1 Shuffles and the Orthogonal Group

10/3: 1. There are two **riffle shuffles** of a deck of 52 cards obtained as follows: Divide the deck into the top 26 and bottom 26 cards. Then interweave the two decks card by card; there are two different shuffles depending on whether the top card from the top deck ends up on top, or the top card from the bottom deck ends up on top. If we denote the shuffles by A and B, respectively, then we saw in class that $A^8 = 1$ and $B^{52} = 1$. Determine whether every permutation of 52 cards can be obtained by some combination of riffle shuffles.

Proof. As functions, $A, B : [52] \to [52]$ can be defined piecewise as follows.

$$A(n) = \begin{cases} 2n-1 & n \in [26] \\ 2n-52 & n \in [27:52] \end{cases} \qquad B(n) = \begin{cases} 2n & n \in [26] \\ 2n-53 & n \in [27:52] \end{cases}$$

We can confirm via casework that both functions obey the rule $f(53-n) = 53 - f(n)$ for all $n \in [52]$[1]: If $n \in [26]$, then

$$\begin{aligned} A(53-n) &\stackrel{?}{=} 53 - A(n) & B(53-n) &\stackrel{?}{=} 53 - B(n) \\ 2(53-n) - 52 &\stackrel{?}{=} 53 - (2n-1) & 2(53-n) - 53 &\stackrel{?}{=} 53 - 2n \\ 54 - 2n &\stackrel{\checkmark}{=} 54 - 2n & 53 - 2n &\stackrel{\checkmark}{=} 53 - 2n \end{aligned}$$

and if $n \in [27:52]$, then

$$\begin{aligned} A(53-n) &\stackrel{?}{=} 53 - A(n) & B(53-n) &\stackrel{?}{=} 53 - B(n) \\ 2(53-n) - 1 &\stackrel{?}{=} 53 - (2n-52) & 2(53-n) &\stackrel{?}{=} 53 - (2n-53) \\ 105 - 2n &\stackrel{\checkmark}{=} 105 - 2n & 106 - 2n &\stackrel{\checkmark}{=} 106 - 2n \end{aligned}$$

It follows since both A, B obey this rule that every permutation of 52 cards obtained by some combination of riffle shuffles (i.e., composition of A, B) obeys this rule. In particular, we can prove that $f^k(53-n) = 53 - f^k(n)$ for all $k \in \mathbb{N}$ via induction. For the base case $k = 2$, we have that

$$f^2(53-n) = f(f(53-n)) = f(53 - f(n)) = 53 - f(f(n)) = 53 - f^2(n)$$

Now suppose inductively that $f^k(53-n) = 53 - f^k(n)$. Then

$$f^{k+1}(53-n) = f(f^k(53-n)) = f(53 - f^k(n)) = 53 - f(f^k(n)) = 53 - f^{k+1}(n)$$

as desired.

Moreover, there are shuffles of 52 cards that do *not* obey this rule. For example, consider the transposition $\tau_{1,2}$: We, for instance, have that

$$\tau_{1,2}(53-1) = 52 \neq 51 = 53 - \tau_{1,2}(1)$$

so $\tau_{1,2}$ doesn't obey this rule. Therefore, we know that:

Every permutation of 52 cards *cannot* be obtained by some combination of riffle shuffles.

□

[1] In layman's terms, we have intuited that the mappings are symmetric about the center of the stack. More specifically, both functions map cards that are initially positioned equidistant from the center of the stack to positions that are *still* equidistant from the center of the stack. For example, notice that 2 and 51 are both 25 cards from the center of the stack, and A maps them to 3 and 50, which are both 24 cards from the center of the stack. Alternative perspective: Cards equidistant from the center of the stack always add to 53.

2. **The Orthogonal Group.** For two vectors $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{R}^n$, let $\langle \mathbf{v}, \mathbf{w} \rangle$ denote the usual dot product of $\mathbf{v}$ and $\mathbf{w}$, so, if $\mathbf{v} = (v_i)$ and $\mathbf{w} = (w_i)$, then $\langle \mathbf{v}, \mathbf{w} \rangle = \sum v_i w_i$. If $M = [a_{ij}]$ is a matrix with coefficients in $\mathbb{R}$, let M^T denote the transpose of M, which is the matrix $[a_{ji}]$.

