# ISOMETRIES OF $\mathbf{R}^n$

KEITH CONRAD

## 1. Introduction

An *isometry* of $\mathbf{R}^n$ is a function $h\colon \mathbf{R}^n \to \mathbf{R}^n$ that preserves the distance between vectors:

$$||h(v) - h(w)|| = ||v - w||$$

for all $v$ and $w$ in $\mathbf{R}^n$, where $||(x_1, \ldots, x_n)|| = \sqrt{x_1^2 + \cdots + x_n^2}$.

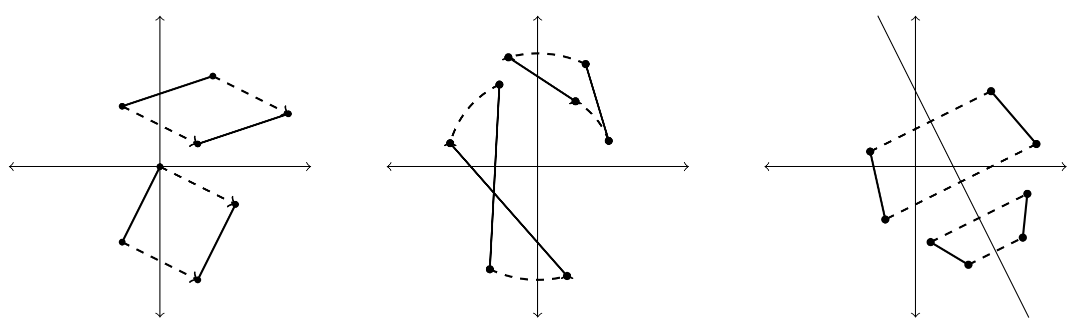
**Example 1.1.** The identity transformation: $\mathrm{id}(v) = v$ for all $v \in \mathbf{R}^n$.

**Example 1.2.** Negation: $-\mathrm{id}(v) = -v$ for all $v \in \mathbf{R}^n$.

**Example 1.3.** Translation: fixing $u \in \mathbf{R}^n$, let $t_u(v) = v + u$. Easily $||t_u(v) - t_u(w)|| = ||v - w||$.

**Example 1.4.** Rotations around points and reflections across lines in the plane are isometries of $\mathbf{R}^2$. Formulas for these isometries will be given in Example 3.3 and Section 4.

The effects of a translation, rotation (around the origin) and reflection across a line in $\mathbf{R}^2$ are pictured below on sample line segments.



The composition of two isometries of $\mathbf{R}^n$ is an isometry. Is every isometry invertible? It is clear that the three kinds of isometries pictured above (translations, rotations, reflections) are each invertible (translate by the negative vector, rotate by the opposite angle, reflect a second time across the same line).

In Section 2, we show the close link between isometries and the dot product on $\mathbf{R}^n$, which is more convenient to use than distances due to its algebraic properties. Section 3 is about the matrices that act as isometries on on $\mathbf{R}^n$, called orthogonal matrices. Section 4 describes the isometries of $\mathbf{R}$ and $\mathbf{R}^2$ geometrically. In Appendix A, we will look more closely at reflections in $\mathbf{R}^n$.

## 2. Isometries, dot products, and linearity

Using translations, we can reduce the study of isometries of $\mathbf{R}^n$ to the case of isometries fixing $\mathbf{0}$.

**Theorem 2.1.** *Every isometry of $\mathbf{R}^n$ can be uniquely written as the composition $t \circ k$ where $t$ is a translation and $k$ is an isometry fixing the origin.*

*Proof.* Let $h\colon \mathbf{R}^n \to \mathbf{R}^n$ be an isometry. If $h = t_w \circ k$, where $t_w$ is translation by a vector $w$ and $k$ is an isometry fixing $\mathbf{0}$, then for all $v$ in $\mathbf{R}^n$ we have $h(v) = t_w(k(v)) = k(v) + w$. Setting $v = \mathbf{0}$ we get $w = h(\mathbf{0})$, so $w$ is determined by $h$. Then $k(v) = h(v) - w = h(v) - h(\mathbf{0})$, so $k$ is determined by $h$. Turning this around, if we define $t(v) = v + h(\mathbf{0})$ and $k(v) = h(v) - h(\mathbf{0})$, then $t$ is a translation, $k$ is an isometry fixing $\mathbf{0}$, and $h(v) = k(v) + h(\mathbf{0}) = t_w \circ k$, where $w = h(\mathbf{0})$. $\square$

**Theorem 2.2.** *For a function $h\colon \mathbf{R}^n \to \mathbf{R}^n$, the following are equivalent:*

(1) *$h$ is an isometry and $h(\mathbf{0}) = \mathbf{0}$,*
(2) *$h$ preserves dot products: $h(v) \cdot h(w) = v \cdot w$ for all $v, w \in \mathbf{R}^n$.*

*Proof.* The link between length and dot product is the formula

$$||v||^2 = v \cdot v.$$

Suppose $h$ satisfies (1). Then for any vectors $v$ and $w$ in $\mathbf{R}^n$,

$$||h(v) - h(w)|| = ||v - w||. \tag{2.1}$$

As a special case, when $w = \mathbf{0}$ in (2.1) we get $||h(v)|| = ||v||$ for all $v \in \mathbf{R}^n$. Squaring both sides of (2.1) and writing the result in terms of dot products makes it

$$(h(v) - h(w)) \cdot (h(v) - h(w)) = (v - w) \cdot (v - w).$$

Carrying out the multiplication,

$$h(v) \cdot h(v) - 2h(v) \cdot h(w) + h(w) \cdot h(w) = v \cdot v - 2v \cdot w + w \cdot w. \tag{2.2}$$

The first term on the left side of (2.2) equals $||h(v)||^2 = ||v||^2 = v \cdot v$ and the last term on the left side of (2.2) equals $||h(w)||^2 = ||w||^2 = w \cdot w$. Canceling equal terms on both sides of (2.2), we obtain $-2h(v) \cdot h(w) = -2v \cdot w$, so $h(v) \cdot h(w) = v \cdot w$.

Now assume $h$ satisfies (2), so

$$h(v) \cdot h(w) = v \cdot w \tag{2.3}$$

for all $v$ and $w$ in $\mathbf{R}^n$. Therefore

$$\begin{aligned} ||h(v) - h(w)||^2 &= (h(v) - h(w)) \cdot (h(v) - h(w)) \\ &= h(v) \cdot h(v) - 2h(v) \cdot h(w) + h(w) \cdot h(w) \\ &= v \cdot v - 2v \cdot w + w \cdot w \quad \text{by (2.3)} \\ &= (v - w) \cdot (v - w) \\ &= ||v - w||^2, \end{aligned}$$

so $||h(v) - h(w)|| = ||v - w||$. Thus $h$ is an isometry. Setting $v = w = \mathbf{0}$ in (2.3), we get $||h(\mathbf{0})||^2 = 0$, so $h(\mathbf{0}) = \mathbf{0}$. $\square$

**Corollary 2.3.** *The only isometry of $\mathbf{R}^n$ fixing $\mathbf{0}$ and the standard basis is the identity.*

*Proof.* Let $h\colon \mathbf{R}^n \to \mathbf{R}^n$ be an isometry that satisfies

$$h(\mathbf{0}) = \mathbf{0},\ h(e_1) = e_1,\ \ldots,\ h(e_n) = e_n.$$

Theorem 2.2 says

$$h(v) \cdot h(w) = v \cdot w$$

for all $v$ and $w$ in $\mathbf{R}^n$. Fix $v \in \mathbf{R}^n$ and let $w$ run over the standard basis vectors $e_1, e_2, \ldots, e_n$, so we see

$$h(v) \cdot h(e_i) = v \cdot e_i.$$

Since $h$ fixes each $e_i$,

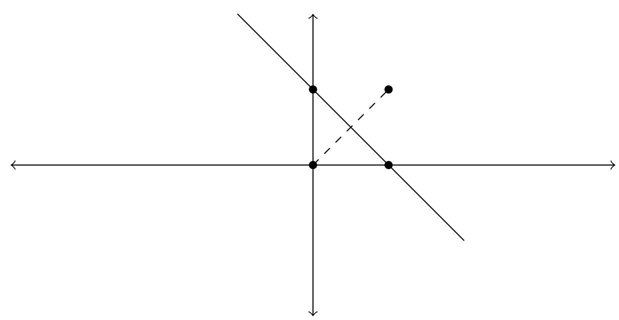
$$h(v) \cdot e_i = v \cdot e_i.$$

Writing $v = c_1e_1 + \cdots + c_ne_n$, we get

$$h(v) \cdot e_i = c_i$$

for all $i$, so $h(v) = c_1e_1 + \cdots + c_ne_n = v$. As $v$ was arbitrary, $h$ is the identity on $\mathbf{R}^n$. $\square$

It is essential in Corollary 2.3 that the isometry fixes $\mathbf{0}$. An isometry of $\mathbf{R}^n$ fixing the standard basis *without* fixing $\mathbf{0}$ need not be the identity! For example, reflection across the line $x + y = 1$ in $\mathbf{R}^2$ is an isometry of $\mathbf{R}^2$ fixing $(1, 0)$ and $(0, 1)$ but not $\mathbf{0} = (0, 0)$. See below.



