_{11},\ x_{12},\ \ldots\ ,\ x_{1n},\ x_{21},\ x_{22},\ \ldots\ ,\ x_{2n},\ \ldots\ ,\ x_{n1},\ x_{n2},\ \ldots\ ,\ x_{nn}$$

e as colunas correspondem a essas variáveis nesta sequência. Podemos então ver essa matriz da seguinte forma:

$$M = \begin{pmatrix} B_{11} & B_{12} & \cdots & B_{1n} \\ B_{21} & B_{22} & \cdots & B_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ B_{n1} & B_{n2} & \cdots & B_{nn} \end{pmatrix}$$

onde

$$B_{si} = \begin{pmatrix} \frac{\partial f_{(s-1)n+1}}{\partial x_{i1}} & \frac{\partial f_{(s-1)n+1}}{\partial x_{i2}} & \cdots & \frac{\partial f_{(s-1)n+1}}{\partial x_{in}} \\ \frac{\partial f_{(s-1)n+2}}{\partial x_{i1}} & \frac{\partial f_{(s-1)n+2}}{\partial x_{i2}} & \cdots & \frac{\partial f_{(s-1)n+2}}{\partial x_{in}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_{sn}}{\partial x_{i1}} & \frac{\partial f_{sn}}{\partial x_{i2}} & \cdots & \frac{\partial f_{sn}}{\partial x_{in}} \end{pmatrix}$$

para s, $i \in \{1, 2, \ldots, n\}$. Assim, em um bloco B_{si}, as derivadas parciais estão em relação às variáveis x_{ij}, com $1 \leq j \leq n$. Considerando o caso $s < i$ (blocos acima da diagonal), temos que as variáveis x_{ij} não aparecem nas funções $f_{(s-1)n+1}$, $f_{(s-1)n+2}$, $\ldots$, f_{sn}, e daí todas as derivadas parciais são nulas. Logo, o bloco B_{si} é nulo, para $s < i$, e portanto a matriz M é triangular em blocos.

Vejamos agora os blocos diagonais, fazendo $x_{ii} = 1$, $x_{ij} = 0$, para $i \neq j$, e $\delta_{ij} = \sqrt{2}$ (o ponto (A, B) mencionado anteriormente). Observemos que:

$$B_{ss} = \begin{pmatrix} \frac{\partial f_{(s-1)n+1}}{\partial x_{s1}} & \frac{\partial f_{(s-1)n+1}}{\partial x_{s2}} & \cdots & \frac{\partial f_{(s-1)n+1}}{\partial x_{sn}} \\ \frac{\partial f_{(s-1)n+2}}{\partial x_{s1}} & \frac{\partial f_{(s-1)n+2}}{\partial x_{s2}} & \cdots & \frac{\partial f_{(s-1)n+2}}{\partial x_{sn}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_{sn}}{\partial x_{s1}} & \frac{\partial f_{sn}}{\partial x_{s2}} & \cdots & \frac{\partial f_{sn}}{\partial x_{sn}} \end{pmatrix}$$

Fixado s arbitrário:

- Para $r < s$, temos que a linha r deste bloco é:

$$2(x_{s1} - x_{r1}) \quad 2(x_{s2} - x_{r2}) \quad \ldots \quad 2(x_{sn} - x_{rn})$$

Fazendo a avaliação no ponto (A, B), aparece -2 na coluna r, 2 na coluna s e 0 nas demais.

- Para $s = r$, temos que a linha $r = s$ deste bloco é:

$$2x_{s1} \quad 2x_{s2} \quad \dots \quad 2x_{sn}$$

Fazendo a avaliação no ponto (A, B), aparece 2 na coluna $r = s$ e 0 nas demais.

- Para $r > s$, temos que a linha r deste bloco é:

$$0 \quad 0 \quad \dots \quad 0 \quad 1 \quad 0 \dots \quad 0$$

onde o 1 aparece na coluna r.

Dessa forma, mostra-se que todos os blocos diagonais de $M(A, B)$ são triangulares superiores com elementos diagonais não nulos. Logo, são inversíveis. Portanto, como o $detM(A, B)$=$detB_{11}$ $detB_{22} \cdots$ $detB_{nn}$ e $detB_{11}$, $detB_{22}$,...,$detB_{nn}$ são todos diferentes de zero, pois os blocos diagonais são inversíveis, temos $detM(A, B) \neq 0$, ou seja, $M(A, B)$ é inversível.

Como a matriz $M(A, B)$ é inversível, segue do Teorema 1.71 (Teorema da Função Implícita) que existem abertos $U \subseteq \mathbb{R}^q$ e $V \subseteq \mathbb{R}^{n^2+q}$, com $(A, B) \in V$ e $B \in U$, e uma única função $\xi : U \longrightarrow \mathbb{R}^{n^2}$ de classe C^1 tais que $(\xi(\overline{\delta}), \overline{\delta}) \in V$ e $f(\xi(\overline{\delta}), \overline{\delta}) = (0, 0, \dots, 0)$ para todo $\overline{\delta} \in U$.

Temos $\xi(B) = A$ e, como $A = (e_1, e_2, \dots, e_n)$ (a base canônica do $\mathbb{R}^n$), segue da Observação 2.9 que existe um aberto $Z \subseteq \mathbb{R}^{n^2}$, com $A \in Z$, tal que para todo $\overline{X} = (X_1, X_2, \dots, X_n) \in Z$ tem-se $\{X_1, X_2, \dots, X_n\}$ linearmente independente. Pela continuidade de ξ, existe um aberto $W \subseteq \mathbb{R}^q$, com $B \in W \subseteq U$, tal que $\xi(W) \subseteq Z$.

Dessa forma, sendo $B = (\sqrt{2}, \sqrt{2}, \dots, \sqrt{2}) \in W$, segue da Observação 2.10 que existe

$$B_1 = (d_{12}, d_{13}, \dots, d_{1n}, d_{23}, \dots, d_{n-1,n}) \in W$$

tal que $d_{ij} > 0$ e $d_{ij} = d_{kl}$ se, e somente se, (i, j) e (k, l) estão no mesmo conjunto D_s da partição de D dada no enunciado.

Sendo $\overline{Y} = (Y_1, Y_2, \dots, Y_n) = \xi(B_1)$, temos

$$f(\overline{Y}, B_1) = f(\xi(B_1), B_1) = (0, 0, \dots, 0).$$

Logo, para Y_1, Y_2, ..., Y_n valem as condições 1, 2 e 3 do enunciado. De fato, seja y_{ij} a j-ésima coordenada de Y_i. Para $i < j$, segue

$$y_{ij} = f_{(i-1)n+j}(\overline{Y}, B_1) = 0.$$

Ademais, quando $s = r$, obtemos $f_{(s-1)n+r}(\overline{Y}, B_1) = y_{s1}^2 + ... + y_{sn}^2 - 1 = 0$, ou seja, $||Y_s||^2 = 1$ e, portanto $||Y_s|| = 1$, com $s \in \{1, 2, ...n\}$. Por fim, para $s > r$, tem-se

$$f_{(s-1)n+r}(\overline{Y}, B_1) = (Y_{s1} - Y_{r1})^2 + ... + (Y_{sn} - Y_{rn})^2 - d_{rs}^2 = 0$$
$$\Rightarrow d_{rs}^2 = (Y_{s1} - Y_{r1})^2 + ... + (Y_{sn} - Y_{rn})^2 = d(Y_r, Y_s)^2.$$

Analogamente, $d_{kl}^2 = (Y_{l1} - Y_{k1})^2 + ... + (Y_{ln} - Y_{kn})^2 = d(Y_k, Y_l)^2$, onde $k < l$. Supondo $d(Y_r, Y_s) = d(Y_k, Y_l)$, temos $d_{rs} = d_{kl}$ e daí, pelo que foi visto acima, concluímos que $(r, s), (k, l)$ estão no mesmo conjunto D_s da partição D. Reciprocamente, supondo que $(r, s), (k, l)$ estão no mesmo conjunto D_s da partição D, segue que $d_{rs} = d_{kl}$, e daí $d(Y_r, Y_s) = d(Y_k, Y_l)$.

Dessa forma, ficam verificadas as três condições do enunciado para $Y_1, Y_2, ..., Y_n$. Ademais, como $\overline{Y} = (Y_1, Y_2, \ldots, Y_n) \in Z$, temos Y_1, Y_2, ..., Y_n LI. □

Definição 2.12. Sejam A e B pontos distintos do $\mathbb{R}^n$. Definimos o *segmento* $[A, B]$ como sendo o conjunto:

$$[A, B] = \{(1 - t)A + tB \ ; \ 0 \leq t \leq 1\}.$$

Observação 2.13. *Denote por d a métrica usual do $\mathbb{R}^n$. Sendo A, B, C $\in \mathbb{R}^n$, dois a dois distintos, são equivalentes:*
i) $B \in [A, C]$
ii) $d(A, C) = d(A, B) + d(B, C)$
iii) $\overrightarrow{AB} = \lambda \overrightarrow{BC}$ para algum λ real e positivo.