   (a) Let $\mathrm{O}(n) \subset M_n(\mathbb{R})$ denote the set of matrices M such that $MM^T = I$. Prove that $\mathrm{O}(n)$ is a group. (Hint: Show that $(AB)^T = B^T A^T$.)

   Proof. To prove that $\mathrm{O}(n)$ is a group, it will suffice to show that it contains an identity element, every element has an inverse, and composition (our chosen operation) is associative and closed on $\mathrm{O}(n)$.

   We can take the $n \times n$ identity matrix I to be our identity element (note that $I \in \mathrm{O}(n)$ since $II^T = II = I$).

   The inverse of every $M \in \mathrm{O}(n)$ is M^T. We know that $M^T \in \mathrm{O}(n)$ since, taking the hint[2] that $(AB)^T = B^T A^T$, we can find that

$$M^T (M^T)^T = (MM^T)^T = I^T = I$$

   Additionally, $M^T = M^{-1}$ since $M \in \mathrm{O}(n)$ implies $MM^T = I$ (i.e., M^T is a right-inverse of M) by definition, and

$$M^T M = M^T (M^T)^T = I$$

   shows that M^T is a left-inverse of M.

   Suppose $A, B, C \in \mathrm{O}(n)$. We know that the entry in the i^{th} row and k^{th} column of AB is given by the left equation below, and the entry in the k^{th} row and j^{th} column of BC is given by the right equation below.

$$ab_{ik} = \sum_{k'=1}^{n} a_{ik'} b_{k'k} \qquad\qquad bc_{kj} = \sum_{k'=1}^{n} b_{kk'} c_{k'j}$$

   It follows that the entry in the i^{th} row and j^{th} column of $(AB)C$ and $A(BC)$ are related as follows.

$$\begin{aligned}
(ab)c_{ij} &= \sum_{k=1}^{n} ab_{ik} c_{kj} \\
&= \sum_{k=1}^{n} \left(\sum_{k'=1}^{n} a_{ik'} b_{k'k} \right) c_{kj} \\
&= \sum_{k=1}^{n} \sum_{k'=1}^{n} a_{ik'} b_{k'k} c_{kj} \\
&= \sum_{k=1}^{n} \sum_{k'=1}^{n} a_{ik} b_{kk'} c_{k'j} \\
&= \sum_{k=1}^{n} a_{ik} \left(\sum_{k'=1}^{n} b_{kk'} c_{k'j} \right) \\
&= \sum_{k=1}^{n} a_{ik} bc_{kj} \\
&= a(bc)_{ij}
\end{aligned}$$

   Therefore, composition is associative.

   Suppose $A, B \in \mathrm{O}(n)$. Then since

$$(AB)(AB)^T = ABB^T A^T = AIA^T = AA^T = I$$

   we have that $\mathrm{O}(n)$ is closed under composition, as desired. □

[2] We'll take this as a fact of linear algebra. To show it, we could use entry-by-entry matrix multiplication, as is done analogously below to show that composition is associative.

(b) Prove that every element in $\mathrm{O}(n)$ has determinant 1 or -1. Let $\mathrm{SO}(n) \subset \mathrm{O}(n)$ denote the matrices $M \in \mathrm{O}(n)$ such that $\det(M) = 1$. Prove that $\mathrm{SO}(n)$ is a group.

Proof. By the construction of the determinant, we know that $\det(A) = \det\left(A^T\right)$, that $\det(AB) = \det(A)\det(B)$, and that $\det(I) = 1$ for $A, B \in M_n(\mathbb{R})$ and I the identity matrix in $M_n(\mathbb{R})$. Let $M \in \mathrm{O}(n)$ be arbitrary. Then

$$\begin{aligned} 1 &= \det(I) \\ &= \det\left(MM^T\right) \\ &= \det(M)\det\left(M^T\right) \\ &= \det(M)\det(M) \\ &= \det(M)^2 \\ \det(M) &= \pm 1 \end{aligned}$$

as desired.