**Theorem 2.4.** *For a function $h\colon \mathbf{R}^n \to \mathbf{R}^n$, the following are equivalent:*

(1) *$h$ is an isometry and $h(\mathbf{0}) = \mathbf{0}$,*
(2) *$h$ is linear, and the matrix $A$ such that $h(v) = Av$ for all $v \in \mathbf{R}^n$ satisfies $AA^\top = I_n$.*

*Proof.* Suppose $h$ is an isometry and $h(\mathbf{0}) = \mathbf{0}$. We want to prove linearity: $h(v + w) = h(v) + h(w)$ and $h(cv) = ch(v)$ for all $v$ and $w$ in $\mathbf{R}^n$ and all $c \in \mathbf{R}$. The mapping $h$ preserves dot products by Theorem 2.2:

$$h(v) \cdot h(w) = v \cdot w$$

for all $v$ and $w$ in $\mathbf{R}^n$. For the standard basis $e_1, \ldots, e_n$ of $\mathbf{R}^n$ this says $h(e_i) \cdot h(e_j) = e_i \cdot e_j = \delta_{ij}$, so $h(e_1), \ldots, h(e_n)$ is an orthonormal basis of $\mathbf{R}^n$. Thus two vectors in $\mathbf{R}^n$ are equal if they have the same dot product with each of $h(e_1), \ldots, h(e_n)$.

For all $u$ in $\mathbf{R}^n$ we have

$$h(v + w) \cdot h(u) = (v + w) \cdot u$$

and

$$(h(v) + h(w)) \cdot h(u) = h(v) \cdot h(u) + h(w) \cdot h(u) = v \cdot u + w \cdot u = (v + w) \cdot u,$$

so $h(v+w) \cdot h(u) = (h(v)+h(w)) \cdot h(u)$ for all $u$. Letting $u = e_1, \ldots, e_n$ shows $h(v+w) = h(v)+h(w)$. Similarly,

$$h(cv) \cdot h(u) = (cv) \cdot u = c(v \cdot u) = c(h(v) \cdot h(u)) = (ch(v)) \cdot h(u),$$

so again letting $u$ run through $e_1, \ldots, e_n$ tells us $h(cv) = ch(v)$. Thus $h$ is linear.

Let $A$ be the matrix for $h$: $h(v) = Av$ for all $v \in \mathbf{R}^n$, where $A$ has $j$th column $h(e_j)$. We want to show $AA^\top = I_n$. Since $h$ preserves dot products, the condition $h(v) \cdot h(w) = v \cdot w$ for all $v, w \in \mathbf{R}^n$ says $Av \cdot Aw = v \cdot w$. The fundamental link between the dot product and matrix transposes, which you should check, is that we can move a matrix to the other side of a dot product by using its transpose:

$$v \cdot Mw = M^\top v \cdot w \tag{2.4}$$

for every $n \times n$ matrix $M$ and $v, w \in \mathbf{R}^n$. Using $M = A$ and $Av$ in place of $v$ in (2.4),

$$Av \cdot Aw = A^\top(Av) \cdot w = (A^\top A)v \cdot w.$$

This is equal to $v \cdot w$ for all $v$ and $w$, so $(A^\top A)v \cdot w = v \cdot w$ for all $v$ and $w$ in $\mathbf{R}^n$. Since the $(i,j)$ entry of a matrix $M$ is $Me_j \cdot e_i$, letting $v$ and $w$ run through the standard basis of $\mathbf{R}^n$ tells us $A^\top A = I_n$, so $A$ is invertible. An invertible matrix commutes with its inverse, so $A^\top A = I_n \Rightarrow AA^\top = I_n$.

For the converse, assume $h(v) = Av$ for $v \in \mathbf{R}^n$ where $AA^\top = I_n$. Trivially $h$ fixes $\mathbf{0}$. To show $h$ is an isometry, by Theorem 2.2 it suffices to show

$$Av \cdot Aw = v \cdot w \tag{2.5}$$

for all $v, w \in \mathbf{R}^n$. Since $A$ and its inverse $A^\top$ commute, we have $A^\top A = I_n$, so $Av \cdot Aw = A^\top(Av) \cdot w = (A^\top A)v \cdot w = v \cdot w$. $\square$

**Corollary 2.5.** *Isometries of $\mathbf{R}^n$ are invertible, the inverse of an isometry is an isometry, and two isometries on $\mathbf{R}^n$ that have the same values at $\mathbf{0}$ and any basis of $\mathbf{R}^n$ are equal.*

This gives a second proof of Corollary 2.3 as a special case.

*Proof.* Let $h\colon \mathbf{R}^n \to \mathbf{R}^n$ be an isometry. By Theorem 2.1, $h = k + h(\mathbf{0})$ where $k$ is an isometry of $\mathbf{R}^n$ fixing $\mathbf{0}$. Theorem 2.4 tells us there is an invertible matrix $A$ such that $k(v) = Av$ for all $v \in \mathbf{R}^n$, so

$$h(v) = Av + h(\mathbf{0}).$$

This has inverse $h^{-1}(v) = A^{-1}(v - h(\mathbf{0}))$. In particular, $h$ is surjective.

The isometry condition $||h(v) - h(w)|| = ||v - w||$ for all $v$ and $w$ in $\mathbf{R}^n$ implies $||v - w|| = ||h^{-1}(v) - h^{-1}(w)||$ for all $v$ and $w$ in $\mathbf{R}^n$ by replacing $v$ and $w$ in the isometry condition with $h^{-1}(v)$ and $h^{-1}(w)$. Thus $h^{-1}$ is an isometry of $\mathbf{R}^n$.

If $h_1$ and $h_2$ are isometries of $\mathbf{R}^n$ that are equal on $\mathbf{0}$ and a basis then the functions $k_1(v) = h_1(v) - h_1(\mathbf{0})$ and $k_2(v) = h_2(v) - h_2(\mathbf{0})$ are linear and are equal on that basis, so by linearity $k_1 = k_2$ on $\mathbf{R}^n$. That is, $h_1(v) - h_1(\mathbf{0}) = h_2(v) - h_2(\mathbf{0})$ for all $v$ in $\mathbf{R}^n$. Since $h_1(\mathbf{0}) = h_2(\mathbf{0})$ we get $h_1 = h_2$ on $\mathbf{R}^n$. $\square$

**Remark 2.6.** That isometries of $\mathbf{R}^n$ fixing $\mathbf{0}$ are linear and invertible is a special case of the following more general result: for a finite-dimensional vector space $V$ over an arbitrary field and a nondegenerate bilinear form $B$ on $V$, a function $A\colon V \to V$ for which $B(v,w) = B(A(v), A(w))$ for all $v$ and $w$ in $V$ must be linear and invertible. A more general version of this is due to A. Vogt [3, Lemma 1.5, Theorem 2.4], and a proof can be found there or in my answer at `https://math.stackexchange.com/questions/137139`. A physically interesting example of this over $\mathbf{R}$ besides $\mathbf{R}^n$ with its usual dot product is 4-dimensional space $(x, y, z, ct)$ with the indefinite bilinear form associated to $x^2+y^2+z^2-c^2t^2$ in special relativity (Minkowski spacetime).

**Definition 2.7.** In $\mathbf{R}^n$, a set of $n+1$ points $P_0, P_1, \ldots, P_n$ is said to be in *general position* if they don't all lie in a hyperplane.

This concept abstracts the idea of 3 points in $\mathbf{R}^2$ not being collinear. In the definition, the hyperplanes in $\mathbf{R}^n$ are translated subspaces of dimension $n-1$, so they need not pass through the origin. For example, a line in $\mathbf{R}^2$ need not be a linear subspace of $\mathbf{R}^2$ since a line doesn't have to contain the origin. Three points in $\mathbf{R}^2$ are in general position if no line passes through all of them and four points in $\mathbf{R}^3$ are in general position if no plane passes through all of them. Saying $P_0, P_1, \ldots, P_n$ are in general position in $\mathbf{R}^n$ does not mean these $n+1$ points are linearly independent as vectors in $\mathbf{R}^n$, but rather that the $n$ *differences* $P_1 - P_0, \ldots, P_n - P_0$ are linearly independent vectors: a nontrivial linear relation would place these $n$ differences, along with $\mathbf{0}$, in a common subspace of dimension $n-1$, so adding $P_0$ to all of the differences and to $\mathbf{0}$ would put $P_0, P_1, \ldots, P_n$ in a common hyperplane.

Adding a common vector to points in general position keeps them in general position since the added vector cancels out when taking differences.

**Corollary 2.8.** *Let $P_0, P_1, \ldots, P_n$ be $n+1$ points in $\mathbf{R}^n$ in "general position". Two isometries of $\mathbf{R}^n$ that are equal at $P_0, \ldots, P_n$ are the same.*

*Proof.* We know isometries of $\mathbf{R}^n$ are invertible. If $h_1$ and $h_2$ are isometries of $\mathbf{R}^n$ with the same values at each $P_i$ then $h_2^{-1} \circ h_1$ is an isometry that fixes each $P_i$. Therefore to prove $h_1 = h_2$ it suffices to show an isometry of $\mathbf{R}^n$ that fixes $P_0, \ldots, P_n$ is the identity.