De fato, temos:
i) $\Rightarrow$ ii)
Suponha que $B \in [A, C]$. Dessa forma, $B = (1 - t_0)A + t_0C$, com $t_0 \in \mathbb{R}$, tal que $0 \leq t_0 \leq 1$. Logo,

$$d(A, B) = ||B - A|| = ||(1 - t_0)A + t_0C - A|| = ||t_0(C - A)||$$

e

$$d(B, C) = ||C - B|| = ||C - ((1 - t_0)A + t_0C)|| = ||(1 - t_0)C + (-1 + t_0)A||.$$

Portanto,

$$\begin{aligned} d(A,B)+d(B,C) &= ||t_0(C-A)|| + ||(1-t_0)C+(-1+t_0)A|| \\ &= |t_0|\cdot||C-A|| + |1-t_0|\cdot||C-A|| \\ &= (t_0+(1-t_0))||C-A|| \\ &= d(A,C). \end{aligned}$$

ii) $\Rightarrow$ iii)

Suponhamos agora $d(A,C) = d(A,B) + d(B,C)$. Dessa forma,

$$||\overrightarrow{AC}|| = ||\overrightarrow{AB}|| + ||\overrightarrow{BC}||$$
$$\Rightarrow ||\overrightarrow{AB}+\overrightarrow{BC}|| = ||\overrightarrow{AB}|| + ||\overrightarrow{BC}||$$
$$\Rightarrow ||\overrightarrow{AB}+\overrightarrow{BC}||^2 = ||\overrightarrow{AB}||^2 + 2||\overrightarrow{AB}||\,||\overrightarrow{BC}|| + ||\overrightarrow{BC}||^2.$$

Por outro lado,

$$||\overrightarrow{AB}+\overrightarrow{BC}||^2 = \langle \overrightarrow{AB}+\overrightarrow{BC}, \overrightarrow{AB}+\overrightarrow{BC}\rangle = ||\overrightarrow{AB}||^2 + 2\langle \overrightarrow{AB}, \overrightarrow{BC}\rangle + ||\overrightarrow{BC}||^2.$$

Assim,

$$||\overrightarrow{AB}||\,||\overrightarrow{BC}|| = \langle \overrightarrow{AB}, \overrightarrow{BC}\rangle$$

e daí $\overrightarrow{AB} // \overrightarrow{BC}$, ou seja, $\overrightarrow{AB} = \lambda\overrightarrow{BC}$ para algum $\lambda \in \mathbb{R}$ (veja [4], seção 6.1).

Mostremos agora que λ é um número positivo. De fato, de $||\overrightarrow{AB}||\,||\overrightarrow{BC}|| = \langle \overrightarrow{AB}, \overrightarrow{BC}\rangle$ temos $|\lambda|\cdot||\overrightarrow{BC}||^2 = \lambda\langle \overrightarrow{BC}, \overrightarrow{BC}\rangle$ e assim $\lambda = |\lambda|$.

iii) $\Rightarrow$ i)

Suponhamos $\overrightarrow{AB} = \lambda\overrightarrow{BC}$, para algum λ real positivo. Assim,

$$\begin{aligned} B - A &= \lambda(C-B) \\ \Rightarrow B + \lambda B &= \lambda C + A \\ \Rightarrow (1+\lambda)B &= A + \lambda C \\ \Rightarrow B &= \frac{1}{1+\lambda}A + \frac{\lambda}{1+\lambda}C, \end{aligned}$$

pois $(1+\lambda) \neq 0$. Observe que $\frac{1}{1+\lambda} = 1 - \frac{\lambda}{1+\lambda}$ e $0 \leq \frac{\lambda}{1+\lambda} \leq 1$. Logo, $B \in [A,C]$.

Observação 2.14. *Sejam $S \subseteq \mathbb{R}^n$ e $f \in Isom(S)$. Se X_1, X_2, $X_3 \in S$ são tais que $X_2 \in [X_1, X_3]$, segue da Observação 2.13 que $d(X_1,X_3) = d(X_1,X_2) + d(X_2,X_3)$, e daí*

$$d(f(X_1), f(X_3)) = d(f(X_1), f(X_2)) + d(f(X_2), f(X_3)).$$

Logo, $f(X_2) \in [f(X_1), f(X_3)]$.

Teorema 2.15. *Seja G um grupo finito de ordem n. Então:*
a) G é isomorfo a um subgrupo de $Isom(\mathbb{R}^n)$.
b) Existe algum subconjunto finito W de $\mathbb{R}^n$ tal que $Isom(W)$ é isomorfo a G.

Demonstração. a) Seja $G = \{g_1 = e, g_2, \ldots, g_n\}$ (onde e é o elemento neutro de G). Tomemos a seguinte partição de G:

$$G = Q_1 \cup Q_2 \cup \ldots \cup Q_m,$$

onde cada Q_i é da forma $\{x, x^{-1}\}$.

Considere o conjunto

$$D = \{(i,j) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq i < j \leq n\}.$$

Para cada $s \in \{1, 2, \ldots, m\}$ defina $D_s = \{(i,j) \in D \mid g_i^{-1} g_j \in Q_s\}$. Observe que:

$$D_1 \cup D_2 \cup \cdots \cup D_m = D \quad e \quad D_s \cap D_t = \varnothing, \text{ para } s \neq t.$$

De fato, consideremos $(i,j) \in D$. Dessa forma, como $g_i^{-1} g_j \in G$ e $G = Q_1 \cup Q_2 \cup \ldots \cup Q_m$, então $g_i^{-1} g_j \in Q_s$, para algum $s \in \{1, 2, ..., m\}$. Logo, $(i,j) \in D_s$, para algum $s \in \{1, 2, ..., m\}$, e portanto $D = \bigcup_{i=1}^{m} D_i$. Ademais, para mostrar que $D_s \cap D_t = \varnothing$, para $s \neq t$, basta observar que $Q_s \cap Q_t = \varnothing$, para $s \neq t$.

Considere uma base $W_1 = \{X_1, X_2, \ldots, X_n\}$ de $\mathbb{R}^n$ que cumpre todas as condições do Lema 2.11, considerando a partição acima do conjunto D. Dessa forma,

$$d(X_i, X_j) = d(X_k, X_l) \iff g_i^{-1} g_j = g_k^{-1} g_l \quad \text{ou} \quad g_i^{-1} g_j = g_l^{-1} g_k.$$

A equivalência acima decorre imediatamente da condição (3) do Lema 2.11.

Para cada $g \in G$, defina

$$\begin{array}{rccl} \sigma_g : & W_1 & \longrightarrow & W_1 \\ & X_i & \longmapsto & \sigma_g(X_i) = gX_i = X_j \end{array}$$

onde j é tal que $g_j = g g_i$. Observe que σ_g é uma permutação de W_1.

Para cada segmento $[X_i, X_j]$ considere o conjunto

$$\mathcal{O}[X_i, X_j] = \{[gX_i, gX_j] \mid g \in G\}.$$

Vamos denominar esses conjuntos de *órbitas*.

Afirmação 1) $\mathcal{O}[X_i, X_j] = \mathcal{O}[X_k, X_l]$ ou $\mathcal{O}[X_i, X_j] \cap \mathcal{O}[X_k, X_l] = \varnothing$.

De fato, suponhamos que $\mathcal{O}[X_i, X_j] \cap \mathcal{O}[X_k, X_l] \neq \varnothing$, ou seja, que existem $a, b \in G$ tais que:

$$[aX_i, aX_j] = [bX_k, bX_l].$$

Daí,

$$ag_i = bg_k \quad \text{e} \quad ag_j = bg_l \implies (b^{-1}a)g_i = g_k \quad \text{e} \quad (b^{-1}a)g_j = g_l.$$

ou

$$ag_i = bg_l \quad \text{e} \quad ag_j = bg_k \implies (b^{-1}a)g_i = g_l \quad \text{e} \quad (b^{-1}a)g_j = g_k.$$

Tomando então $g = b^{-1}a$, concluímos que $[X_k, X_l] = [gX_i, gX_j]$.

Agora, dado $h \in G$, temos

$$[hX_k, hX_l] = [(hg)X_i, (hg)X_j] \in \mathcal{O}[X_i, X_j]$$

e assim $\mathcal{O}[X_k, X_l] \subseteq \mathcal{O}[X_i, X_j]$. De maneira análoga, mostra-se a inclusão contrária.

Afirmação 2) $\mathcal{O}[X_i, X_j] = \mathcal{O}[X_k, X_l] \iff d(X_i, X_j) = d(X_k, X_l)$.

Suponha que $\mathcal{O}[X_i, X_j] = \mathcal{O}[X_k, X_l]$. Daí, existe $g \in G$ tal que $[X_i, X_j] = [gX_k, gX_l]$, ou seja, $X_i = gX_k$ e $X_j = gX_l$, ou $X_i = gX_l$ e $X_j = gX_k$. Logo, $g_i = gg_k$ e $g_j = gg_l$, ou $g_i = gg_l$ e $g_j = gg_k$. Portanto,

$$g_i^{-1}g_j = (gg_k)^{-1}gg_l = g_k^{-1}g^{-1}gg_l = g_k^{-1}g_l$$

ou

$$g_i^{-1}g_j = (gg_l)^{-1}gg_k = g_l^{-1}g^{-1}gg_k = g_l^{-1}g_k.$$

Assim, $d(X_i, X_j) = d(X_k, X_l)$.

