ISOMETRIAS DE $\mathbb{R}^n$

1. Transformações

Seja Ω um conjunto. Uma aplicação $f : \Omega \to \Omega$ chama-se uma *transformação* de Ω. A transformação f é dita *injetiva* se $f(v) = f(w)$ implica $v = w$ para todo $v, w \in \Omega$; f chama-se *sobrejetiva* se para todo $w \in \Omega$ existe $v \in \Omega$ tal que $f(v) = w$. A transformação f chama-se *bijetiva* ou *invertível* se ela é injetiva e sobrejetiva. Se f é uma transformação invertível, então existe a sua inversa $f^{-1} : \Omega \to \Omega$ definida pela regra que $f(v) = w$ se e somente se $f^{-1}(w) = v$ para todo $v, w \in \Omega$.

As transformações de Ω podem ser compostas. Se $f, g : \Omega \to \Omega$ então $f \circ g : \Omega \to \Omega$ é definida como $(f \circ g)(v) = f(g(v))$ para todo $v \in \Omega$. A composição de transformações é associativa no sentido que $(f \circ g) \circ h = f \circ (g \circ h)$ para todo $f, g, h : \Omega \to \Omega$.

Nós vamos estudar principalmente as transformações do plano $\mathbb{R}^2$ e o espaço $\mathbb{R}^3$.

Exemplo 1. Todo conjunto Ω tem a transformação identidade $\mathrm{id}_\Omega : \Omega \to \Omega$, $v \mapsto v$ para todo $v \in \Omega$. Se $f : \Omega \to \Omega$ é uma transformação invertível, então $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_\Omega$.

Exemplo 2. Seja $\Omega = \mathbb{R}^n$ com $n \geq 1$. Uma transformação $T : \mathbb{R}^n \to \mathbb{R}^n$ é dita linear se

$$T(\alpha v + \beta w) = \alpha T(v) + \beta T(w)$$

para todo $v, w \in \mathbb{R}^n$ e $\alpha, \beta \in \mathbb{R}$. Transformações lineares são estudadas em álgebra linear. Uma transformação linear $T : \mathbb{R}^n \to \mathbb{R}^n$ é invertível se e somente se

$$\ker T = \{v \in \mathbb{R}^n \mid T(v) = 0\} = \{0\}.$$

Exemplo 3. Seja $t \in \mathbb{R}^n$ e considere a transformação $T_t : \mathbb{R}^n \to \mathbb{R}^n$ definido como

$$T_t(v) = v + t.$$

A transformação T_t é chamado *a translação de* $\mathbb{R}^n$ pelo vetor t. Note que se $t \neq 0$, então T_t não é linear, pois $T_t(0) = t \neq 0$. A transformação T_t é invertível e $T_t^{-1} = T_{-t}$.

2. Grupos

Seja G um conjunto não vazio com uma operação que pode ser denotada por $\cdot$ (ou por $+$, ou simplesmente por concatenação). Isso quer dizer que com cada par de elementos $a, b \in G$ associamos um elemento $a \cdot b \in G$. O conjunto G considerado com a operação $\cdot$ é dito *grupo* se as seguintes propriedades estão válidas para todo $a, b, c \in G$.

(1) A operação $\cdot$ é associativa; ou seja $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
(2) Existe identidade $1 \in G$ tal que $1 \cdot a = a \cdot 1 = a$.
(3) Todo elemento $a \in G$ possui inverso a^{-1} que satisfaz $a \cdot a^{-1} = a^{-1}a = 1$.

Um grupo G é dito *abeliano* ou *comutativo* se $ab = ba$ para todo $a, b \in G$.

Exemplo 4. O conjunto $\mathbb{Z}$ dos inteiros é um grupo abeliano com a operação de adição. A mesma coisa vale para $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Se V é um espaço vetorial, então V é um grupo abeliano com a operação de adição.

Nós vamos considerar dois tipos de grupos, nomeadamente grupos de transformações e grupos de matrizes.

Exemplo 5. Seja $n \geq 1$, e seja G um conjunto não vazio de matrizes invertíveis $n \times n$ tal que G é fechado para multiplicação e se $X \in G$, então $X^{-1} \in G$. Então G é um grupo com a multiplicação matricial. Um tal grupo G é chamado um *grupo de matrizes* ou *grupo matricial.* Os primeiros exemplos de grupos matriciails são

$$\begin{aligned} \mathrm{GL}_n &= \{X \text{ é matriz } n \times n \mid X \text{ é invertível}\} \\ \mathrm{SL}_n &= \{X \in \mathrm{GL}_n \mid \det X = 1\}. \end{aligned}$$

Os conjuntos GL_n e SL_n são grupos. É óbvio que $\mathrm{SL}_n \subseteq \mathrm{GL}_n$ e neste caso dizemos que SL_n é um subgrupo de GL_n e escrevemos que $\mathrm{SL}_n \leq \mathrm{GL}_n$.