Let $h$ be an isometry of $\mathbf{R}^n$ such that $h(P_i) = P_i$ for $0 \leq i \leq n$. Set $t(v) = v - P_0$, which is a translation. Then $tht^{-1}$ is an isometry with formula

$$(tht^{-1})(v) = h(v + P_0) - P_0.$$

Thus $(tht^{-1})(\mathbf{0}) = h(P_0) - P_0 = \mathbf{0}$, so $tht^{-1}$ is linear by Theorem 2.4. Also $(tht^{-1})(P_i - P_0) = h(P_i) - P_0 = P_i - P_0$.

Since $P_0, \ldots, P_n$ are in general position, the differences $P_1 - P_0, \ldots, P_n - P_0$ form a basis of $\mathbf{R}^n$. Therefore by Corollary 2.5, $tht^{-1}$ is the identity, so $h$ is the identity. $\square$

## 3. Orthogonal matrices

We have seen that the isometries of $\mathbf{R}^n$ that fix $\mathbf{0}$ come from matrices $A$ such that $AA^\top = I_n$. These matrices have a name.

**Definition 3.1.** An $n \times n$ matrix $A$ is called *orthogonal* if $AA^\top = I_n$, or equivalently if $A^\top A = I_n$.

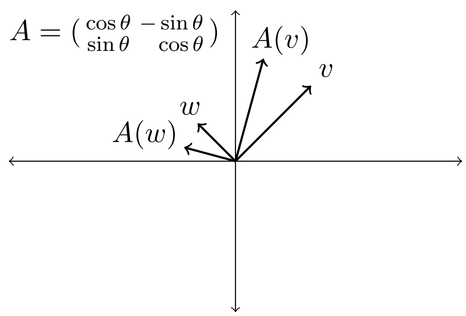
A matrix is orthogonal when its transpose is its inverse. Since $\det(A^\top) = \det A$, an orthogonal matrix $A$ satisfies $(\det A)^2 = 1$, so $\det A = \pm 1$. (For $n \geq 2$ not all matrices with determinant $\pm 1$ are orthogonal, such as $\left(\begin{smallmatrix} 3 & 1 \\ 5 & 2 \end{smallmatrix}\right)$. The orthogonal $1 \times 1$ matrices are $\pm 1$.)

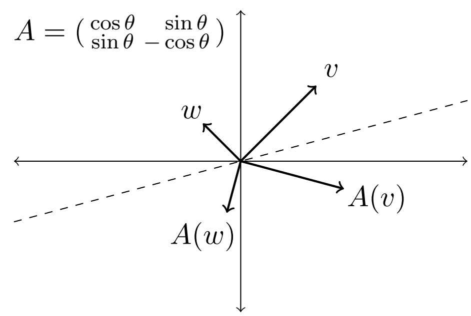
**Example 3.2.** Negation on $\mathbf{R}^n$ (Example 1.2) is an isometry that is described by the matrix $-I_n$, which is orthogonal: $(-I_n)(-I_n)^\top = (-I_n)(-I_n) = I_n$.

**Example 3.3.** Let $n = 2$. By algebra, $AA^\top = I_2$ if and only if $A = \left(\begin{smallmatrix} a & -\varepsilon b \\ b & \varepsilon a \end{smallmatrix}\right)$, where $a^2+b^2 = 1$ and $\varepsilon = \pm 1$. Writing $a = \cos\theta$ and $b = \sin\theta$, we get the matrices $\left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ and

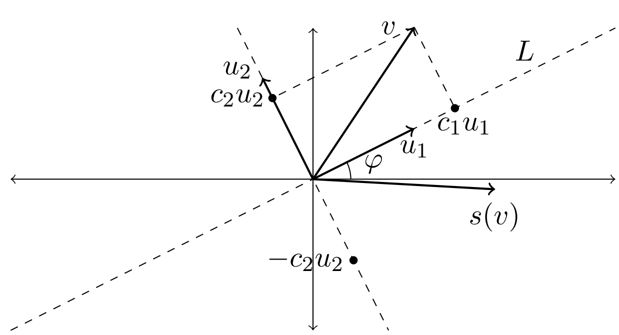
$\left(\begin{smallmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{smallmatrix}\right)$. Algebraically, these types of matrices are distinguished by their determinants: the first type has determinant 1 and the second type has determinant $-1$.

The geometric effects of these two types of matrices differ. Below on the left, $\left(\begin{smallmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{smallmatrix}\right)$ is a counterclockwise rotation by angle $\theta$ around the origin. Below on the right, $\left(\begin{smallmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{smallmatrix}\right)$ is a reflection across the line through the origin at angle $\theta/2$ with respect to the positive $x$-axis. (Check $\left(\begin{smallmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{smallmatrix}\right)$ squares to the identity, as any reflection should.)




Let's explain why $\left(\begin{smallmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{smallmatrix}\right)$ is a reflection at angle $\theta/2$. See the figure below. Pick a line $L$ through the origin, say at an angle $\varphi$ with respect to the positive $x$-axis. To find a formula for reflection across $L$, we'll use a basis of $\mathbf{R}^2$ with one vector **on** $L$ and the other vector **perpendicular** to $L$. The unit vector $u_1 = \binom{\cos\varphi}{\sin\varphi}$ lies on $L$ and the unit vector $u_2 = \binom{-\sin\varphi}{\cos\varphi}$ is perpendicular to $L$. For any $v \in \mathbf{R}^2$, write $v = c_1u_1 + c_2u_2$ with $c_1, c_2 \in \mathbf{R}$.




The reflection of $v$ across $L$ is $s(v) = c_1u_1 - c_2u_2$. Writing $a = \cos\varphi$ and $b = \sin\varphi$ (so $a^2 + b^2 = 1$), in standard coordinates this becomes

$$v = c_1u_1 + c_2u_2 = c_1\binom{a}{b} + c_2\binom{-b}{a} = \begin{pmatrix} c_1a - c_2b \\ c_1b + c_2a \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \tag{3.1}$$

and in a similar way

$$\begin{aligned} s(v) &= c_1u_1 - c_2u_2 \\ &= \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} v \quad \text{by (3.1)} \\ &= \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} v \\ &= \begin{pmatrix} a^2 - b^2 & 2ab \\ 2ab & -(a^2 - b^2) \end{pmatrix} v. \end{aligned}$$

By the sine and cosine duplication formulas, the last matrix is $\left(\begin{smallmatrix} \cos(2\varphi) & \sin(2\varphi) \\ \sin(2\varphi) & -\cos(2\varphi) \end{smallmatrix}\right)$. Therefore $\left(\begin{smallmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{smallmatrix}\right)$ is a reflection across the line through the origin at angle $\theta/2$.

We return to orthogonal $n \times n$ matrices for any $n \geq 1$. The geometric meaning of the condition $A^\top A = I_n$ is that the columns of $A$ are mutually perpendicular unit vectors (check!). From this we see how to create orthogonal matrices: starting with an orthonormal basis of $\mathbf{R}^n$, an $n \times n$ matrix having this basis as its columns (in any order) is an orthogonal matrix, and all $n \times n$ orthogonal matrices arise in this way.

Let $\mathrm{O}_n(\mathbf{R})$ denote the set of $n \times n$ orthogonal matrices:

$$\mathrm{O}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) : AA^\top = I_n\}. \tag{3.2}$$

**Theorem 3.4.** *The set* $\mathrm{O}_n(\mathbf{R})$ *is a group under matrix multiplication.*

*Proof.* Clearly $I_n \in \mathrm{O}_n(\mathbf{R})$. If $A$ and $B$ are in $\mathrm{O}_n(\mathbf{R})$, then

$$(AB)(AB)^\top = ABB^\top A^\top = AA^\top = I_n,$$

so $AB \in \mathrm{O}_n(\mathbf{R})$. For $A \in \mathrm{O}_n(\mathbf{R})$, we have $A^{-1} = A^\top$ and

$$(A^{-1})(A^{-1})^\top = A^\top (A^\top)^\top = A^\top A = I_n.$$

Therefore $A^{-1} \in \mathrm{O}_n(\mathbf{R})$. $\square$

The link between isometries and dot products (Theorem 2.2) gives us a more geometric description of $\mathrm{O}_n(\mathbf{R})$ than (3.2):

$$\mathrm{O}_n(\mathbf{R}) = \{A \in \mathrm{GL}_n(\mathbf{R}) : Av \cdot Aw = v \cdot w \text{ for all } v, w \in \mathbf{R}^n\}. \tag{3.3}$$

The label "orthogonal matrix" is very unfortunate. It suggests that such matrices should be the ones that preserve orthogonality of vectors:

$$v \cdot w = 0 \Longrightarrow Av \cdot Aw = 0 \tag{3.4}$$

for all $v$ and $w$ in $\mathbf{R}^n$. While orthogonal matrices *do* satisfy (3.4), since (3.4) is a special case of the condition $Av \cdot Aw = v \cdot w$ in (3.3), many matrices satisfy (3.4) and are not orthogonal matrices! That is, orthogonal matrices (which, by definition, preserve *all* dot products) are not the only matrices that preserve orthogonality of vectors (dot products equal to 0). A simple example of a nonorthogonal matrix satisfying (3.4) is a scalar matrix $cI_n$, where $c \neq \pm 1$. Since $(cv) \cdot (cw) = c^2(v \cdot w)$, $cI_n$ does not preserve dot products in general but it does preserve dot products equal to 0. It's natural to ask which matrices besides orthogonal matrices preserve orthogonality. Here is the complete answer, which shows they are not that far from being orthogonal.