Suponha agora que $d(X_i, X_j) = d(X_k, X_l)$. Logo, $g_i^{-1}g_j = g_k^{-1}g_l$ ou $g_i^{-1}g_j = g_l^{-1}g_k$. Se $g_i^{-1}g_j = g_k^{-1}g_l$, então $g_k g_i^{-1} = g_l g_j^{-1}$ e, chamando este elemento de a, temos $g_k = ag_i$ e $g_l = ag_j$, donde $\begin{cases} X_k = aX_i \\ X_l = aX_j \end{cases}$. Analogamente, se $g_i^{-1}g_j = g_l^{-1}g_k$, então existe $b \in G$ tal que $g_l = bg_i$ e $g_k = bg_j$, donde $\begin{cases} X_k = bX_j \\ X_l = bX_i \end{cases}$. Portanto, $\mathcal{O}[X_i, X_j] \cap \mathcal{O}[X_k, X_l] \neq \varnothing$, e pelo que já foi visto anteriormente, temos $\mathcal{O}[X_i, X_j] = \mathcal{O}[X_k, X_l]$.

Para cada $g \in G$ considere o operador linear $T_g : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ tal que $T_g(X_i) = gX_i$, para todo $i = 1, \ldots, n$. Observe que T_g é um operador linear bijetivo. Note que $d(T_g(X_i), T_g(X_j)) = d(X_i, X_j)$ para $i, j \in \{1, 2, \ldots, n\}$.

De fato,

$$d(T_g(X_i), T_g(X_j)) = d(gX_i, gX_j) = d(X_i, X_j),$$

pois $[gX_i, gX_j] \in \mathcal{O}[X_i, X_j]$ e assim $\mathcal{O}[gX_i, gX_j] = \mathcal{O}[X_i, X_j]$.

Logo,

$$\begin{aligned} d(T_g(X_i), T_g(X_j))^2 &= d(X_i, X_j)^2 \\ \Rightarrow ||T_g(X_i) - T_g(X_j)||^2 &= ||X_i - X_j||^2 \\ \Rightarrow \ \langle T_g(X_i) - T_g(X_j), T_g(X_i) - T_g(X_j)\rangle &= \langle X_i - X_j, X_i - X_j\rangle \\ \Rightarrow ||T_g(X_i)||^2 - 2\langle T_g(X_i), T_g(X_j)\rangle + ||T_g(X_j)||^2 &= \\ = ||X_i||^2 - 2\langle X_i, X_j\rangle + ||X_j||^2. & \end{aligned}$$

Observe que $||T_g(X_i)|| = ||T_g(X_j)|| = ||X_i|| = ||X_j|| = 1$, pois $T_g(X_i) = X_k$ e $T_g(X_j) = X_l$. Assim, $\langle T_g(X_i), T_g(X_j)\rangle = \langle X_i, X_j\rangle$. (onde $\langle\ ,\rangle$ é o produto interno canônico do $\mathbb{R}^n$). Podemos estender essa ideia para todo o $\mathbb{R}^n$, isto é, podemos mostrar que T_g é uma isometria do $\mathbb{R}^n$. De fato, sejam $y, z \in \mathbb{R}^n$. Podemos escrever y e z, de forma única, da seguinte maneira:

$$\begin{aligned} y &= \alpha_1 X_1 + \alpha_2 X_2 + ... + \alpha_n X_n \\ z &= \beta_1 X_1 + \beta_2 X_2 + ... + \beta_n X_n. \end{aligned}$$

Logo,

$$\begin{aligned} T_g(y) &= \alpha_1(T_g(X_1)) + ... + \alpha_n(T_g(X_n)) \\ T_g(z) &= \beta_1(T_g(X_1)) + ... + \beta_n(T_g(X_n)). \end{aligned}$$

Assim,

$$\begin{aligned} \langle T_g(y), T_g(z)\rangle &= \langle \sum_{i=1}^{n} \alpha_i T_g(X_i), \sum_{j=1}^{n} \beta_j T_g(X_j)\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i\beta_j \langle T_g(X_i), T_g(X_j)\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i\beta_j \langle X_i, X_j\rangle \\ &= \langle y, z\rangle. \end{aligned}$$

Portanto,

$$\begin{aligned} d(T_g(y), T_g(z))^2 &= \langle T_g(y) - T_g(z), T_g(y) - T_g(z) \rangle \\ &= \langle T_g(y - z), T_g(y - z) \rangle \\ &= \langle y - z, y - z \rangle \\ &= (d(y, z))^2. \end{aligned}$$

Segue daí que $d(T_g(y), T_g(z)) = d(y, z)$, para quaisquer $y, z \in \mathbb{R}^n$, e portanto T_g é uma isometria do $\mathbb{R}^n$.

Considerando agora a aplicação

$$\begin{array}{rccc} \psi: & G & \longrightarrow & Isom(\mathbb{R}^n) \\ & g & \longmapsto & \psi(g) = T_g \end{array}$$

temos que ψ é um homomorfismo injetivo de grupos e assim $G \simeq Im\ \psi$, ou seja, G é isomorfo a um subgrupo de $Isom(\mathbb{R}^n)$. Com efeito, sendo $g, h \in G$ e supondo $\psi(g) = \psi(h)$, temos $T_g(X) = T_h(X)$ para todo $X \in \mathbb{R}^n$, ou seja, $gX = hX$, para todo $X \in \mathbb{R}^n$. Em particular, $gX_1 = hX_1$. Logo, $g = h$ (lembrando que $g_1 = e$) e assim fica provada a injetividade. Ademais, observe que

$$T_{gh}(X_i) = (gh)X_i = g(hX_i) = T_g(hX_i) = T_g(T_h(X_i)) = (T_g \circ T_h)(X_i),$$

para todo $X_i \in W_1$. Daí, como T_{gh} e $T_g \circ T_h$ são lineares, e W_1 é base de $\mathbb{R}^n$, concluímos que

$$\psi(gh) = T_{gh} = T_g \circ T_h = \psi(g) \circ \psi(h)$$

e assim a aplicação ψ é um homomorfismo.

b) Para demonstrar o item (b), começaremos construindo o conjunto W_2. Fixada uma órbita $\mathcal{O}$, escolha um segmento $[X_i, X_j] \in \mathcal{O}$ (considere $i < j$).

Afirmação 3) Se $(g_i^{-1} g_j)^2 = e$, considere o ponto médio do segmento $[X_i, X_j]$:

$$u_{ij} = \frac{1}{2}(X_i + X_j).$$

Se o segmento $[X_k, X_l]$ (considere $k < l$) pertence à órbita $\mathcal{O}$, então $\mathcal{O}[X_i, X_j] = \mathcal{O}[X_k, X_l]$ e daí $g_k^{-1} g_l = g_i^{-1} g_j$ ou $g_k^{-1} g_l = g_j^{-1} g_i$, e assim $(g_k^{-1} g_l)^2 = e$ e daí tome

$$u_{kl} = \frac{1}{2}(X_k + X_l).$$

Observe que $[X_k, X_l] = [gX_i, gX_j]$ para algum $g \in G$ e daí

$$u_{kl} = \frac{1}{2}(gX_i + gX_j) = T_g(u_{ij}).$$

Vamos denotar este elemento por gu_{ij}.

Afirmação 4) Se $(g_i^{-1}g_j)^2 \neq e$, considere no segmento $[X_i, X_j]$ o ponto:

$$u_{ij} = X_i + \frac{1}{3}(X_j - X_i).$$

Fixado $g \in G$, considere $X_k = gX_i$ e $X_l = gX_j$. Temos então $g_k^{-1}g_l = g_i^{-1}g_j \neq e$ e assim tomamos no segmento $[X_k, X_l]$ o ponto

$$X_k + \frac{1}{3}(X_l - X_k) = gX_i + \frac{1}{3}(gX_j - gX_i).$$

Observe que este ponto, que vamos denotar por gu_{ij}, é exatamente $T_g(u_{ij})$. Este ponto será o elemento u_{kl} (ou u_{lk}, dependendo se $k < l$ ou $l < k$).

Consideremos então $W_2 = \{u_{ij}\,;\,(i,j) \in D\}$ e $W = W_1 \cup W_2$ (observemos que $W_1 \cap W_2 = \varnothing$). Segue da independência linear do conjunto $W_1 = \{X_1, X_2, \ldots, X_n\}$ que dois segmentos $[X_i, X_j]$ e $[X_k, X_l]$ não se intersectam, a não ser por um dos extremos. Logo, $u_{ij} \neq u_{kl}$ para $(i,j) \neq (k,l)$, e assim W_2 tem exatamente $(n^2 - n)/2$ elementos.

Segue também da independência linear de W_1 que não se pode ter $X_i \in [X_l, X_k]$ e nem $X_i \in [u_{lk}, u_{jt}]$ (basta observar a definição de segmento no $\mathbb{R}^n$). Também não se pode ter $X_i \in [X_j, u_{kl}]$. De fato, supondo $X_i = \lambda_1 X_j + \lambda_2 u_{kl}$, com λ_1, $\lambda_2 \in [0,1]$ e $\lambda_1 + \lambda_2 = 1$, como u_{kl} é combinação linear de X_k e X_l, devemos ter $j = k$ e $i = l$ (ou $j = l$ ou $i = k$), donde $X_i \in [X_j, u_{ij}]$, um absurdo (já que $u_{ij} \in [X_i, X_j]$).