As in part (a), to prove that $\mathrm{SO}(n)$ is a group, it will suffice to show that it contains an identity element, every element has an inverse, and composition is associative and closed on $\mathrm{SO}(n)$.

Since $I \in \mathrm{O}(n)$ has $\det(I) = 1$, we may choose $I \in \mathrm{SO}(n)$ (the same matrix) to be our identity.

If $\det(M) = 1$, $\det\left(M^T\right) = 1$, so $M \in \mathrm{SO}(n)$ implies that $M^T \in \mathrm{SO}(n)$. As in part (a), we can show that $M^T = M^{-1}$.

The proof that composition is associative is entirely symmetric to that given in part (a).

To prove that $\mathrm{SO}(n)$ is closed under composition, we supplement the proof in part (a) with the fact that if A, B have determinant equal to one, then

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$$

as desired. □

(c) Show that any element $M \in \mathrm{SO}(2)$ is of the form

$$M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

where $a, b \in \mathbb{R}$ satisfy $a^2 + b^2 = 1$. Prove that for such a and b, one can find a unique $\theta \in [0, 2\pi)$ such that $a = \cos(\theta)$ and $b = \sin(\theta)$, and that M is a rotation by θ about the origin.

Proof. Let $M \in \mathrm{SO}(2)$ be arbitrary. As a 2×2 matrix, we can denote M by

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

for $a, b, c, d \in \mathbb{R}$. It follows since $MM^T = I$ that

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} \\ &= \begin{pmatrix} a^2 + b^2 & ac + bd \\ ca + db & c^2 + d^2 \end{pmatrix} \end{aligned}$$

Since $a^2 + b^2 = 1$, we know that $a \in [-1, 1]$. Thus, since cosine is a bijective mapping between $[0, \pi]$ and $[-1, 1]$, we know that $a = \cos(\theta)$ for a unique $\theta \in [0, \pi]$. It follows since $\cos^2(\theta) + \sin^2(\theta) = 1$ for all θ that we may take $b = \pm\sin(\theta)$. If $b < 0$, redefine $\theta := 2\pi - \theta$; this will keep the value of a the same since cosine is even about $x = \pi$ and flip the sign of $\sin(\theta)$ since sine is odd about $x = \pi$. This process yields a unique $\theta \in [0, 2\pi)$ such that $a = \cos(\theta)$ and $b = \sin(\theta)$.

Now repeat the process for c, d to get $c = \cos(\gamma)$ and $d = \sin(\gamma)$ for some $\gamma \in [0, 2\pi)$. We will now use the determinant to relate θ and γ: We have that

$$\begin{aligned} 1 &= \det(M) \\ &= ad - bc \\ &= \cos(\theta)\sin(\gamma) - \sin(\theta)\cos(\gamma) \\ &= \sin(\gamma - \theta) \end{aligned}$$

Hence,

$$\begin{aligned} \gamma - \theta &= \frac{\pi}{2} + 2\pi n \\ \gamma &= \frac{\pi}{2} + \theta + 2\pi n \end{aligned}$$

for some $n \in \mathbb{Z}$. It follows that

$$\begin{aligned} c &= \cos(\gamma) \\ &= \cos\Big(\frac{\pi}{2} + \theta + 2\pi n\Big) \\ &= -\sin(\theta + 2\pi n) \\ &= -\sin(\theta) \end{aligned} \qquad \begin{aligned} d &= \sin(\gamma) \\ &= \sin\Big(\frac{\pi}{2} + \theta + 2\pi n\Big) \\ &= \cos(\theta + 2\pi n) \\ &= \cos(\theta) \end{aligned}$$

Therefore,

$$c = -\sin(\theta) = -b \qquad\qquad d = \cos(\theta) = a$$

so M has the desired form with $a^2 + b^2 = 1$ and we have found the appropriate θ.