**Theorem 3.5.** *An $n \times n$ real matrix $A$ satisfies (3.4) if and only if $A$ is a scalar multiple of an orthogonal matrix.*

*Proof.* If $A = cA'$ where $A'$ is orthogonal, then $Av \cdot Aw = c^2(A'v \cdot A'w) = c^2(v \cdot w)$, so if $v \cdot w = 0$ then $Av \cdot Aw = 0$.

Now assume $A$ satisfies (3.4). Then the vectors $Ae_1, \dots, Ae_n$ are mutually perpendicular, so the columns of $A$ are perpendicular to each other. We want to show that they have the same length.

Note that $e_i + e_j \perp e_i - e_j$ when $i \neq j$, so by (3.4) and linearity $Ae_i + Ae_j \perp Ae_i - Ae_j$. Writing this in the form $(Ae_i + Ae_j) \cdot (Ae_i - Ae_j) = 0$ and expanding, we are left with $Ae_i \cdot Ae_i = Ae_j \cdot Ae_j$, so $||Ae_i|| = ||Ae_j||$. Therefore the columns of $A$ are mutually perpendicular vectors with the same length. Call this common length $c$. If $c = 0$ then $A = O = 0 \cdot I_n$. If $c \neq 0$ then the matrix $(1/c)A$ has an orthonormal basis as its columns, so it is an orthogonal matrix. Therefore $A = c((1/c)A)$ is a scalar multiple of an orthogonal matrix. $\square$

Since a composition of isometries is an isometry and isometries are invertible with the inverse of an isometry being an isometry, isometries form a group under composition. We will describe the elements of this group and show how the group law looks in that description.

**Theorem 3.6.** *For $A \in \mathrm{O}_n(\mathbf{R})$ and $w \in \mathbf{R}^n$, the function $h_{A,w} \colon \mathbf{R}^n \to \mathbf{R}^n$ given by*

$$h_{A,w}(v) = Av + w = (t_w A)(v)$$

*is an isometry. Moreover, every isometry of $\mathbf{R}^n$ has this form for unique $A$ and $w$.*

*Proof.* The indicated formula always gives an isometry, since it is the composition of a translation and orthogonal matrix transformation, which are both isometries.

To show every isometry of $\mathbf{R}^n$ has the form $h_{A,w}$ for some $A$ and $w$, let $h \colon \mathbf{R}^n \to \mathbf{R}^n$ be an isometry. By Theorem 2.1, $h = k + h(\mathbf{0})$ where $k$ is an isometry of $\mathbf{R}^n$ fixing $\mathbf{0}$. Theorem 2.4 tells us there is an $A \in \mathrm{O}_n(\mathbf{R})$ such that $k(v) = Av$ for all $v \in \mathbf{R}^n$, so

$$h(v) = k(v) + h(\mathbf{0}) = Av + h(\mathbf{0}) = h_{A,w}(v),$$

where $w = h(\mathbf{0})$.

If $h_{A,w} = h_{A',w'}$ as functions on $\mathbf{R}^n$, then evaluating both sides at $\mathbf{0}$ gives $w = w'$. Therefore $Av + w = A'v + w$ for all $v$, so $Av = A'v$ for all $v$, which implies $A = A'$. $\square$

Let $\mathrm{Iso}(\mathbf{R}^n)$ denote the group of isometries of $\mathbf{R}^n$. Its elements have the form $h_{A,w}$ by Theorem 3.6. Here is what composition of such mappings looks like:

$$\begin{aligned} h_{A,w}(h_{A',w'}(v)) &= A(A'v + w') + w \\ &= AA'v + Aw' + w \\ &= h_{AA',Aw'+w}(v). \end{aligned}$$

This is similar to the multiplication law in the $ax + b$ group:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' + b \\ 0 & 1 \end{pmatrix}.$$

In fact, if we write an isometry $h_{A,w} \in \mathrm{Iso}(\mathbf{R}^n)$ as an $(n+1) \times (n+1)$ matrix $\left(\begin{smallmatrix} A & w \\ 0 & 1 \end{smallmatrix}\right)$, where the 0 in the bottom is a row vector of $n$ zeros, then the composition law in $\mathrm{Iso}(\mathbf{R}^n)$ is multiplication of the corresponding $(n+1)\times(n+1)$ matrices, so $\mathrm{Iso}(\mathbf{R}^n)$ can be viewed as a subgroup of $\mathrm{GL}_{n+1}(\mathbf{R})$, acting on $\mathbf{R}^n$ as the column vectors $\binom{v}{1}$ in $\mathbf{R}^{n+1}$ (not a subspace!).

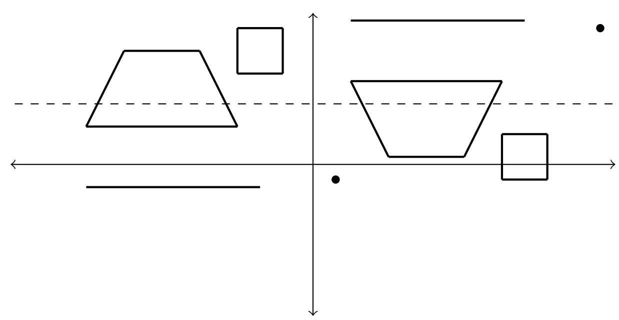
## 4. Geometric description of isometries of $\mathbf{R}$ and $\mathbf{R}^2$

Let's classify the isometries of $\mathbf{R}^n$ for $n = 1$ and $n = 2$.

Since $\mathrm{O}_1(\mathbf{R}) = \{\pm 1\}$, the isometries of $\mathbf{R}$ are the functions $h(x) = x+c$ and $h(x) = -x+c$ for $c \in \mathbf{R}$. (Of course, this case can be worked out easily without the earlier material.)

Now consider isometries of $\mathbf{R}^2$. Write an isometry $h \in \mathrm{Iso}(\mathbf{R}^2)$ as $h(v) = Av + w$ with $A \in \mathrm{O}_2(\mathbf{R})$ and $w \in \mathbf{R}^2$. By Example 3.3, $A$ is a rotation or reflection, depending on $\det A$.

There turn out to be four possibilities for $h$: translations, rotations, reflections, and glide reflections. A *glide reflection* is the composition of a reflection and a nonzero translation in a direction parallel to the line of reflection. A picture of a glide reflection is in the figure below, where the (horizontal) line of reflection is dashed and the translation is a movement to the right.



The image above, which includes "before" and "after" states, suggests a physical interpretation of a glide reflection: it is the result of turning the plane in space like a half-turn of a screw. A more picturesque image, suggested to me by Michiel Vermeulen, is the effect of successive steps with a left foot and then a right foot in the sand or snow (if your feet are mirror reflections).

The possibilities for isometries of $f$ are collected in Table 1 below. It describes how the type of an isometry $h$ is determined by $\det A$ and the geometry of the set of fixed points of $h$ (solutions to $h(v) = v$): empty, a point, a line, or the plane. (The only isometry belonging to more than one of the four possibilities is the identity, which is both a translation and a rotation, so we make the identity its own row in the table.) The table also shows how a description of the fixed points can be obtained algebraically from $A$ and $w$.

| Isometry | Condition | Fixed pts |
|---|---|---|
| Identity | $A = I_2, w = 0$ | $\mathbf{R}^2$ |
| Nonzero Translation | $A = I_2, w \neq 0$ | $\emptyset$ |
| Nonzero Rotation | $\det A = 1, A \neq I_2$ | $(I_2 - A)^{-1}w$ |
| Reflection | $\det A = -1,\ Aw = -w$ | $w/2 + \ker(A - I_2)$ |
| Glide Reflection | $\det A = -1,\ Aw \neq -w$ | $\emptyset$ |

Table 1. Isometries of $\mathbf{R}^2$: $h(v) = Av + w$, $A \in \mathrm{O}_2(\mathbf{R})$.

To justify the information in the table we move down the middle column. The first two rows are obvious, so we start with the third row.

Row 3: Suppose $\det A = 1$ and $A \neq I_2$, so $A = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$ for some $\theta$ and $\cos\theta \neq 1$. We want to show $h$ is a rotation. First of all, $h$ has a unique fixed point: $v = Av + w$ precisely when $w = (I_2 - A)v$. We have $\det(I_2 - A) = 2(1 - \cos\theta) \neq 0$, so $I_2 - A$ is invertible and $p = (I_2 - A)^{-1}w$ is the fixed point of $h$. Then $w = (I_2 - A)p = p - Ap$, so

$$h(v) = Av + (p - Ap) = A(v - p) + p. \tag{4.1}$$

Since $A$ is a rotation by $\theta$ around the origin, (4.1) shows $h$ is a rotation by $\theta$ around $P$.