Exemplo 6. Seja G um conjunto de transformações invertíveis de um conjunto Ω tal que G é fechado para a composição e $T^{-1} \in G$ sempre quando $T \in G$. Neste caso G é um grupo. Tal grupo chama-se um *grupo de transformações.* Por exemplo seja $\Omega = V$ um espaço vetorial de dimensão finita e considere

$$\begin{aligned} \mathrm{Sym}(V) &= \{f : V \to V \mid f \text{ é invertível}\} \\ \mathrm{GL}(V) &= \{T \in \mathrm{Sym}(V) \mid T \text{ é linear}\} \\ \mathrm{SL}(V) &= \{T \in \mathrm{GL}(V) \mid \det T = 1\}. \end{aligned}$$

O conjunto $\mathcal{T}(V) = \{T_t \mid t \in V\}$ de um espaço vetorial V é um grupo pois $T_{t_1} \circ T_{t_2} = T_{t_1+t_2}$ e $T_t^{-1} = T_{-t}$ (ou seja este conjunto é fechado para a composição e para os inversos). Como

$$T_{t_1} \circ T_{t_2} = T_{t_1+t_2} = T_{t_2+t_1} = T_{t_2} \circ T_{t_1},$$

temos que $\mathcal{T}(V)$ é um grupo abeliano.

Lema 7. *Seja $t \in V$ e $X \in GL(V)$. Então $XT_tX^{-1} = T_{X(t)}$.*

Demonstração. Seja $v \in V$ e computemos que

$$XT_tX^{-1}(v) = XT_t(X^{-1}(v)) = X(X^{-1}(v) + t) = v + X(t) = T_{X(t)}(v).$$

$\square$

Teorema 8. *Assuma que G é um subgrupo de transformações de $GL(V)$ e seja $\mathcal{T}$ o grupo de translações. Então o produto $\mathcal{T}G = \{T_tX \mid t \in V,\ X \in G\}$ é um subgrupo de $Sym(V)$.*

Demonstração. Seja Y o conjunto de produtos no enunciado do teorema. Precisamos provar que Y é fechado para a composição e para tomar inversos. Sejam $T_{t_1}X_1$ e $T_{t_2}X_2$. Então temos que

$$(T_{t_1}X_1)(T_{t_2}X_2) = T_{t_1}X_1T_{t_2}(X_1^{-1}X_1)X_2 = T_{t_1}(X_1T_{t_2}X_1^{-1})X_1X_2 = (T_{t_1}T_{X_1(t_2)})(X_1X_2) \in Y.$$

Além disso, temos que

$$(T_t X)^{-1} = X^{-1}T_t^{-1} = X^{-1}T_{-t} = X^{-1}T_{-t}XX^{-1} = T_{X^{-1}(-t)}X^{-1} \in Y.$$

□

3. Isometrias de $\mathbb{R}^n$

Considere o espaço $\mathbb{R}^n$. Lembre que o produto escalar (ou produto interno) de dois vetores $v = (\alpha_1, \ldots, \alpha_n)$ e $w = (\beta_1, \ldots, \beta_n)$ é definido como

$$v \cdot w = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n.$$

O produto escalar pode ser escrito usando multiplicação matricial como

$$v \cdot w = vw^t.$$

Usando o produto escalar, podemos definir a norma $\|v\|$ de um vetor $v \in \mathbb{R}^n$ como

$$\|v\| = \sqrt{v \cdot v}.$$

A distância entre dois vetores $v, w \in \mathbb{R}^n$ pode ser definida como

$$d(v, w) = \|v - w\|.$$

Alêm disso, o cosseno do ângulo ϑ entre v e w é definido como

$$\cos\vartheta = \frac{v \cdot w}{\|v\|\|w\|}$$

Dois vetores $v, w \in \mathbb{R}^n$ são ortogonais se e somente se $v \cdot w = 0$.

Da definição da norma fica clara que a norma está determinada pelo produto escalar. De acrodo do lema seguinte, a norma determina o produto escalar.