The last piece of the puzzle is proving that M is a rotation by θ about the origin. To do so, we will prove that M sends every

$$\begin{pmatrix} r\cos(\phi) \\ r\sin(\phi) \end{pmatrix} \mapsto \begin{pmatrix} r\cos(\phi - \theta) \\ r\sin(\phi - \theta) \end{pmatrix}$$

i.e., is a clockwise rotation. But indeed, if M is arbitrary, we have by invoking its form and basic rules of trigonometry that

$$\begin{aligned} \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} r\cos(\phi) \\ r\sin(\phi) \end{pmatrix} &= \begin{pmatrix} r\cos(\theta)\cos(\phi) + r\sin(\theta)\sin(\phi) \\ -r\sin(\theta)\cos(\phi) + r\cos(\theta)\sin(\phi) \end{pmatrix} \\ &= \begin{pmatrix} r\left[\cos(\theta)\cos(\phi) + \sin(\theta)\sin(\phi)\right] \\ r\left[\sin(\phi)\cos(\theta) - \cos(\phi)\sin(\theta)\right] \end{pmatrix} \\ &= \begin{pmatrix} r\left[\cos(\theta - \phi)\right] \\ r\left[\sin(\phi - \theta)\right] \end{pmatrix} \\ &= \begin{pmatrix} r\cos(\phi - \theta) \\ r\sin(\phi - \theta) \end{pmatrix} \end{aligned}$$

□

(d) Show that any $M \in \mathrm{O}(2) \setminus \mathrm{SO}(2)$ has the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -b & a \\ a & b \end{pmatrix}$$

Proof. This proof will begin analogously to that of part (c), i.e., we can still conclude that

$$a = \cos(\theta) \qquad b = \sin(\theta) \qquad c = \cos(\gamma) \qquad d = \sin(\gamma)$$

However, with the opposite determinant, we now have

$$-1 = \sin(\gamma - \theta)$$

Thus,

$$\begin{aligned}\gamma - \theta &= -\frac{\pi}{2} + 2\pi n \\ \gamma &= -\frac{\pi}{2} + \theta + 2\pi n\end{aligned}$$

for some $n \in \mathbb{Z}$. It follows that

$$\begin{aligned} c &= \cos(\gamma) \\ &= \cos\Big(-\frac{\pi}{2} + \theta + 2\pi n\Big) \\ &= \sin(\theta + 2\pi n) \\ &= \sin(\theta) \end{aligned} \qquad \begin{aligned} d &= \sin(\gamma) \\ &= \sin\Big(-\frac{\pi}{2} + \theta + 2\pi n\Big) \\ &= -\cos(\theta + 2\pi n) \\ &= -\cos(\theta) \end{aligned}$$

Therefore,

$$c = \sin(\theta) = b \qquad d = -\cos(\theta) = -a$$

The relabeling $a := -b$ and $b := a$ gives the desired form. □

Prove that these elements also have the following properties.

i. M^2 is the identity.

Proof. We have that

$$\begin{aligned} M^2 &= \begin{pmatrix} -b & a \\ a & b \end{pmatrix}\begin{pmatrix} -b & a \\ a & b \end{pmatrix} \\ &= \begin{pmatrix} (-b)(-b) + (a)(a) & (-b)(a) + (a)(b) \\ (a)(-b) + (b)(a) & (a)(a) + (b)(b) \end{pmatrix} \\ &= \begin{pmatrix} a^2 + b^2 & ab - ab \\ ab - ab & a^2 + b^2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= I \end{aligned}$$

as desired. □

ii. M is a reflection through some line that passes through the origin $(0, 0)$.

Proof. Consider a matrix, the action of which is a reflection across a line through the origin. This matrix must map every vector collinear with the line of reflection to itself, and every vector $\mathbf{v}$ orthogonal to the line of reflection to $-\mathbf{v}$. Thus, if M is a reflection matrix, it has eigenvalues 1 and -1 (of multiplicity 1 and $n - 1$, respectively). Furthermore, it must have a mutually orthogonal set of eigenvectors. In fact, these properties are enough to fully characterize a reflection matrix. Therefore, to prove that M is a reflection matrix, we need only show that it has eigenvalues 1 and -1 and that its two eigenvectors are orthogonal. Let's begin.