Para todo $g \in G$ tem-se $T_g(W_1) = W_1$. Ademais, pela construção de W_2, tem-se que $T_g(W_2) \subseteq W_2$, e assim, como W_2 é finito e T_g é injetora, concluímos que $T_g(W_2) = W_2$ e portanto

$$T_g(W) = T_g(W_1 \cup W_2) = T_g(W_1) \cup T_g(W_2) = W_1 \cup W_2 = W.$$

Assim, a restrição de T_g a W é uma isometria de W. Resta então mostrar que toda isometria de W é desta forma.

Sendo $\varphi \in Isom(W)$, mostremos primeiramente que $\varphi(W_2) = W_2$. De fato, se $\varphi(u_{ij}) = X_k$, como $u_{ij} \in [X_i, X_j]$ e φ é uma isometria, pela Observação 2.14 teríamos $X_k \in [\varphi(X_i), \varphi(X_j)]$, o que já vimos que não pode acontecer. Logo, devemos ter de fato $\varphi(W_2) = W_2$ e daí, como φ é bijetora e $W = W_1 \cup W_2$, segue que $\varphi(W_1) = W_1$.

Seja $\varphi(X_1) = X_{j_0}$. Dessa forma, $\varphi(X_1) = g_{j_0}X_1$ (lembrando que $g_1 = e$) e mostremos que $\varphi(X_i) = g_{j_0}X_i$ para todo $i \in \{1, 2, \ldots, n\}$. De fato, fixemos então $i \in \{1, 2, \ldots, n\}$, arbitrário. Como $\varphi(X_1)$, $\varphi(X_i) \in W_1$ e $d(\varphi(X_1), \varphi(X_i)) = d(X_1, X_i)$, pois φ é uma isometria, segue da *Afirmação*

2) que $\mathcal{O}[X_1, X_i] = \mathcal{O}[\varphi(X_1), \varphi(X_i)]$. Logo, $[\varphi(X_1), \varphi(X_i)] \in \mathcal{O}[X_1, X_i]$ e daí temos:

$$\begin{cases} \varphi(X_1) = aX_1 \\ \varphi(X_i) = aX_i \end{cases} \qquad \text{ou} \qquad \begin{cases} \varphi(X_1) = bX_i \\ \varphi(X_i) = bX_1 \end{cases}$$

com a, $b \in G$.

- Se $g_i^2 = e$, temos

$$g_1 = g_i g_i = e \Rightarrow X_1 = g_i X_i.$$

Como $X_i = g_i X_1$ e $X_1 = g_i X_i$, se vale a segunda alternativa acima, basta tomar $a = bg_i$ e teremos

$$\begin{cases} \varphi(X_1) = bX_i = ag_iX_i = aX_1 \\ \varphi(X_i) = bX_1 = ag_iX_1 = aX_i \end{cases}$$

- Se $g_i^2 \neq e$, então $(g_1^{-1}g_i)^2 \neq e$. Assim, segue da *Afirmação 4)* que u_{1i} não é o ponto médio do segmento $[X_1, X_i]$ e daí $d(X_1, u_{1i}) \neq d(X_i, u_{1i})$. Suponhamos que

$$\begin{cases} \varphi(X_1) = bX_i \\ \varphi(X_i) = bX_1 \end{cases}$$

para algum $b \in G$. Como $u_{1i} \in [X_1, X_i]$, segue da Observação 2.14 que $\varphi(u_{1i}) \in [\varphi(X_1), \varphi(X_i)] = [bX_i, bX_1]$. Ademais, segue da *Afirmação 4)* que $bu_{1i} \in [bX_1, bX_i]$. Como $\varphi(u_{1i})$ e bu_{1i} são elementos de W_2 e estão ambos em $[bX_i, bX_1]$, devemos ter $\varphi(u_{1i}) = bu_{1i} = T_b(u_{1i})$. Daí,

$$d(X_1, u_{1i}) = d(T_b(X_1), T_b(u_{1i})) = d(\varphi(X_i), \varphi(u_{1i})) = d(X_i, u_{1i}),$$

o que é um absurdo.

Assim, em qualquer situação ($g_i^2 = e$ ou $g_i^2 \neq e$), temos $\begin{cases} \varphi(X_1) = aX_1 \\ \varphi(X_i) = aX_i \end{cases}$, para algum $a \in G$. Como $aX_1 = \varphi(X_1) = X_{j_0} = g_{j_0}X_1$, devemos ter $a = g_{j_0}$. Logo, $\varphi(X_i) = g_{j_0}X_i$, para todo $i \in \{1, 2, \ldots, n\}$. Ademais, dados $i, j \in \{1, 2, \ldots, n\}$, com $i < j$, temos

$$\varphi(u_{ij}) \in [\varphi(X_i), \varphi(X_j)] = [g_{j_0}X_i, g_{j_0}X_j]$$

e assim $\varphi(u_{ij}) = g_{j_0}u_{ij}$. Segue então que φ é a restrição de $T_{g_{j_0}}$ a W.

Para cada $g \in G$, seja $T_g|_W : W \longrightarrow W$ a restrição de T_g a W. Assim, a aplicação

$$\begin{array}{rccc} \zeta: & G & \longrightarrow & Isom(W) \\ & g & \longmapsto & \zeta(g) = T_g|_W \end{array}$$

é um isomorfismo de grupos. De fato, como visto no item (a), ψ é um homomorfismo injetivo e daí conclui-se que ζ também é. Pelo que foi discutido anteriormente, temos que a aplicação ζ é sobrejetiva, pois toda isometria de W tem a forma $T_g|_W$, ou seja, é a restrição de uma aplicação T_g a W. Dessa forma, temos de fato que ζ é um isomorfismo de grupos.

□

Capítulo 3

Isometrias de Espaços Vetoriais Reais Normados

Já mencionamos anteriormente o grupo de isometrias de um espaço métrico M qualquer. Como um espaço vetorial normado, em particular, é um espaço métrico, podemos ser ainda mais específicos e mencionar os grupos de isometrias de espaços vetoriais normados. Esses grupos de isometrias serão os objetos de estudo deste capítulo.

Em todo este capítulo, todos os espaços vetoriais mencionados serão sobre o corpo dos reais.

3.1 Translações e Isometrias Lineares

3.1.1 Translações

No Exemplo 1.68 definimos as translações num espaço vetorial normado E. Vejamos agora que o conjunto das translações é um subgrupo do grupo das isometrias de E.

Proposição 3.1. *Sejam E um espaço vetorial normado e $a \in E$ fixado. Considere a aplicação*

$$\begin{array}{rccc} T_a: & E & \longrightarrow & E \\ & x & \longmapsto & T_a(x) = x + a. \end{array}$$

O conjunto $H = \{T_a\,;\, a \in E\}$ é um subgrupo abeliano de $Isom(E)$.

Demonstração. 1) H é um subgrupo de $Isom(E)$:

De fato, $H \subseteq Isom(E)$, pois as aplicações $T_a : E \longrightarrow E$ são isometrias, como já foi visto no Exemplo 1.68. Além disso, sejam $T_a, T_{a'} \in H$ com $a, a' \in E$ fixados, tais que

$$\begin{array}{rccl} T_a: & E & \longrightarrow & E \\ & x & \longmapsto & T_a(x) = x + a. \end{array}$$

e

$$\begin{array}{rccl} T_{a'}: & E & \longrightarrow & E \\ & x & \longmapsto & T_{a'}(x) = x + a'. \end{array}$$

Temos:

$$(T_a \circ T_{a'})(z) = T_a(T_{a'}(z)) = T_a(z + a') = z + (a' + a) = T_{a'+a}(z),$$

para todo $z \in E$, onde $a' + a \in E$. Portanto, como $T_a \circ T_{a'} = T_{a'+a}$ e $T_{a'+a} \in H$, então $T_a \circ T_{a'} \in H$.

Seja $T_a \in H$. Como $T_a \circ T_a^{-1} = Id_E$, temos:

$$(T_a \circ T_a^{-1})(z) = z \Rightarrow T_a(T_a^{-1}(z)) = z \Rightarrow T_a^{-1}(z) + a = z \Rightarrow T_a^{-1}(z) = z - a,$$

para todo $z \in E$. Como $T_a^{-1}(z) = z - a = z + (-a) = T_{-a}(z)$, então $T_a^{-1} = T_{-a} \in H$.

Assim, concluímos que H é um subgrupo de $Isom(E)$.

2) H é abeliano:

Seja E_+ o grupo aditivo do espaço vetorial E. Observe a seguinte aplicação:

$$\begin{array}{rccl} \phi: & E_+ & \longrightarrow & H \\ & a & \longmapsto & \phi(a) = T_a. \end{array}$$

A aplicação ϕ é um isomorfismo. De fato, a sobrejetividade é imediata. Sendo $a, b \in E_+$, temos:

$$\phi(a) = \phi(b) \Rightarrow T_a(x) = T_b(x),\ \forall x \in E \Rightarrow x + a = x + b,\ \forall x \in E \Rightarrow a = b.$$

Fica provado assim a injetividade. Por fim, sendo $a, b \in E_+$, temos:

$$T_{a+b}(x) = x + a + b = x + b + a = T_a(x + b) = T_a(T_b(x)),$$

para todo $x \in E$, e portanto $\phi(a + b) = T_{a+b} = T_a \circ T_b = \phi(a) \circ \phi(b)$. Dessa forma, concluímos que ϕ de fato é um isomorfismo. Portanto, como E_+ é abeliano (veja o Exemplo 1.11), então H é abeliano.