Rows 4, 5: Suppose $\det A = -1$, so $A = \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{smallmatrix}\right)$ for some $\theta$ and $A^2 = I_2$. We again look at fixed points of $h$. As before, $h(v) = v$ for some $v$ if and only if $w = (I_2 - A)v$. But unlike the previous case, now $\det(I_2 - A) = 0$ (check!), so $I_2 - A$ is not invertible and therefore $w$ may or may not be in the image of $I_2 - A$. When $w$ is in the image of $I_2 - A$, we will see that $h$ is a reflection. When $w$ is not in the image of $I_2 - A$, we will see that $h$ is a glide reflection.

Suppose the isometry $h(v) = Av + w$ with $\det A = -1$ has a fixed point. Then $w/2$ must be a fixed point. Indeed, let $p$ be any fixed point, so $p = Ap + w$. Since $A^2 = I_2$,

$$Aw = A(p - Ap) = Ap - p = -w,$$

so

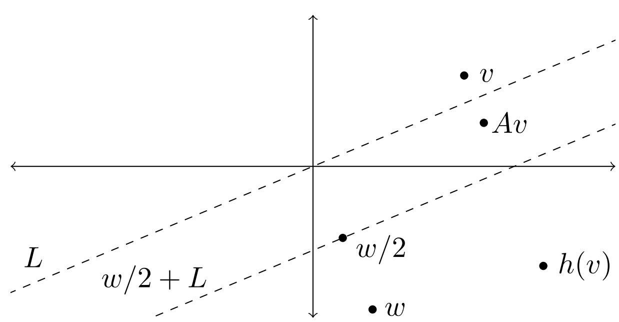
$$h\left(\frac{w}{2}\right) = A\left(\frac{w}{2}\right) + w = \frac{1}{2}Aw + w = \frac{w}{2}.$$

Conversely, if $h(w/2) = w/2$ then $A(w/2) + w = w/2$,, so $Aw = -w$.

Thus $h$ has a fixed point if and only if $Aw = -w$, in which case

$$h(v) = Av + w = A\left(v - \frac{w}{2}\right) + \frac{w}{2}. \tag{4.2}$$

Since $A$ is a reflection across some line $L$ through 0, (4.2) says $h$ is a reflection across the parallel line $w/2 + L$ passing through $w/2$. See the figure below. (Algebraically, we can say $L = \{v : Av = v\} = \ker(A - I_2)$. Since $A - I_2$ is not invertible and not identically 0, its kernel really is 1-dimensional.)




Now assume $h$ has no fixed point, so $Aw \neq -w$. We will show $h$ is a glide reflection. (The formula $h = Av + w$ shows $h$ is the composition of a reflection and a nonzero translation, but $w$ need not be parallel to the line of reflection of $A$, which is $\ker(A - I_2)$, so this formula for $h$ does *not* show directly that $h$ is a glide reflection.) We will now take stronger advantage of the fact that $A^2 = I_2$.

Since $O = A^2 - I_2 = (A - I_2)(A + I_2)$ and $A \neq \pm I_2$ (after all, $\det A = -1$), $A + I_2$ and $A - I_2$ are not invertible. Therefore the subspaces

$$W_1 = \ker(A - I_2), \quad W_2 = \ker(A + I_2)$$

are both nonzero, and neither is the whole plane, so $W_1$ and $W_2$ are both one-dimensional. We already noted that $W_1$ is the line of reflection of $A$ (fixed points of $A$ form the kernel of $A - I_2$). It turns out that $W_2$ is the line perpendicular to $W_1$. To see why, pick $w_1 \in W_1$ and $w_2 \in W_2$, so

$$Aw_1 = w_1, \quad Aw_2 = -w_2.$$

Then, since $Aw_1 \cdot Aw_2 = w_1 \cdot w_2$ by orthogonality of $A$, we have

$$w_1 \cdot (-w_2) = w_1 \cdot w_2.$$

Thus $w_1 \cdot w_2 = 0$, so $w_1 \perp w_2$.

Now we are ready to show $h$ is a glide reflection. Pick nonzero vectors $w_i \in W_i$ for $i = 1, 2$, and use $\{w_1, w_2\}$ as a basis of $\mathbf{R}^2$. Write $w = h(\mathbf{0})$ in terms of this basis: $w = c_1w_1 + c_2w_2$. To say there are no fixed points for $h$ is the same as $Aw \neq -w$, so $w \notin W_2$. That is, $c_1 \neq 0$. Then

$$h(v) = Av + w = (Av + c_2w_2) + c_1w_1. \tag{4.3}$$

Since $A(c_2w_2) = -c_2w_2$, our previous discussion shows $v \mapsto Av + c_2w_2$ is a reflection across the line $c_2w_2/2 + W_1$. Since $c_1w_1$ is a nonzero vector in $W_1$, (4.3) exhibits $h$ as the composition of a reflection across the line $c_2w_2/2 + W_1$ and a nonzero translation by $c_1w_1$, whose direction is parallel to the line of reflection, so $h$ is a glide reflection.

We have now justified the information in Table 1. Each row describes a different kind of isometry. Using fixed points it is easy to distinguish the first four rows from each other and to distinguish glide reflections from any isometry besides translations. A glide reflection can't be a translation since any isometry of $\mathbf{R}^2$ is uniquely of the form $h_{A,w}$, and translations have $A = I_2$ while glide reflections have $\det A = -1$.

**Lemma 4.1.** *A composition of two reflections of $\mathbf{R}^2$ is a translation or a rotation.*

*Proof.* The product of two matrices with determinant $-1$ has determinant 1, so the composition of two reflections has the form $v \mapsto Av + w$ where $\det A = 1$. Such isometries are translations or rotations by Table 1 (consider the identity to be a trivial translation or rotation). $\square$

In Example A.2 we will express any translation in $\mathbf{R}^n$ as the composition of two reflections.

**Theorem 4.2.** *Each isometry of $\mathbf{R}^2$ is a composition of at most 2 reflections except for glide reflections, which are a composition of 3 (and no fewer) reflections.*

*Proof.* We check the theorem for each type of isometry in Table 1 besides reflections, for which the theorem is obvious.

The identity is the square of any reflection.

For a translation $t(v) = v + w$, let $A$ be the matrix representing the reflection across the line $w^\perp$. Then $Aw = -w$. Set $s_1(v) = Av + w$ and $s_2(v) = Av$. Both $s_1$ and $s_2$ are reflections, and $(s_1 \circ s_2)(v) = A(Av) + w = v + w$ since $A^2 = I_2$.

Now consider a rotation, say $h(v) = A(v - p) + p$ for some $A \in \mathrm{O}_2(\mathbf{R})$ with $\det A = 1$ and $p \in \mathbf{R}^2$. We have $h = t \circ r \circ t^{-1}$, where $t$ is translation by $p$ and $r(v) = Av$ is a rotation around the origin. Let $A'$ be any reflection matrix (*e.g.*, $A' = (\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix})$). Set $s_1(v) = AA'v$ and $s_2(v) = A'v$. Both $s_1$ and $s_2$ are reflections and $r = s_1 \circ s_2$ (check). Therefore

$$h = t \circ r \circ t^{-1} = (t \circ s_1 \circ t^{-1}) \circ (t \circ s_2 \circ t^{-1}). \tag{4.4}$$

The conjugate of a reflection by a translation (or by any isometry, for that matter) is another reflection, as an explicit calculation using Table 1 shows. Thus, (4.4) expresses the rotation $h$ as a composition of 2 reflections.

Finally we consider glide reflections. Since this is the composition of a translation and a reflection, it is a composition of 3 reflections. We can't use fewer reflections to get a glide reflection, since a composition of two reflections is either a translation or a rotation by Lemma 4.1 and we know that a glide reflection is not a translation or rotation (or reflection). $\square$

In Table 2 we record the minimal number of reflections whose composition can equal a particular type of isometry of $\mathbf{R}^2$.

| Isometry | Min. Num. Reflections | dim(fixed set) |
|---|---|---|
| Identity | 0 | 2 |
| Nonzero Translation | 2 | 0 |
| Nonzero Rotation | 2 | 0 |
| Reflection | 1 | 1 |
| Glide Reflection | 3 | 0 |

Table 2. Counting Reflections in an Isometry

That each isometry of $\mathbf{R}^2$ is a composition of at most 3 reflections can be proved geometrically, without recourse to a prior classification of all isometries of the plane. We will give a rough sketch of the argument. We will take for granted (!) that an isometry that fixes at least two points is a reflection across the line through those points or is the identity. (This is related to Corollary 2.3 when $n = 2$.) Pick any isometry $h$ of $\mathbf{R}^2$. We may suppose $h$ is not a reflection or the identity (the identity is the square of any reflection), so $h$ has at most one fixed point. If $h$ has one fixed point, say $P$, choose $Q \neq P$. Then $h(Q) \neq Q$ and the points $Q$ and $h(Q)$ lie on a common circle centered at $P$ (because $h(P) = P$). Let $s$ be the reflection across the line through $P$ that is perpendicular to the line connecting $Q$ and $h(Q)$. Then $s \circ h$ fixes $P$ and $Q$, so $s \circ h$ is the identity or is a reflection. Thus $h = s \circ (s \circ h)$ is a reflection or a composition of two reflections. If $h$ has no fixed points, pick any point $P$. Let $s$ be the reflection across the perpendicular bisector of the line connecting $P$ and $h(P)$, so $s \circ h$ fixes $P$. Thus $s \circ h$ has a fixed point, so our previous argument shows $s \circ h$ is either the identity, a reflection, or the composition of two reflections, so $h$ is the composition of at most 3 reflections.