Teorema 9 (Identidade de polarização)**.** *Sejam $v, w \in \mathbb{R}^n$, então*

$$v \cdot w = \frac{1}{2}\left(\|v + w\| - \|v\| - \|w\|\right).$$

Demonstração. Exercício. □

Uma transformação $T : \mathbb{R}^n \to \mathbb{R}^n$ que preserva distância (ou seja $d(T(v), T(w)) = d(v, w)$ para todo $v, w \in \mathbb{R}^n$) chama-se *isometria* de $\mathbb{R}^n$. Se T é uma isometria e $T(v) = T(w)$, então

$$0 = d(T(v), T(w)) = d(v, w);$$

ou seja $v = w$. Isso implica que uma isometria é necessáriamente injetiva. Vamos ver que isometrias são também sobrejetivas, mas neste momento esta afirmação não é tão fácil de provar. Por outro lado, se $T : \mathbb{R}^n \to \mathbb{R}^n$ é uma isometria *linear*, então ela é injetiva e precisa ser sobrejetiva. Logo, as isometrias lineares são invertíveis.

Exemplo 10. A translação $T_t : \mathbb{R}^n \to \mathbb{R}^n$ é uma isometria para todo $t \in \mathbb{R}^n$. De fato, temos para $v, w \in \mathbb{R}^n$ que

$$d(v + t, w + t) = \|v + t - (w + t)\| = \|v - w\| = d(v, w).$$

4. O grupo ortogonal

Teorema 11. *Seja $T : \mathbb{R}^n \to \mathbb{R}^n$ uma transformação linear. As seguintes são equivalentes para T.*

1. *T preserva o produto escalar; ou seja $T(v) \cdot T(w) = v \cdot w$ para todo $v, w \in \mathbb{R}^n$.*
2. *T preserva a norma; ou seja $\|T(v)\| = \|v\|$ para todo $v \in \mathbb{R}^n$;*
3. *T preserva a distância $d(T(v), T(w)) = d(v, w)$ para todo $v, w \in \mathbb{R}^n$.*

Demonstração. O fato que (1) implica (2) e que (2) implica (3) segue das definições da norma e da distância. O fato que (3) implica (1) segue dos fatos que $\|v\| = d(v, 0)$, $T(0) = 0$ (T sendo linear) e da identidade de polarização. □

Uma transformação linear $T : \mathbb{R}^n \to \mathbb{R}^n$ chama se *ortogonal* se T satisfaz uma (e então todas) das propriedades no teorema anterior. Por definição, as transformações ortogonais são exatamente as isometrias lineares do espaço $\mathbb{R}^n$. Lembre que uma matriz X é dita ortogonal se $X^t X = I$.

Teorema 12. *As seguintes afirmações são verdadeiras.*

1. *As transformações ortogonais formam um subgrupo de $GL(V)$.*
2. *Uma transformação $T : \mathbb{R}^n \to \mathbb{R}^n$ é ortogonal se e somente se sua matriz na base canônica é ortogonal.*
3. *O determinante de uma transformação ortogonal é ± 1.*

Demonstração. (1) Pode mostrar com uma conta direta que a composição de duas transformações ortogonais é ortogonal e o inverso de uma transformação ortogonal é também ortogonal.

(2) Se $T : \mathbb{R}^n \to \mathbb{R}^n$ é uma isometria linear, então T preserva a norma de vetores e o ângulo entre vetores. Como os vetores $e_1, \ldots, e_n$ na base canônica formam um sistema ortonormal, os vetores $T(e_1), \ldots, T(e_n)$ também formam um sistema ortonormal. Isso quer dizer que $[T]_B^B$ é uma matriz ortogonal.

Assuma agora que $T : \mathbb{R}^n \to \mathbb{R}^n$ é uma transformação linear tal que a sua matriz X na base canônica é ortogonal. Sejam $v, w \in \mathbb{R}^n$. Então

$$v \cdot w = vw^t = vX^t X w^t = (Xv^t)^t (Xw^t) = (Xv) \cdot (Xw) = T(v) \cdot T(w).$$

Ou seja, T preserva produto escalar e T é uma isometria.

(3) Seja $T : \mathbb{R}^n \to \mathbb{R}^n$ uma isometria. Temos que $\det T = \det X$ onde X é a matriz de T na base canônica. Como X é uma matriz ortogonal, temos que

$$1 = \det I = \det(X^t X) = \det(X^t) \det X = (\det X)^2$$

e segue que $\det T = \det X = \pm 1$. □

O grupo das transformações ortogonais de $\mathbb{R}^n$ é denotado por $O(\mathbb{R}^n)$. O subgrupo das transformações ortogonais com determinante 1 é denotado por $SO(\mathbb{R}^n)$. Os grupos $O(\mathbb{R}^n)$ e $SO(\mathbb{R}^n)$ são chamados *grupo ortogonal* e *grupo especial ortogonal*. Os elementos de $SO(\mathbb{R}^n)$ são chamadas de *rotações* enquanto os demais elementos de $O(\mathbb{R}^n)$ são chamadas de *reflexões*.