□

3.1.2 Isometrias Lineares

Seja E um espaço vetorial normado.

Proposição 3.2. *Considere o subgrupo $H = \{T_a\,;\, a \in E\}$ (mencionado na Proposição 3.1) de $Isom(E)$. O conjunto $K = \{g \in Isom(E)\,;\, g \text{ é linear}\}$ é um subgrupo de $Isom(E)$ e $H^{g^{-1}} \subseteq H$, para todo $g \in K$.*

Demonstração. 1) K é um subgrupo de $Isom(E)$:

De fato, $K \subseteq Isom(E)$. Sendo $g_1, g_2 \in K$ note que a composição $g_1 \circ g_2$ está bem definida e é uma isometria, visto que temos uma composição de isometrias, como já foi mostrado anteriormente no Exemplo 1.69. Ademais, $g_1 \circ g_2$ é uma aplicação linear, pois g_1 e g_2 são aplicações lineares.

Além disso, para cada $g_1 \in K$, temos $g_1^{-1} \in K$. Isto ocorre porque g_1^{-1} também é uma isometria, pois é inversa de uma isometria (veja o Exemplo 1.69), e g_1^{-1} é linear, visto que g_1 é linear.

2) $H^{g^{-1}} \subseteq H$:

Seja $g \in K$. Logo, $g \in Isom(E)$ e g é linear. Além disso, sendo $a \in E$, queremos mostrar que $g^{-1} \circ T_a \circ g = T_b$, onde $b \in E$. Para isso, basta considerar $b = g^{-1}(a)$ e observar que

$$
\begin{aligned}
& b = g^{-1}(a) \\
\Rightarrow\ & x + b = x + g^{-1}(a) \\
\Rightarrow\ & g(x + b) = g(x + g^{-1}(a)) \\
\Rightarrow\ & g(x) + g(b) = g(x + g^{-1}(a)) \\
\Rightarrow\ & g(x) + a = g(x + g^{-1}(a)) \\
\Rightarrow\ & T_a(g(x)) = g(T_{g^{-1}(a)}(x)) \\
\Rightarrow\ & g^{-1}(T_a(g(x))) = T_{g^{-1}(a)}(x),
\end{aligned}
$$

para todo $x \in E$. Logo, $g^{-1} \circ T_a \circ g = T_b \in H$.

Observe que nas implicações acima utilizamos a linearidade da aplicação g e o fato de que $b = g^{-1}(a)$, ou seja, $g(b) = a$. □

Denotaremos K, dado na proposição anterior, por $IsomL(E)$, ou seja,

$$IsomL(E) = \{g \in Isom(E);\ g \text{ é linear}\}.$$

Como todos os elementos de $IsomL(E)$ são operadores lineares bijetores de E (lembrando que isometrias são aplicações bijetoras), temos que $IsomL(E)$ é um subgrupo de $GL(E)$ (veja o Exemplo 1.42).

3.1.3 Isometrias Lineares da Reta e do Plano

Nesta subseção, estudaremos as isometrias lineares da Reta e do Plano. No caso da Reta, consideraremos apenas a norma euclidiana. No caso do Plano, iremos considerar a norma euclidiana e outra norma, a saber, a norma da soma.

Observação 3.3. *Seja E um espaço vetorial normado e $f : E \longrightarrow E$ um operador linear sobrejetor. São equivalentes:*
i) f é uma isometria.
ii) $|f(v)| = |v|$ para todo $v \in E$.

De fato, supondo (i), temos

$$|v - 0_E| = |f(v) - f(0_E)| \Rightarrow |v| = |f(v)|,$$

para todo $v \in E$, pois $0_E + f(0_E) = f(0_E) = f(0_E + 0_E) = f(0_E) + f(0_E)$, e daí $f(0_E) = 0_E$. Logo, temos (ii).

Reciprocamente, supondo (ii), como $|f(v)| = |v|$ para todo $v \in V$, temos:

$$|f(u - v)| = |u - v| \Rightarrow |f(u) - f(v)| = |u - v|,$$

para quaisquer $u, v \in V$, ou seja, f é uma isometria.

Exemplo 3.4. *(Isometrias Lineares da Reta) Já havíamos mencionado no Exemplo 2.5 que dada $f \in Isom(\mathbb{R})$, temos apenas duas possibilidades para f: $f(x) = x + a$, para todo $x \in \mathbb{R}$, ou $f(x) = -x + a$, para todo $x \in \mathbb{R}$, onde $a = f(0)$. Para que f seja uma isometria linear temos que ter $f(0) = 0 = a$. Portanto, se f for uma isometria linear da reta, temos apenas duas possibilidades para f: $f(x) = x$, para todo $x \in \mathbb{R}$, ou $f(x) = -x$, para todo $x \in \mathbb{R}$.*

Exemplo 3.5. *(Isometrias Lineares do Plano) Consideremos o espaço vetorial real $\mathbb{R}^2$ munido do seu produto interno canônico $\langle , \rangle : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, o qual é definido por*

$$\langle (x_1, y_1), (x_2, y_2) \rangle = x_1x_2 + y_1y_2.$$

Consideremos também a norma usual do $\mathbb{R}^2$: $\|(x, y)\| = \sqrt{x^2 + y^2}$. Esta é exatamente a norma proveniente do produto interno usual. Observe que a métrica induzida por esta norma é exatamente a métrica usual do plano.

Considere o $\mathbb{R}^2$ munido da norma usual (o plano) e seja $f \in IsomL(\mathbb{R}^2)$. Como f é linear, existem a, b, c, $d \in \mathbb{R}$ tais que $f(x, y) = (ax + by, cx + dy)$. Como f é uma isometria, segue da Observação 3.3 que $\|f(v)\| = \|v\|$ e daí $\|f(v)\|^2 = \|v\|^2$, para todo $v \in \mathbb{R}^2$. Logo,

$$(a^2 + c^2)x^2 + 2(ab + cd)xy + (b^2 + d^2)y^2 = x^2 + y^2,$$

para quaisquer x, $y \in \mathbb{R}$. Esta última afirmação equivale a

$$a^2 + c^2 = b^2 + d^2 = 1 \qquad e \qquad ab + cd = 0.$$

Dessa forma, existe $\theta \in \mathbb{R}$ tal que $a = Cos\,\theta$ e $c = Sen\,\theta$. Além disso, $a^2b^2 + c^2b^2 = b^2$ e daí, como $ab = -cd$, vale $c^2 = c^2(b^2 + d^2) = b^2$. Logo, $b = nc$, com $n = \pm 1$, e $d = -na$. Assim, como

$$f(1,0) = (a,c) = (Cos\,\theta, Sen\,\theta)$$

e $f(0,1) = (b,d) = (nSen\,\theta, -nCos\,\theta)$, a matriz de f em relação à base canônica é

$$[f] = \begin{pmatrix} Cos\,\theta & nSen\,\theta \\ Sen\,\theta & -nCos\,\theta \end{pmatrix} \quad , \quad com\ \theta \in \mathbb{R}\ ,\ n = \pm 1.$$

Agora, mostraremos que todos os operadores lineares desta forma são isometrias. Para isso, seja f um operador linear tal que:

$$[f] = \begin{pmatrix} Cos\,\theta & nSen\,\theta \\ Sen\,\theta & -nCos\,\theta \end{pmatrix} \quad , \quad com\ \theta \in \mathbb{R}\ ,\ n = \pm 1.$$

Sendo $(x,y) \in \mathbb{R}^2$, temos $f(x,y) = (ax + by, cx + dy)$ com $a = Cos\,\theta$, $b = nSen\,\theta$, $c = Sen\,\theta$ e $d = -nCos\,\theta$. Logo,

$$||f(x,y)||^2 = (a^2x^2 + 2abxy + b^2y^2) + (c^2x^2 + 2cdxy + d^2y^2) = x^2 + y^2 = ||(x,y)||^2$$

e assim, pela Observação 3.3, f é uma isometria.

Como $\varphi : GL(\mathbb{R}^2) \longrightarrow GL_2(\mathbb{R})$, definida por $\varphi(f) = [f]$, é um isomorfismo (veja Exemplo 1.42) e mostramos que $\varphi(IsomL(\mathbb{R}^2)) = O_2(\mathbb{R})$, onde

$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} Cos\,\theta & nSen\,\theta \\ Sen\,\theta & -nCos\,\theta \end{pmatrix} \,\middle|\, \theta \in \mathbb{R},\ n = \pm 1 \right\}$$

temos que $\varphi|_{IsomL(\mathbb{R}^2)} : IsomL(\mathbb{R}^2) \longrightarrow O_2(\mathbb{R})$ é um isomorfismo. O conjunto $O_2(\mathbb{R})$ é um subgrupo de $GL_2(\mathbb{R})$, chamado de grupo ortogonal de grau 2 sobre $\mathbb{R}$.