The eigenvalues of M can be computed as follows

$$\begin{aligned} 0 &= (-b - \lambda)(b - \lambda) - a^2 \\ &= -b^2 + b\lambda - b\lambda + \lambda^2 - a^2 \\ &= \lambda^2 - (a^2 + b^2) \\ &= \lambda^2 - 1 \\ \lambda &= \pm 1 \end{aligned}$$

giving the desired result.
It follows by solving the systems of equations

$$\begin{pmatrix} -b & a \\ a & b \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \qquad \begin{pmatrix} -b & a \\ a & b \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = -\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

that suitable eigenvectors are

$$\mathbf{x} = \begin{pmatrix} a \\ b+1 \end{pmatrix} \qquad \mathbf{y} = \begin{pmatrix} a \\ b-1 \end{pmatrix}$$

Indeed, we have by direct computation that

$$\langle \mathbf{x}, \mathbf{y} \rangle = a^2 + (b+1)(b-1) = a^2 + b^2 - 1 = 1 - 1 = 0$$

as desired. □

iii. If $M, N \in \mathrm{O}(2) \setminus \mathrm{SO}(2)$, then $MN \in \mathrm{SO}(2)$ is a rotation.

Proof. Since $\mathrm{O}(2)$ is a group (and hence closed) by part (a), $MN \in \mathrm{O}(2)$. Additionally,

$$\det(MN) = \det(M)\det(N) = (-1)(-1) = 1$$

so $MN \in \mathrm{SO}(2)$ by part (b). Lastly, since every element of $\mathrm{SO}(2)$ is a rotation by part (c), MN is a rotation, as desired. □

(e) Let $\mathbf{u}$ be any non-zero vector in $\mathbb{R}^3$ of length one, so $\|\mathbf{u}\|^2 = \langle \mathbf{u}, \mathbf{u} \rangle = 1$. The vectors $\mathbf{v}$ with $\langle \mathbf{u}, \mathbf{v} \rangle = 0$ live inside the plane orthogonal to $\mathbf{u}$. Show that if $\mathbf{u}_1 = \mathbf{u}$, then there exist vectors $\mathbf{u}_i \in \mathbb{R}^3$ $(i = 1, 2, 3)$ which are orthonormal and mutually orthogonal, that is, $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$ for $i \neq j$ and $\|\mathbf{u}_i\|^2 = \langle \mathbf{u}_i, \mathbf{u}_i \rangle = 1$. Suppose that $M \in \mathrm{SO}(3)$ is a matrix such that $M\mathbf{u} = \mathbf{u}$. Prove that $M\mathbf{u}_1 = \mathbf{u}_1$, $M\mathbf{u}_2 = a\mathbf{u}_2 + b\mathbf{u}_3$, and $M\mathbf{u}_3 = -b\mathbf{u}_2 + a\mathbf{u}_3$ for some a, b with $a^2 + b^2 = 1$, that $a = \cos(\theta)$ and $b = \sin(\theta)$ for a unique $\theta \in [0, 2\pi)$, and deduce that M is a rotation about the line $\mathbf{u}$ by angle θ.

Proof. Let $\mathbf{u}$ be defined as in the problem statement. Pick $\mathbf{x}, \mathbf{y}$ linearly independent from each other and from $\mathbf{u}$ (this is possible since the space we are working with has dimension 3). Use Gram-Schmidt orthogonalization to orthonormalize $\{\mathbf{u}, \mathbf{x}, \mathbf{y}\}$. Symbolically, let

$$\mathbf{u}_1 = \mathbf{u} \qquad \mathbf{u}_2 = \frac{\mathbf{x} - \langle \mathbf{x}, \mathbf{u}_1 \rangle \mathbf{u}_1}{\|\mathbf{x} - \langle \mathbf{x}, \mathbf{u}_1 \rangle \mathbf{u}_1\|} \qquad \mathbf{u}_3 = \frac{\mathbf{y} - \langle \mathbf{y}, \mathbf{u}_1 \rangle \mathbf{u}_1 - \langle \mathbf{y}, \mathbf{u}_2 \rangle \mathbf{u}_2}{\|\mathbf{y} - \langle \mathbf{y}, \mathbf{u}_1 \rangle \mathbf{u}_1 - \langle \mathbf{y}, \mathbf{u}_2 \rangle \mathbf{u}_2\|}$$