Lema 13. *Seja $T : \mathbb{R}^n \to \mathbb{R}^n$ uma transformação tal que $T(0) = 0$. T é uma isometria se e somente se T preserva o produto interno (ou seja, $T(u) \cdot T(v) = u \cdot v$).*

Demonstração. Assuma primeiro que T é uma isometria. Sejam $u, v \in \mathbb{R}^n$. Então

$$\|T(u) - T(v)\| = d(T(u), T(v)) = d(u, v) = \|u - v\|.$$

Note que, tomando $v = 0$, isso implica que

$$\|T(u)\| = \|u\|,$$

ou seja, T preserva norma. Ora,

$$\|T(u) - T(v)\|^2 = \|u - v\|^2$$

e assim

$$(T(u) - T(v)) \cdot (T(u) - T(v)) = (u - v) \cdot (u - v).$$

Agora segue que

$$\|T(u)\|^2 + \|T(v)\|^2 - 2T(u) \cdot T(v) = \|u\|^2 + \|v\|^2 - 2(u, v).$$

Considerando que $\|T(v)\| = \|v\|$ e $\|T(u)\| = \|u\|$, obtemos que

$$T(v) \cdot T(u) = u \cdot v.$$

Vice versa, assuma que T preserve a produto interno. Então

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

Logo $d(T(u), T(v)) = d(u, v)$ e d é uma isometria. □

Corolário 14. *Seja $T : \mathbb{R}^n \to \mathbb{R}^n$ uma isometria tal que $T(0) = 0$. Então T é linear e consequentemente T é uma transformação ortogonal.*

Demonstração. Primeiro provaremos que $T(\alpha v) = \alpha T(v)$ para todo $v \in \mathbb{R}^n$. Pelo lema anterior, T preserva o produto interno, e assim

$$\begin{aligned} \|T(\alpha v) - \alpha T(v)\|^2 &= (T(\alpha v) - \alpha T(v)) \cdot (T(\alpha v) - \alpha T(v)) \\ &= T(\alpha v) \cdot T(\alpha v) - 2\alpha T(\alpha v) \cdot T(v) + \alpha^2 T(v) \cdot T(v) \\ &= (\alpha v) \cdot (\alpha v) - 2\alpha(\alpha v) \cdot v + \alpha^2 v \cdot v = 0. \end{aligned}$$

Ou seja $\|T(\alpha v) - \alpha T(v)\| = 0$ que implica que $T(\alpha v) - \alpha T(v) = 0$ e que $T(\alpha v) = \alpha T(v)$.

Provaremos agora, para todo $u, v \in \mathbb{R}^n$, que $T(u+v) = T(u) + T(v)$. Usamos um argumento similar e calculamos que

$$\begin{aligned}
\|T(u+v) - T(u) - T(v)\|^2 &= (T(u+v) - T(u) - T(v)) \cdot (T(u+v) - T(u) - T(v)) \\
&= T(u+v) \cdot T(u+v) + T(u) \cdot T(u) + T(v) \cdot T(v) \\
&- 2T(u+v) \cdot T(u) - 2T(u+v) \cdot T(v) - 2T(u) \cdot T(v) \\
&= (u+v) \cdot (u+v) + v \cdot v + u \cdot u \\
&- 2(u+v) \cdot u - 2(u+v) \cdot v - 2u \cdot v \\
&= ((u+v) - u - v) \cdot ((u+v) - u - v) = 0 \cdot 0 = 0.
\end{aligned}$$

Logo $T(u+v) - T(u) - T(v) = 0$; ou seja, $T(u+v) = T(u) + T(v)$. □

Corolário 15. *Assuma que $T : \mathbb{R}^n = \mathbb{R}^n$ é uma isometria. Então $T = T_t \circ X$ onde T é uma translação e $X : \mathbb{R}^n \to \mathbb{R}^n$ é ortogonal (em particular, X é linear).*

Demonstração. Assuma que $T(0) = t$. Então $X = T_{-t} \circ T$ é uma isometria tal que $X(0) = 0$. Pelo corolário anterior, $X : \mathbb{R}^n \to \mathbb{R}^n$ é ortogonal (e linear). Ora notamos que $T = T_t \circ X$. □

Corolário 16. *Qualquer isometria $T : \mathbb{R}^n \to \mathbb{R}^n$ é invertível.*