Geometricamente, observemos que no grupo $O_2(\mathbb{R})$ temos dois tipos de elementos. Para $n = 1$, temos reflexões enquanto para $n = -1$ temos rotações.

Sabe-se que $\mathbb{C}^* = \mathbb{C} - \{0\}$, munido da multiplicação usual de números complexos, é um grupo (o grupo multiplicativo dos números complexos), e que $C = \{z \in \mathbb{C}\,;\, |z| = 1\}$ é um subgrupo de $\mathbb{C}^*$. Mostra-se que

$$\begin{array}{rccl} \psi : & DC & \longrightarrow & O_2(\mathbb{R}) \\ & (a+bi, n) & \longmapsto & \psi(a+bi,n) = \begin{pmatrix} a & -nb \\ b & na \end{pmatrix} \end{array}$$

é um isomorfismo, onde DC é um caso particular do grupo DG, mencionado no Exemplo 1.10, no qual o grupo G é o grupo C. Daí, temos que $IsomL(\mathbb{R}^2)$ *é isomorfo também ao grupo DC.*

No próximo exemplo mostraremos que o grupo das isometrias lineares do $\mathbb{R}^2$ pode ser isomorfo a outro grupo, diferente do grupo $O_2(\mathbb{R})$, quando consideramos uma norma diferente da usual.

Exemplo 3.6. *Considere agora no espaço vetorial real* $\mathbb{R}^2$ *a norma da soma:* $\|(x,y)\|_s = |x|+|y|$. *Vamos descrever o grupo* $IsomL(\mathbb{R}^2, \|\|_s)$ *das isometrias lineares do espaço vetorial normado* $(\mathbb{R}^2, \|\|_s)$. *Considere*

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Mostra-se que G é um subgrupo de $GL_2(\mathbb{R})$ *isomorfo ao grupo* D_4 *(o grupo diedral 4). Para ver este isomorfismo, basta observar a classificação dos grupos de ordem 8, a qual pode ser encontrada em [6], na Seção VI.5. Se f é um operador linear do* $\mathbb{R}^2$ *tal que* $[f]$ *(matriz de f em relação à base canônica) pertence a G, então* $f \in IsomL(\mathbb{R}^2)$. *Para verificarmos esta afirmação, dividiremos em dois casos.*

1º caso: *Diagonal principal não nula, onde a matriz* $[f]$ *é da forma*

$$[f] = \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \in G,$$

com $n, m \in \{-1, 1\}$. *Daí, sendo* $v = (x, y)$, *temos* $f(v) = (nx, my)$. *Portanto,*

$$||f(v)|| = |nx| + |my| = |n| \cdot |x| + |m| \cdot |y| = |x| + |y| = ||(x,y)|| = ||v||$$

e segue da Observação 3.3 que f é uma isometria.

2º caso: *Diagonal secundária não nula, onde a matriz* $[f]$ *é da forma*

$$[f] = \begin{pmatrix} 0 & n \\ m & 0 \end{pmatrix} \in G,$$

com $n, m \in \{-1, 1\}$. *Daí, sendo* $v = (x, y)$, *temos* $f(v) = (ny, mx)$. *Portanto,*

$$||f(v)|| = |ny| + |mx| = |n| \cdot |y| + |m| \cdot |x| = |y| + |x| = ||(x,y)|| = ||v||$$

e segue da Observação 3.3 que f é uma isometria.

Supondo agora $f \in IsomL(\mathbb{R}^2)$, tomemos a, b, c, $d \in \mathbb{R}$ tais que

$$f(x, y) = (ax + by, cx + dy).$$

Como $\|f(v)\|_s = \|v\|_s$ para todo $v \in \mathbb{R}^2$, considerando particularmente $v_1 = (1, 0)$, $v_2 = (0, 1)$, $v_3 = (1, 1)$ e $v_4 = (1, -1)$, temos as seguintes igualdades:

$$|a| + |c| = |b| + |d| = 1 \quad e \quad |a + b| + |c + d| = |a - b| + |c - d| = 2.$$

Segue destas igualdades que $|a + b| + |c + d| = |a| + |b| + |c| + |d|$, e assim, como $|a + b| \leq |a| + |b|$ e $|c + d| \leq |c| + |d|$, devemos ter

$$|a + b| = |a| + |b| \quad e \quad |c + d| = |c| + |d|$$

e daí $|a - b| \leq |a + b|$ e $|c - d| \leq |c + d|$. Usando agora a igualdade $|a + b| + |c + d| = |a - b| + |c - d|$, concluímos que $|a - b| = |a + b|$ e $|c - d| = |c + d|$, donde segue que a ou b é igual a 0 e c ou d é igual a 0. Se $a = 0$, então $c = \pm 1$, $d = 0$ e $b = \pm 1$ e, portanto $[f] \in G$. Se $b = 0$, então $d = \pm 1$, $c = 0$ e $a = \pm 1$ e, daí $[f] \in G$.

Considerando novamente o isomorfismo $\varphi : GL(\mathbb{R}^2) \longrightarrow GL_2(\mathbb{R})$, mencionado no Exemplo 3.5, temos que $\varphi(IsomL(\mathbb{R}^2), || \ ||_s) = G$, e daí concluímos que $IsomL(\mathbb{R}^2, || \ ||_s)$ é isomorfo a G, e portanto ao grupo D_4.

3.2 Teorema de Mazur-Ulam

Um questionamento que o leitor pode fazer é: Será que existe alguma relação entre as isometrias e as transformações lineares? Primeiramente, note que nem toda transformação linear é uma isometria, e nem toda isometria é uma transformação linear, como veremos nos próximos exemplos.

Exemplo 3.7. *Se considerarmos o plano (o espaço $\mathbb{R}^2$ munido da métrica usual) e a aplicação $T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, definida por $T(x, y) = 2(x, y)$, mostra-se que T é uma transformação linear, porém T não é uma isometria, visto que se considerarmos $(1, 0), (1, 2) \in \mathbb{R}^2$ temos:*

$$|T(1, 0) - T(1, 2)| = |(0, -4)| = 4 \neq 2 = |(0, -2)| = |(1, 0) - (1, 2)|.$$

Exemplo 3.8. *Não necessariamente uma isometria será uma transformação linear como é o caso do Exemplo 1.68. Note que neste caso, g é uma isometria como já foi mostrado. Porém, tomando $a \in E - \{0_E\}$, temos $g(0_E) = a \neq 0_E$ e assim g não é uma transformação linear.*

Veremos agora que sob certas condições se pode garantir que uma isometria é uma transformação linear.

Proposição 3.9. *Seja E um espaço vetorial com produto interno. Se $T : E \longrightarrow E$ é uma isometria tal que $T(0_E) = 0_E$, então T é uma transformação linear.*

Demonstração. Inicialmente iremos mostrar que T preserva produto interno, isto é, $\langle T(u), T(v)\rangle = \langle u, v\rangle$ para quaisquer $u,\ v \in E$. De fato, sendo $u, v \in E$, tem-se:

$$\begin{aligned}|T(u) - T(v)|^2 = |T(u - v)|^2 &= \langle T(u - v), T(u - v)\rangle \\ &= \langle T(u) - T(v), T(u) - T(v)\rangle \\ &= |T(u)|^2 - 2\langle T(u), T(v)\rangle + |T(v)|^2,\end{aligned}$$

onde estamos considerando a norma proveniente do produto interno em questão. Logo,

$$\begin{aligned}|T(u) - T(v)|^2 + 2\langle T(u), T(v)\rangle &= |T(u)|^2 + |T(v)|^2 \\ \Rightarrow \langle T(u), T(v)\rangle &= \frac{1}{2}(|T(u)|^2 + |T(v)|^2 - |T(u - v)|^2).\end{aligned}$$

Como T é uma isometria e $T(0_E) = 0_E$, temos $|T(w)| = |w|$ para todo $w \in E$ e assim

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

Portanto,

$$\langle T(u), T(v)\rangle = \langle u, v\rangle.$$

Agora, mostraremos que $T(au + bv) = aT(u) + bT(v)$ para quaisquer $a, b \in \mathbb{R}$ e $u, v \in E$, ou seja, que T é linear. De fato, como

$$\begin{aligned}|T(au + bv) - aT(u) - bT(v)|^2 &= |T(au + bv)|^2 + a^2|T(u)|^2 + b^2|T(v)|^2 \\ &\quad - 2a\langle T(au + bv), T(u)\rangle \\ &\quad - 2b\langle T(au + bv), T(v)\rangle + 2ab\langle T(u), T(v)\rangle \\ &= |au + bv|^2 + a^2|u|^2 + b^2|v|^2 \\ &\quad - 2a\langle au + bv, u\rangle - 2b\langle au + bv, v\rangle + 2ab\langle u, v\rangle \\ &= |au + bv - au - bv|^2 = 0,\end{aligned}$$

onde na terceira igualdade usamos o fato de que T preserva produto interno, segue que $T(au + bv) - aT(u) - bT(v) = 0_E$.

□

Veremos no próximo exemplo que sem a hipótese de isometria, não conseguiríamos necessariamente concluir que a transformação é linear.