Since $M\mathbf{u}_1 = \mathbf{u}_1$ and $MM^T = M^T M = I$, we know that

$$\begin{aligned} M^T M \mathbf{u}_1 &= M^T \mathbf{u}_1 \\ \mathbf{u}_1 &= M^T \mathbf{u}_1 \end{aligned}$$

Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ denote the linear transformation defined by M. It follows from the above that the matrix $\mathcal{M}(T)$ of T with respect to the basis $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\}$ must be of the form

$$\mathcal{M}(T) = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & a & b \\ 0 & c & d \end{array}\right)$$

Knowing that analogous blocks multiply in matrix multiplication, we can thus use part (c) to show that $\mathcal{M}(T)$ is of the form

$$\mathcal{M}(T) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & -b & a \end{pmatrix}$$

with $a^2+b^2=1$ and an appropriate θ. Moreover, it follows that if S is the change of basis matrix from $\{\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3\}$ to $\{\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3\}$, then

$$\begin{aligned}
M\mathbf{u}_2 &= S\mathcal{M}(T)S^{-1}\mathbf{u}_2 \\
&= \begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \mathbf{u}_3\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & a & b\\ 0 & -b & a\end{pmatrix}\begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \mathbf{u}_3\end{pmatrix}^{-1}\mathbf{u}_2 \\
&= \begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \mathbf{u}_3\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & a & b\\ 0 & -b & a\end{pmatrix}\begin{pmatrix}0\\1\\0\end{pmatrix} \\
&= \begin{pmatrix}\mathbf{u}_1 & \mathbf{u}_2 & \mathbf{u}_3\end{pmatrix}\begin{pmatrix}0\\a\\-b\end{pmatrix} \\
&= a\mathbf{u}_2 - b\mathbf{u}_3
\end{aligned}$$

The relabeling $b := -b$ gives the desired result. The proof of the statement $M\mathbf{u}_3 = -b\mathbf{u}_2 + a\mathbf{u}_3$ is entirely symmetric.

We define a "rotation about the line $\mathbf{u}$ by angle θ" to be a matrix M which sends every

$$t\mathbf{u}_1 + r\cos(\phi)\mathbf{u}_2 + r\sin(\phi)\mathbf{u}_3 \mapsto t\mathbf{u}_1 + r\cos(\phi-\theta)\mathbf{u}_2 + r\sin(\phi-\theta)\mathbf{u}_3$$

i.e., which fixes the $\mathbf{u}_1$ component and rotates the $\mathbf{u}_2,\mathbf{u}_3$ component in that perpendicular plane analogously to part (c). Using the same $M = S\mathcal{M}(T)S^{-1}$ trick as above and the argument from part (c), we can clearly see that M is such a matrix. □

(f) **Triviality**: Let $\mathbf{v}_1,\mathbf{v}_2$ be any two linearly independent vectors in $\mathbb{R}^3$. Prove that if $g \in \mathrm{SO}(3)$ fixes $\mathbf{v}_1,\mathbf{v}_2$, then it is the identity. (Hint: Let $\mathbf{u} = \mathbf{v_1}/|\mathbf{v}_1|$ and use part (e).)

Proof. Let $\mathbf{x} = c\mathbf{v}_1 + d\mathbf{v}_2$. Then

$$g\mathbf{x} = cg\mathbf{v}_1 + dg\mathbf{v}_2 = c\mathbf{v}_1 + d\mathbf{v}_2$$

In other words, if g fixes $\mathbf{v}_1,\mathbf{v}_2$, then it fixes all linear combinations of them as well.