A byproduct of this argument, which did not use the classification of isometries, is another proof that all isometries of $\mathbf{R}^2$ are invertible: any isometry is a composition of reflections and reflections are invertible.

From the fact that all isometries fixing $\mathbf{0}$ in $\mathbf{R}$ and $\mathbf{R}^2$ are rotations or reflections, the following general description can be proved about isometries of any Euclidean space in terms of rotations and reflections on one-dimensional and two-dimensional subspaces.

**Theorem 4.3.** *If $h$ is an isometry of $\mathbf{R}^n$ that fixes $\mathbf{0}$ then there is an orthogonal decomposition $\mathbf{R}^n = W_1 \oplus W_2 \oplus \cdots \oplus W_m$ such that $\dim(W_i) = 1$ or $2$ for all $i$, and the restriction of $h$ to $W_i$ is a rotation unless $i = m$ and $\dim(W_m) = 1$ and $\det h = -1$, in which case the restriction of $h$ to $W_m$ is a reflection.*

*Proof.* See [1, Theorem 6.47] or [2, Cor. to Theorem 2]. $\square$

## Appendix A. Reflections

A reflection is an isometry of $\mathbf{R}^n$ that fixes all the points in a chosen hyperplane and interchanges the position of points along each line perpendicular to that hyperplane at equal distance from it. These isometries play a role that is analogous to transpositions in the symmetric group. Reflections, like transpositions, have order 2.

Let's look first at reflections across hyperplanes that *contain the origin*. Let $H$ be a hyperplane containing the origin through which we wish to reflect. Set $L = H^\perp$, so $L$ is a one-dimensional subspace. Every $v \in \mathbf{R}^n$ can be written uniquely in the form $v = w + u$, where $w \in H$ and $u \in L$. The reflection across $H$, by definition, is the function

$$s(v) = s(w + u) = w - u. \tag{A.1}$$

That is, $s$ fixes $H = u^\perp$ and acts like $-1$ on $L = \mathbf{R}u$. From the formula defining $s$, it is linear in $v$. Since $w \perp u$, $||s(v)|| = ||w|| + ||u|| = ||v||$, so by linearity $s$ is an isometry: $||s(v) - s(w)|| = ||s(v - w)|| = ||v - w||$.

Since $s$ is linear, it can be represented by a matrix. To write this matrix simply, pick an orthogonal basis $\{v_1, \dots, v_{n-1}\}$ of $H$ and let $v_n$ be a nonzero vector in $L = H^\perp$, so $v_n$ is orthogonal to $H$. Then

$$s(c_1v_1 + \cdots + c_nv_n) = c_1v_1 + \cdots + c_{n-1}v_{n-1} - c_nv_n.$$

The matrix for $s$ has 1's along the diagonal except for $-1$ in the last position:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_{n-1} \\ -c_n \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & -1 \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_{n-1} \\ c_n \end{pmatrix}. \tag{A.2}$$

The matrix in (A.2) represents $s$ relative to a convenient choice of basis. In particular, from the matrix representation we see $\det s = -1$: every reflection in $\mathrm{O}_n(\mathbf{R})$ has determinant $-1$. Notice the analogy with transpositions in the symmetric group, which have sign $-1$.

We now derive another formula for $s$, which will look more complicated than what we have seen so far but should be considered more fundamental. Fix a nonzero vector $u$ on the line $L = H^\perp$. Since $\mathbf{R}^n = H \oplus L$, any $v \in \mathbf{R}^n$ can be written as $w + cu$, where $w \in H$ and $c \in \mathbf{R}$. Since $w \perp L$, $v \cdot u = c(u \cdot u)$, so $c = (v \cdot u)/(u \cdot u)$. Then

$$s(v) = w - cu = v - 2cu = v - 2\frac{v \cdot u}{u \cdot u}u. \tag{A.3}$$

The last expression is our desired formula for $s(v)$. Note for all $v$ that $s(v) \cdot u = -v \cdot u$.

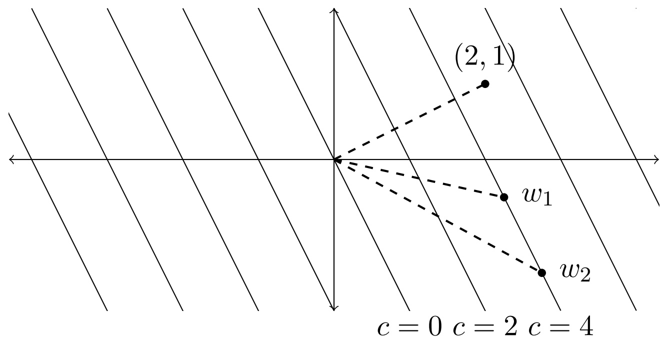
It is standard to label the reflection across a hyperplane *containing the origin* using a vector in the orthogonal complement to the hyperplane, so we write $s$ in (A.3) as $s_u$. This is the reflection in the hyperplane $u^\perp$, so $s_u(u) = -u$. By (A.3), $s_{au} = s_u$ for any $a \in \mathbf{R} - \{0\}$, which makes geometric sense since $(au)^\perp = u^\perp$, so the reflection in the hyperplane orthogonal to $u$ and to $au$ is the same. Moreover, $H$ is the set of points fixed by $s_u$, and we can confirm this with (A.3): $s_u(v) = 0$ if and only if $v \cdot u = 0$, which means $v \in u^\perp = H$.

To get a formula for the reflection across any hyperplane in $\mathbf{R}^n$ (not just those containing the origin), we use the following lemma to describe any hyperplane.

**Lemma A.1.** *Every hyperplane in* $\mathbf{R}^n$ *has the form* $H_{u,c} = \{v \in \mathbf{R}^n : v \cdot u = c\}$ *for some nonzero* $u \in \mathbf{R}^n$ *that is orthogonal to the hyperplane and some* $c \in \mathbf{R}$. *The hyperplane contains* $\mathbf{0}$ *if and only if* $c = 0$.

*Proof.* Let $H$ be a hyperplane and choose $w \in H$. Then $H - w$ is a hyperplane containing the origin. Fix a nonzero vector $u$ that is perpendicular to $H$. Since $H - w$ is a hyperplane through the origin parallel to $H$, a vector $v$ lies in $H$ if and only if $v - w \perp u$, which is equivalent to $v \cdot u = w \cdot u$. Thus $H = H_{u,c}$ for $c = w \cdot u$. $\square$

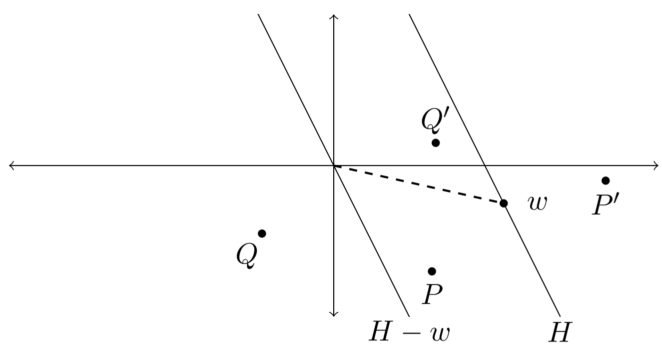
Below are hyperplanes (lines) in $\mathbf{R}^2$ of the form $H_{(2,1),c} = \{v : v \cdot (2,1) = c\}$.




As the figure suggests, the different hyperplanes $H_{u,c}$ as $c$ varies are parallel to each other. Specifically, if $w \in H_{u,c}$ then $H_{u,c} = H_{u,0} + w$ (check!). (The choice of $w$ in $H_{u,c}$ affects how $H_{u,0}$ is translated over to $H_{u,c}$, since adding $w$ to $H_{u,0}$ sends $\mathbf{0}$ to $w$. Compare in the above figure how $H_{u,0}$ is carried onto $H_{u,4}$ using translation by $w_1$ and by $w_2$.)

In the family of parallel hyperplanes $\{H_{u,c} : c \in \mathbf{R}\}$, we can replace $u$ with any nonzero scalar multiple, since $H_{au,c} = H_{u,c/a}$, so $\{H_{u,c} : c \in \mathbf{R}\} = \{H_{au,c} : c \in \mathbf{R}\}$. Geometrically this makes sense, since the importance of $u$ relative to the hyperplanes is that it is an orthogonal direction, and $au$ also provides an orthogonal direction to the same hyperplanes.