Exemplo 3.10. *Considere a aplicação $T : \mathbb{R} \longrightarrow \mathbb{R}$, definida por $T(x) = x^2$. De fato, nesta aplicação temos $T(0) = 0$, porém se considerarmos $\alpha = 2$ e $x = 3$, temos:*

$$T(\alpha x) = T(2 \cdot 3) = (2 \cdot 3)^2 = 36 \neq 18 = 2 \cdot 3^2 = \alpha x^2 = \alpha T(x).$$

Portanto, T não é linear e não é difícil de verificar que T não é uma isometria.

O próximo passo será dá uma demonstração de um teorema que generaliza a Proposição 3.9, visto que neste teorema retiramos a hipótese de produto interno. Mas antes de demonstrá-lo, precisaremos dos seguintes lemas.

Lema 3.11. *Sejam X e X' dois espaços vetoriais normados sobre os reais e $T : X \longrightarrow X'$ uma isometria tal que $T(x + y) = T(x) + T(y)$ para quaisquer $x, y \in X$. Então $T(\alpha x) = \alpha T(x)$ para quaisquer $\alpha \in \mathbb{R}$ e $x \in X$.*

Demonstração. Dividiremos essa demonstração em quatro passos:

1 Passo: $T(nx) = nT(x)$, $\forall n \in \mathbb{N} \cup \{0\}$.

Esse passo será demonstrado por indução. Como

$$T(0_X) = T(0_X + 0_X) = T(0_X) + T(0_X),$$

temos $T(0_X) = 0_X$ e assim temos o caso $n = 0$. O caso $n = 1$ é imediato. Suponha que $T(nx) = nT(x)$, para algum $n \in \mathbb{N}$. Queremos mostrar que $T((n + 1)x) = (n + 1)T(x)$. Com efeito,

$$T((n + 1)x) = T(nx + x) = T(nx) + T(x),$$

visto que por hipótese $T(x+y) = T(x)+T(y)$, para quaisquer $x, y \in X$. Por hipótese de indução $T(nx) = nT(x)$, então

$$T(nx) + T(x) = nT(x) + T(x) = (n + 1)T(x).$$

Assim, $T((n + 1)x) = (n + 1)T(x)$ e portanto $T(nx) = nT(x)$, para todo $n \in \mathbb{N}$.

2 Passo: $T(px) = pT(x)$, $\forall p \in \mathbb{Z}$.

Mostremos agora o caso $p = -1$. Como $T(0_X) = 0_X$, temos:

$$\begin{aligned} &T(x + (-x)) = 0 \\ \Rightarrow &T(x) + T(-x) = 0 \\ \Rightarrow &T(-x) = -T(x), \end{aligned}$$

para todo $x \in X$. Se p for um número inteiro negativo diferente de -1, note que $p = -|p|$ e assim

$$T(px) = T(-|p|x) = -T(|p|x),$$

onde essa última igualdade segue do fato que $T(-x) = -T(x)$, para todo $x \in X$. Mas segue do 1 Passo que $-T(|p|x) = -|p|T(x)$. Daí,

$$T(px) = T(-|p|x) = -T(|p|x) = -|p|T(x) = pT(x).$$

Logo, unindo o 1 e o 2 Passo temos $T(px) = pT(x)$, para todo $p \in \mathbb{Z}$.

3 Passo: $T(rx) = rT(x)$, $\forall r \in \mathbb{Q}$.

De fato, considere $r = \dfrac{p}{q}$, com $p, q \in \mathbb{Z}$ e $q > 0$. Logo,

$$T(rx) = T\left(\frac{p}{q}x\right) = pT\left(\frac{1}{q}x\right),$$

onde a última igualdade segue do 2 Passo. Mas

$$pT\left(\frac{1}{q}x\right) = \frac{p}{q}qT\left(\frac{1}{q}x\right) = \frac{p}{q}T(x) = rT(x).$$

Assim, $T(rx) = rT(x)$ para todo $r \in \mathbb{Q}$.

4 Passo: $T(\alpha x) = \alpha T(x)$, $\forall \alpha \in \mathbb{R}$.

Fixado $\alpha \in \mathbb{R}$, seja $(r_n)_{n\in\mathbb{N}}$ um sequência de números racionais convergindo para α. Segue do Exemplo 1.60 e da Proposição 1.62 que $\alpha x = lim\, r_n x$, e daí

$$T(\alpha x) = T(lim\, r_n x) = lim\, T(r_n x),$$

pois T é contínua, já que é isometria (aqui novamente usamos a Proposição 1.62). Segue do 3 Passo que $limT(r_n x) = lim\, r_n T(x)$ e portanto

$$T(\alpha x) = lim\, T(r_n x) = lim\, r_n T(x) = \alpha T(x),$$

sendo a última igualdade consequência do Exemplo 1.60 e da Proposição 1.62. □

Lema 3.12. *Seja o diâmetro de A_n o número real:*

$$diam(A_n) = sup\{d(x, y)\,;\, x, y \in A_n\}.$$

Sejam M um espaço métrico e $A_1 \supseteq A_2 \supseteq A_3 \supseteq \ldots$ subconjuntos limitados tais que $\bigcap_{n=1}^{\infty} A_n$ é não vazia e $lim_{n\to\infty} diam(A_n) = 0$. Então, $\bigcap_{n=1}^{\infty} A_n$ é um conjunto unitário.

Demonstração. Sejam $a, b \in \bigcap_{n=1}^{\infty} A_n$. Dessa forma, $a, b \in A_n$, para todo $n \in \mathbb{N}$. Logo, $d(a,b) \leq diam(A_n)$, para todo $n \in \mathbb{N}$, e assim

$$0 \leq d(a,b) \leq lim_{n\to\infty} diam(A_n) = 0.$$

Daí $d(a,b) = 0$, e portanto $a = b$.

□

Observação 3.13. *Observe que o Lema 3.12 é um resultado muito similar ao* ***Teorema dos Intervalos Encaixantes****. Enquanto que no Lema 3.12, não temos a hipótese de subconjuntos fechados e temos as hipóteses que a* $\bigcap_{n=1}^{\infty} A_n$ *é não vazia e* $lim_{n\to\infty} diam(A_n) = 0$*, no* ***Teorema dos Intervalos Encaixantes*** *temos as hipóteses de subconjuntos fechados e limitados.*

Teorema 3.14. *(Mazur-Ulam) Sejam* X *e* X' *dois espaços vetoriais normados sobre os reais e* $T : X \longrightarrow X'$ *uma isometria tal que* $T(0_X) = 0_{X'}$*. Então* T *é linear.*

Demonstração. Fixemos $x, y \in X$ um par de pontos e consideremos z o ponto médio:

$$z = \frac{x+y}{2}\ .$$

O ponto z satisfaz

$$|x - z| = \left|x - \frac{x+y}{2}\right| = \frac{|x-y|}{2} = \left|y - \frac{x+y}{2}\right| = |y - z|.$$

Denotemos por A o conjunto de todos os pontos $u \in X$ que satisfaçam

$$|x - u| = |y - u| = \frac{|x-y|}{2} \qquad (I)$$

Afirmamos que o conjunto A é simétrico com relação ao ponto z, isto é, se $u \in A$, então $2z - u \in A$. De fato, note que $2z = x + y$ e assim

$$(2z - u) - x = x + y - u - x = y - u$$

$$e$$

$$(2z - u) - y = x + y - u - y = x - u.$$

Como $u \in A$, segue de (I) que

$$|(2z - u) - x| = |y - u| = \frac{|x-y|}{2} = |x - u| = |(2z - u) - y|.$$

Logo, $2z - u \in A$ e portanto A é simétrico com relação ao ponto z.

Segue de (I) que A é limitado. Como A é simétrico com relação a z, então $u, 2z-u \in A$ para todo $u \in A$. Portanto, pela definição de diâmetro, temos $2|z-u| = |2z-u-u| \leq diam(A)$ para todo $u \in A$, e daí

$$|z-u| \leq \frac{1}{2} diam(A) \quad , \quad \forall\ u \in A.$$

Denotemos por A_1 o conjunto de todos os pontos $p \in A$ que satisfaçam

$$|p-u| \leq \frac{1}{2} diam(A) \quad , \quad \forall\ u \in A. \qquad (II)$$

Afirmamos que o conjunto A_1 também é simétrico com relação ao ponto z, ou seja, se $p \in A_1$, então $2z-p \in A_1$. De fato, para todo $u \in A$ temos

$$(2z-p)-u = (2z-u)-p$$

e daí $|(2z-p)-u| = |(2z-u)-p|$. Como $2z-u \in A$, desde que $u \in A$, segue de (II) que

$$|(2z-p)-u| = |(2z-u)-p| \leq \frac{1}{2} diam(A).$$

Segue de (II) que o diâmetro de A_1 não excede a metade do diâmetro de A, pois $|u_1 - p| \leq (1/2) diam(A)$ para quaisquer u_1, $p \in A_1$, uma vez que (por construção) todo elemento de A_1 está em A.

Partindo agora de A_1, podemos construir

$$A_2 = \{p \in A_1;\ |p-u| \leq (1/2) diam(A_1),\ \forall\ u \in A_1\} \qquad (III)$$

e usar o que foi feito anteriormente para mostrar que $z \in A_2$, A_2 é simétrico com relação a z e $diam(A_2) \leq (1/2) diam(A_1)$.