To reflect points across a hyperplane $H$, fix a *nonzero* vector $w \in H$. Geometric intuition suggests that to reflect across $H$ we can subtract $w$, then reflect across $H - w$ (a hyperplane through the origin), and then add $w$ back. In the figure below, this corresponds to moving from $P$ to $Q$ (subtract $w$ from $P$) to $Q'$ (reflect $Q$ across $H - w$) to $P'$ (add $w$ to $Q'$), getting the reflection of P across $H$.




Therefore reflection across $H$ should be given by the formula

$$s'(v) = s(v - w) + w, \tag{A.4}$$

where $s$ is reflection across $H - w$. Setting $H = H_{u,c}$ by Lemma A.1, where $u$ is a nonzero vector orthogonal to $H$, $c = u \cdot w$ (since $w \in H$) and by (A.3) and (A.4)

$$s'(v) = (v - w) - 2\frac{(v-w)\cdot u}{u \cdot u}u + w = v - 2\left(\frac{v \cdot u - c}{u \cdot u}\right)u. \tag{A.5}$$

The following properties show (A.5) *is* the reflection across the hyperplane $H_{u,c}$.

- If $v \in H_{u,c}$ then $v \cdot u = c$, so (A.5) implies $s'(v) = v$: $s'$ fixes points in $H_{u,c}$.
- For any $v$ in $\mathbf{R}^n$, the average $\frac{1}{2}(v + s'(v))$, which is the midpoint of the segment connecting $v$ and $s'(v)$, lies in $H_{u,c}$: it equals $v - \left(\frac{v \cdot u - c}{u \cdot u}\right)u$, whose dot product with $u$ is $c$.
- For any $v$ in $\mathbf{R}^n$ the difference $v - s'(v)$, which is the direction of the segment connecting $v$ and $s'(v)$, is perpendicular to $H_{u,c}$ since, by (A.5), it lies in $\mathbf{R}u = H^\perp$.

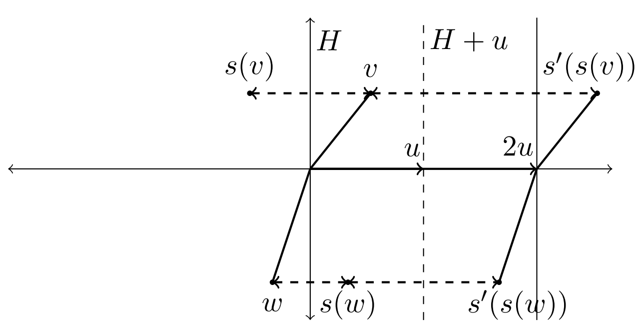
**Example A.2.** We use (A.5) to show any nonzero translation $t_u(v) = v + u$ is the composition of two reflections. Set $H = u^\perp = H_{u,0}$ and write $s_u$ for the reflection across $H$ and $s'_u$ for the reflection across $H + u$, the hyperplane parallel to $H$ that contains $u$. By (A.3) and (A.5),

$$s'_u(s_u(v)) = s_u(v) - 2\left(\frac{s_u(v)\cdot u - u \cdot u}{u \cdot u}\right)u = s_u(v) - 2\left(\frac{-v \cdot u}{u \cdot u} - 1\right)u = v + 2u,$$

so $s'_u \circ s_u = t_{2u}$. This is true for all $u$, so $t_u = s'_{u/2} \circ s_{u/2}$.

These formulas show any translation is a composition of two reflections across hyperplanes perpendicular to the direction of the translation.

The figure below illustrates Example A.2 in the plane, with $u$ being a vector along the $x$-axis. Reflecting $v$ and $w$ across $H = u^\perp$ and then across $H + u$ is the same as translation of $v$ and $w$ by $2u$.




**Theorem A.3.** *Let $w$ and $w'$ be distinct in $\mathbf{R}^n$. There is a unique reflection $s$ in $\mathbf{R}^n$ such that $s(w) = w'$. This reflection is in $\mathrm{O}_n(\mathbf{R})$ if and only if $w$ and $w'$ have the same length.*

*Proof.* A reflection taking $w$ to $w'$ has a fixed hyperplane that contains the average $\frac{1}{2}(w+w')$ and is orthogonal to $w - w'$. Therefore the fixed hyperplane of a reflection taking $w$ to $w'$ must be $H_{w-w',c}$ for some $c$. Since $\frac{1}{2}(w+w') \in H_{w-w',c}$, we have $c = (w - w')\cdot\frac{1}{2}(w+w') = \frac{1}{2}(w \cdot w - w' \cdot w')$. Thus the only reflection that could send $w$ to $w'$ is the one across the hyperplane $H_{w-w',\frac{1}{2}(w\cdot w - w'\cdot w')}$.

Let's check that reflection across this hyperplane does send $w$ to $w'$. Its formula, by (A.5), is

$$s(v) = v - 2\left(\frac{v\cdot(w-w')-c}{(w-w')\cdot(w-w')}\right)(w-w'),$$

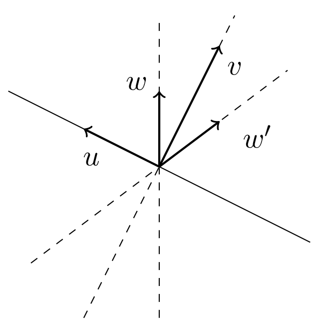
where $c = \frac{1}{2}(w\cdot w - w'\cdot w')$. When $v = w$, the coefficient of $w - w'$ in the above formula becomes $-1$, so $s(w) = w - (w - w') = w'$.

If $w$ and $w'$ have the same length then $w \cdot w = w' \cdot w'$, so $c = 0$ and that means $s$ has fixed hyperplane $H_{w-w',0}$. Therefore $s$ is a reflection fixing $\mathbf{0}$, so $s \in \mathrm{O}_n(\mathbf{R})$. Conversely, if $s \in \mathrm{O}_n(\mathbf{R})$ then $s(\mathbf{0}) = \mathbf{0}$, which implies $\mathbf{0} \in H_{w-w',c}$, so $c = 0$, and therefore $w\cdot w = w'\cdot w'$, which means $w$ and $w'$ have the same length.

To illustrate techniques, when $w$ and $w'$ are distinct vectors in $\mathbf{R}^n$ with the same length let's construct a reflection across a hyperplane through the origin that sends $w$ to $w'$ geometrically, without using the algebraic formulas for reflections and hyperplanes.

If $w$ and $w'$ are on the same line through the origin then $w' = -w$ (the only vectors on $\mathbf{R}w$ with the same length as $w$ are $w$ and $-w$). For the reflection $s$ across the hyperplane $w^\perp$, $s(w) = -w = w'$.

If $w$ and $w'$ are not on the same line through the origin then the span of $w$ and $w'$ is a plane. The vector $v = w + w'$ is nonzero and lies on the line in this plane that bisects the angle between $w$ and $w'$. (See the figure below.) Let $u$ be a vector in this plane orthogonal to $v$, so writing $w = av + bu$ we have $w' = av - bu$.[1] Letting $s$ be the reflection in $\mathbf{R}^n$ across the hyperplane $u^\perp$, which contains $\mathbf{R}v$ (and contains more than $\mathbf{R}v$ when $n > 2$), we have $s(v) = v$ and $s(u) = -u$, so $s(w) = s(av + bu) = av - bu = w'$.




□

We have already noted that reflections in $\mathrm{O}_n(\mathbf{R})$ are analogous to transpositions in the symmetric group $S_n$: they have order 2 and determinant $-1$, just as transpositions have order 2 and sign $-1$. The next theorem, due to E. Cartan, is the analogue for $\mathrm{O}_n(\mathbf{R})$ of the generation of $S_n$ by transpositions.

**Theorem A.4** (Cartan)**.** *The group* $\mathrm{O}_n(\mathbf{R})$ *is generated by its reflections.*

Note that a reflection in $\mathrm{O}_n(\mathbf{R})$ fixes $\mathbf{0}$ and therefore its fixed hyperplane contains the origin, since a reflection does not fix any point outside its fixed hyperplane.

[1] This is geometrically clear, but algebraically tedious. Since $v = w + w'$, we have $w' = v - w = (1-a)v - bu$, so to show $w' = av - bu$ we will show $a = \frac{1}{2}$. Since $v \perp u$, $w\cdot v = a(v\cdot v)$. The vectors $w$ and $w'$ have the same length, so $w\cdot v = w\cdot(w+w') = w\cdot w + w\cdot w'$ and $v\cdot v = (w+w')\cdot(w+w') = 2(w\cdot w + w\cdot w')$, so $w \cdot v = \frac{1}{2}(v\cdot v)$. Comparing this with $w\cdot v = a(v\cdot v)$, we have $a = \frac{1}{2}$.

*Proof.* We argue by induction on $n$. The theorem is trivial when $n = 1$, since $\mathrm{O}_1(\mathbf{R}) = \{\pm 1\}$. Let $n \geq 2$. (While the case $n = 2$ was treated in Theorem 4.2, we will reprove it here.)

Pick $h \in \mathrm{O}_n(\mathbf{R})$, so $h(e_n)$ and $e_n$ have the same length. If $h(e_n) \neq e_n$, by Theorem A.3 there is a (unique) reflection $s$ in $\mathrm{O}_n(\mathbf{R})$ such that $s(h(e_n)) = e_n$, so the composite isometry $sh = s \circ h$ fixes $e_n$. If $h(e_n) = e_n$ then we can write $s(h(e_n)) = e_n$ where $s$ is the identity on $\mathbf{R}^n$. We will use $s$ with this meaning (reflection or identity) below.

Any element of $\mathrm{O}_n(\mathbf{R})$ preserves orthogonality, so $sh$ sends the hyperplane $H := e_n^\perp = \mathbf{R}^{n-1} \oplus \{0\}$ back to itself and is the identity on the line $\mathbf{R}e_n$. Since $e_n^\perp = \mathbf{R}^{n-1} \oplus \{0\}$ has dimension $n-1$, by induction[2] there are a finite number of reflections $\overline{s}_1, \ldots, \overline{s}_m$ in $H$ fixing the origin such that

$$sh|_H = \overline{s}_1\overline{s}_2 \cdots \overline{s}_m.$$

Any reflection $H \to H$ that fixes $\mathbf{0}$ extends naturally to a reflection of $\mathbf{R}^n$ fixing $\mathbf{0}$, by declaring it to be the identity on the line $H^\perp = \mathbf{R}e_n$ and extending by linearity from the behavior on $H$ and $H^\perp$.[3] Write $s_i$ for the extension of $\overline{s}_i$ to a reflection on $\mathbf{R}^n$ in this way. Consider now the two isometries

$$sh, \quad s_1s_2 \cdots s_m$$

of $\mathbf{R}^n$. They agree on $H = e_n^\perp$ and they each fix $e_n$. Thus, by linearity, we have equality as functions on $\mathbf{R}^n$:

$$sh = s_1s_2 \cdots s_m.$$

Therefore $h = s^{-1}s_1s_2 \cdots s_m$. □

From the proof, if $(sh)|_H$ is a composition of $m$ isometries of $H$ fixing $\mathbf{0}$ that are the identity or reflections then $h$ is a composition of $m + 1$ isometries of $\mathbf{R}^n$ fixing $\mathbf{0}$ that are the identity or reflections. Therefore every element of $\mathrm{O}_n(\mathbf{R})$ is a composition of at most $n$ elements of $\mathrm{O}_n(\mathbf{R})$ that are the identity or reflections (in other words, from $m \leq n-1$ we get $m+1 \leq n$). If $h$ is not the identity then such a decomposition of $h$ must include reflections, so by removing the identity factors we see $h$ is a composition of at most $n$ reflections. The identity on $\mathbf{R}^n$ is a composition of 2 reflections. This establishes the stronger form of Cartan's theorem: every element of $\mathrm{O}_n(\mathbf{R})$ is a composition of at most $n$ reflections (except for the identity when $n = 1$, unless we use the convention that the identity is a composition of 0 reflections).

**Remark A.5.** Cartan's theorem can be deduced from the decomposition of $\mathbf{R}^n$ in Theorem 4.3. Let $a$ be the number of 2-dimensional $W_i$'s and $b$ be the number of 1-dimensional $W_i$'s, so $2a + b = n$ and $h$ acts as a rotation on any 2-dimensional $W_i$. By Theorem 4.2, any rotation of $W_i$ is a composition of two reflections in $W_i$. A reflection in $W_i$ can be extended to a reflection in $\mathbf{R}^n$ by setting it to be the identity on the other $W_j$'s. If $W_i$ is 1-dimensional then $h$ is the identity on $W_i$ except perhaps once, in which case $b \geq 1$ and $h$ is a reflection on that $W_i$. Putting all of these reflections together, we can express $h$ as a composition of at most $2a$ reflections if $b = 0$ and at most $2a + 1$ reflections if $b \geq 1$. Either way, $h$ is a

[2]Strictly speaking, since $H$ is not $\mathbf{R}^{n-1}$, to use induction we really should be proving the theorem not just for orthogonal transformations of the Euclidean spaces $\mathbf{R}^n$, but for orthogonal transformations of their subspaces as well. The definition of an orthogonal transformation of a subspace $W \subset \mathbf{R}^n$ is based on the property (3.3): it is a linear transformation $W \to W$ that preserves dot products between all pairs of vectors in $W$. We use (A.3) – rather than a matrix formula – to define a reflection across a hyperplane in a subspace.

[3]Geometrically, for $n - 1 \geq 2$ if $\overline{s}$ is a reflection on $H$ fixing the orthogonal complement of a line $L$ in $H$, then this extension of $\overline{s}$ to $\mathbf{R}^n$ is the reflection on $\mathbf{R}^n$ fixing the orthogonal complement of $L$ in $\mathbf{R}^n$.

composition of at most $2a + b = n$ reflections, with the understanding when $n = 1$ that the identity is a composition of 0 reflections.

**Example A.6.** For $0 \le m \le n$, we will show the orthogonal matrix

$$\begin{pmatrix} -1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

with $m$ $-1$'s and $n - m$ 1's on the diagonal is a composition of $m$ reflections in $\mathrm{O}_n(\mathbf{R})$ and not less than $m$ reflections in $\mathrm{O}_n(\mathbf{R})$.

Any reflection in $\mathrm{O}_n(\mathbf{R})$ has a fixed hyperplane through $\mathbf{0}$ of dimension $n-1$. Therefore a composition of $r$ reflections in $\mathrm{O}_n(\mathbf{R})$ fixes the intersection of $r$ hyperplanes through the origin, whose dimension is at least $n-r$ (some hyperplanes may be the same). If $h \in \mathrm{O}_n(\mathbf{R})$ is a composition of $r$ reflections and fixes a subspace of dimension $d$ then $d \ge n - r$, so $r \ge n - d$. Hence we get a lower bound on the number of reflections in $\mathrm{O}_n(\mathbf{R})$ whose composition can equal $h$ in terms of the dimension of $\{v \in \mathbf{R}^n : h(v) = v\}$. For the above matrix, the subspace of fixed vectors is $\{0\}^m \oplus \mathbf{R}^{n-m}$, which has dimension $n-m$. Therefore the least possible number of reflections in $\mathrm{O}_n(\mathbf{R})$ whose composition could equal this matrix is $n - (n - m) = m$, and this bound is achieved: the $m$ matrices with $-1$ in one of the first $m$ positions on the main diagonal and 1 elsewhere on the main diagonal are all reflections in $\mathrm{O}_n(\mathbf{R})$ and their composition is the above matrix.

In particular, the isometry $h(v) = -v$ is a composition of $n$ and no fewer reflections in $\mathrm{O}_n(\mathbf{R})$.

**Corollary A.7.** *Every isometry of $\mathbf{R}^n$ is a composition of at most $n + 1$ reflections. An isometry that fixes at least one point is a composition of at most $n$ reflections.*

The difference between this corollary and Cartan's theorem is that in the corollary we are not assuming isometries, or in particular reflections, are taken from $\mathrm{O}_n(\mathbf{R})$, *i.e.*, they need not fix $\mathbf{0}$.

*Proof.* Let $h$ be an isometry of $\mathbf{R}^n$. If $h(\mathbf{0}) = \mathbf{0}$, then $h$ belongs to $\mathrm{O}_n(\mathbf{R})$ (Theorem 2.4) and Cartan's theorem implies $h$ is a composition of at most $n$ reflections through hyperplanes containing $\mathbf{0}$. If $h(p) = p$ for some $p \in \mathbf{R}^n$, then we can change the coordinate system (using a translation) so that the origin is placed at $p$. Then the previous case shows $h$ is a composition of at most $n$ reflections through hyperplanes containing $p$.

Suppose $h$ has no fixed points. Then in particular, $h(\mathbf{0}) \neq \mathbf{0}$. By Theorem A.3 there is some reflection $s$ across a hyperplane in $\mathbf{R}^n$ such that $s(h(\mathbf{0})) = \mathbf{0}$. Then $sh \in \mathrm{O}_n(\mathbf{R})$, so by Cartan's theorem $sh$ is a composition of at most $n$ reflections, and that implies $h = s(sh)$ is a composition of at most $n + 1$ reflections. □

The proof of Corollary A.7 shows an isometry of $\mathbf{R}^n$ is a composition of at most $n$ reflections except possibly when it has no fixed points. Then $n + 1$ reflections may be required. For example, when $n = 2$ nonzero translations and glide reflections have no fixed points, and the first type requires 2 reflections while the second type requires 3 reflections.

## References

[1] S. H. Friedberg, A. J. Insel, and L. E. Spence, "Linear Algebra," 4th ed., Pearson, Upper Saddle River NJ, 2003.
[2] L. Rudolph, "The Structure of Orthogonal Transformations," *Amer. Math. Monthly* **98** (1991), 349–352.
[3] A. Vogt, "On the linearity of form isometries," *SIAM Journal on Applied Mathematics* **22** (1972), 553–560.