Podemos repetir essa construção e obter uma sequência de conjuntos encaixados $A \supseteq A_1 \supseteq A_2 \supseteq \ldots$, todos contendo o ponto z, todos simétricos com relação a z e com os diâmetros satisfazendo:

$$diam(A_{n+1}) \leq \frac{1}{2} diam(A_n). \qquad (IV)$$

Como $diam(A_n) \geq 0$ (por definição) e $diam(A_n) \leq \frac{1}{2^n} diam(A)$ para todo $n \in \mathbb{N}$ (o que prova-se por indução, utilizando (IV)), temos

$$0 \leq d_{A_n} \leq \frac{1}{2^n} d_A. \qquad (V)$$

Como $lim\ \dfrac{1}{2^n} d_A = 0$, utilizando o Teorema do Confronto em (V), concluímos que $diam(A_n)$ tende para zero. Mas, se $diam(A_n)$ tende para zero, pelo Lema 3.12 concluímos que a interseção de todos os conjuntos A_n é apenas o ponto z.

Tomando agora em X' os elementos

$$x' = T(x)\ ,\ y' = T(y) \quad \text{e} \quad z' = (x' + y')/2$$

denotemos por A', A'_1, ..., A'_n, ... os conjuntos definidos a partir de x' e y', análogos àqueles definidos em X. De modo análogo, mostramos que a interseção de todos os conjuntos A'_n é apenas o ponto z'.

Observando a condição (I), que define o conjunto A, e a condição análoga envolvendo x' e y', que define o conjunto A', concluímos que $T(A) \subseteq A'$ e $T^{-1}(A') \subseteq A$, já que T e T^{-1} são isometrias. Logo, $T(A) = A'$ e $diam(A) = diam(A')$. Ademais, observando a condição (II), que define o conjunto A_1, e a condição análoga envolvendo x' e y', que define o conjunto A'_1, concluímos que $T(A_1) = A'_1$ e daí $diam(A_1) = diam(A'_1)$. Indutivamente, temos $T(A_n) = A'_n$ para todo $n \in \mathbb{N}$. Como T é bijetora, segue que T leva a interseção dos A_n na interseção dos A'_n. Como estas interseções são, respectivamente, $\dfrac{x+y}{2}$ e $\dfrac{x'+y'}{2}$, tem-se

$$T\left(\frac{x+y}{2}\right) = \frac{x'+y'}{2} = \frac{T(x)}{2} + \frac{T(y)}{2}\ . \qquad (VI)$$

Considerando $y = 0_X$ e usando a hipótese que $T(0_X) = 0_{X'}$, concluímos que $T\left(\dfrac{x}{2}\right) = \dfrac{T(x)}{2}$. Tomando então u, $v \in X$, $x = 2u$ e $y = 2v$, e aplicando (VI), temos:

$$T(u+v) = T\left(\frac{x+y}{2}\right) = T\left(\frac{x}{2}\right) + T\left(\frac{y}{2}\right) = T(u) + T(v).$$

Isto mostra a primeira condição da linearidade. A segunda condição da linearidade segue do Lema 3.11.

□

Uma das consequências do *Teorema de Mazur-Ulam* é o corolário que apresentaremos a seguir. O resultado que será apresentado neste corolário é muito importante, pois descreve a estrutura algébrica do grupo das isometrias de um espaço vetorial real normado, em termos das translações e isometrias lineares.

Corolário 3.15. *Considere o subgrupo* $H = \{T_a\,;\, a \in E\}$ *de* $Isom(E)$ *(mencionado na Proposição 3.1) e o seguinte conjunto*

$$N = \{f \in Isom(E)\,;\, f(0_E) = 0_E\}.$$

Temos $N = IsomL(E)$ *e* $Isom(E) = HN$.

Demonstração. Como toda transformação linear tem o vetor nulo como ponto fixo, tem-se $IsomL(E) \subseteq N$. A inclusão contrária é consequência imediata do Teorema de Mazur-Ulam.

Suponha agora que $g \in Isom(E)$ e definamos as seguintes aplicações:

$$\begin{array}{rccl} f: & E & \longrightarrow & E \\ & x & \longmapsto & f(x) = g(x) - g(0_E) \end{array}$$

e

$$\begin{array}{rccl} T_{g(0_E)}: & E & \longrightarrow & E \\ & x & \longmapsto & T_{g(0_E)}(x) = x + g(0_E). \end{array}$$

Observe que a aplicação f pertence a N e a aplicação $T_{g(0_E)}$ pertence a H. Para ver que $f \in N$, basta observar que é uma isometria (uma vez que g é) e $f(0_E) = 0_E$. Como

$$\begin{aligned} & f(x) = g(x) - g(0_E) \\ \Rightarrow\ & g(x) = f(x) + g(0_E) \\ \Rightarrow\ & g(x) = (T_{g(0_E)} \circ f)(x), \end{aligned}$$

para todo $x \in E$. Assim, $g \in HN$ e portanto $Isom(E) = HN$. □

Para encerrar, vamos ver o grupo de isometrias $Isom(E)$ como um produto semidireto de N por H. De fato, temos:

i) $Isom(E) = HN = NH$

Sejam G um grupo e H e N subgrupos de G. Quando falamos no Capítulo 1 sobre o produto de subgrupos HN, mencionamos que:

$$HN \text{ é subgrupo de } G \Longleftrightarrow HN = NH.$$

Como pelo Corolário anterior temos $Isom(E) = HN$, concluímos que HN é um subgrupo, e portanto $HN = NH$.

ii) $H \cap N = \{Id_E\}$

Para ver isso, considere $h \in H \cap N$. Dessa forma,

$$\begin{array}{rccl} h = T_a: & E & \longrightarrow & E \\ & x & \longmapsto & T_a(x) = x + a \end{array}$$

para algum $a \in E$, e $h(0_E) = 0_E$. Logo, $h(0_E) = 0_E + a = 0_E$, e portanto $a = 0_E$. Então,

$$\begin{array}{rccl} h = T_{0_E}: & E & \longrightarrow & E \\ & x & \longmapsto & T_{0_E}(x) = x + 0_E = x, \end{array}$$

e assim $h = T_{0_E} = Id_E$.

iii) $H \trianglelefteq Isom(E)$

Como $Isom(E) = HN$, então, sendo $g \in Isom(E)$, temos $g = \phi \circ T_c$, onde $\phi \in N$ e $T_c \in H$. Queremos mostrar que $H^g \subseteq H$, para toda $g \in Isom(E)$. Sendo assim, para $a \in E$, arbitrário, considere a seguinte aplicação

$$\begin{array}{rccl} T_{\phi(a)}: & E & \longrightarrow & E \\ & x & \longmapsto & T_{\phi(a)}(x) = x + \phi(a). \end{array}$$

Observe que $T_{\phi(a)} \in H$. Ademais, temos:

$$\begin{aligned} (g \circ T_a \circ g^{-1})(x) &= (\phi \circ T_c \circ T_a \circ (\phi \circ T_c)^{-1})(x) \\ &= (\phi \circ T_c \circ T_a \circ T_c^{-1} \circ \phi^{-1})(x) \\ &= (\phi \circ T_a \circ T_c \circ T_c^{-1} \circ \phi^{-1})(x) \\ &= \phi(T_a(\phi^{-1}(x))) \\ &= \phi(\phi^{-1}(x) + a) \\ &= \phi(\phi^{-1}(x)) + \phi(a) \\ &= x + \phi(a) \\ &= T_{\phi(a)}(x), \end{aligned}$$

para todo $x \in E$. Na terceira igualdade acima, utilizamos o fato que os elementos de H comutam. Posteriormente, utilizamos o fato da aplicação ϕ ser linear, pois $\phi \in N$.

Referências Bibliográficas

[1] ALBERTSON, M. O, BOUTIN, D. L. *Realizing Finite Groups in Euclidean Space*. J. Algebra 225, 947-956 (2000).

[2] ASIMOV, D. *Finite Groups as Isometry Groups*. Transactions of the American Mathematical Society. Volume 216, 389-391 (1976).

[3] BARTLE, R. G. *The Elements of Real Analysis*. 2ª Edição. John Wiley & Sons, Inc , 1976.

[4] COELHO, F. U. , LOURENÇO, M. L. *Um Curso de Álgebra Linear*. EDUSP, São Paulo, 2001.

[5] FRALEIGH, J. B. *A First Course in Abstract Algebra*. 6ª Edição. New York: Addison-Wesley, 2000.

[6] GARCIA, A. , LEQUAIN, Y. *Elementos de Álgebra*. 6ª Edição. IMPA, 2018.

[7] GONÇALVES, A. *Introdução à Álgebra*. 2ª Edição. Rio de Janeiro: Projeto Euclides, IMPA, 2003.

[8] LIMA, E. L. *Espaços Métricos*. 2ª Edição. Rio de Janeiro: Projeto Euclides, IMPA, 1983.

[9] LIMA, E. L. *Álgebra Linear*. 1ª Edição. Rio de Janeiro: IMPA, 2014.

[10] LIMA, E. L. *Curso de Análise - Vol 1*. 11ª Edição. Rio de Janeiro: IMPA, 2015.

[11] LIMA, E. L. *Curso de Análise - Vol 2*. 11ª Edição. Rio de Janeiro: IMPA, 2015.

[12] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura*. 2ª Edição. Campina Grande: EDUEPB, 2015.