Taking the hint, let $\mathbf{u}_1 = \mathbf{v_1}/|\mathbf{v}_1|$. Define $\mathbf{u}_2$ from $\mathbf{v}_2$ as in part (e), and define $\mathbf{u}_3$ from some third linearly independent vector as in part (e). By the construction of $\mathbf{u}_1,\mathbf{u}_2$, we know that $\mathbf{u}_1,\mathbf{u}_2 \in \mathrm{span}(\mathbf{v}_1,\mathbf{v}_2)$. Thus, g fixes $\mathbf{u}_1,\mathbf{u}_2$. This combined with part (e) shows that

$$1\mathbf{u}_2 + 0\mathbf{u}_3 = \mathbf{u}_2 = g\mathbf{u}_2 = a\mathbf{u}_2 + b\mathbf{u}_3$$

i.e., that $a=1$ and $b=0$. Thus,

$$g\mathbf{u}_3 = -b\mathbf{u}_2 + a\mathbf{u}_3 = 0\mathbf{u}_2 + 1\mathbf{u}_3 = \mathbf{u}_3$$

i.e., g fixes $\mathbf{u}_3$ as well. Since g fixes a basis of $\mathbb{R}^3$, g must be the identity on $\mathbb{R}^3$, as desired. □

(g) **Equality**: Let $\mathbf{v}_1,\mathbf{v}_2$ be any two linearly independent vectors in $\mathbb{R}^3$. Prove that if $g \in \mathrm{SO}(3)$ and $h \in \mathrm{SO}(3)$ satisfy $g(\mathbf{v}_1) = h(\mathbf{v}_1)$ and $g(\mathbf{v}_2) = h(\mathbf{v}_2)$, then $g = h$.

Proof. Since $g(\mathbf{v}_1) = h(\mathbf{v}_1)$ and $g(\mathbf{v}_2) = h(\mathbf{v}_2)$, we know that

$$\begin{aligned} h^T g(\mathbf{v}_1) &= h^T h(\mathbf{v}_1) \\ &= \mathbf{v}_1 \end{aligned} \qquad \begin{aligned} h^T g(\mathbf{v}_2) &= h^T h(\mathbf{v}_2) \\ &= \mathbf{v}_2 \end{aligned}$$

Thus, $h^T g$ fixes two linearly independent vectors, so by part (f), $h^T g = I$. Therefore,

$$\begin{aligned} hh^T g &= hI \\ g &= h \end{aligned}$$

as desired. □

(h) Prove that any matrix M has the same eigenvalues as the transpose matrix M^T. (Hint: Show that M and M^T have the same characteristic polynomial.) Prove that if M is invertible, then the matrix M^{-1} has eigenvalues which are the inverses of the eigenvalues of M.

Proof. We know that $\det(A) = \det\big(A^T\big)$ for all $A \in M_n(\mathbb{R})$ and, since λI is symmetric, that

$$M^T - \lambda I = M^T - (\lambda I)^T = (M - \lambda I)^T$$

Thus,

$$\det(M - \lambda I) = \det\big((M - \lambda I)^T\big) = \det\big(M^T - \lambda I\big)$$

so M, M^T have the same characteristic polynomial. Since the eigenvalues of a matrix are the roots of its characteristic polynomial, it follows that M, M^T have the same eigenvalues.

To prove that the eigenvalues of M^{-1} are the inverses of the eigenvalues of M, it will suffice to show that for every eigenvalue λ of M, λ^{-1} is an eigenvalue of M^{-1}, and for every eigenvalue γ of M^{-1}, γ^{-1} is an eigenvalue of M. Let's begin.

Suppose λ is an eigenvalue of M and $\mathbf{x}$ is a corresponding eigenvector. Then $M\mathbf{x} = \lambda\mathbf{x}$. It follows that

$$M^{-1}M\mathbf{x} = \mathbf{x} = \lambda^{-1}\lambda\mathbf{x} = \lambda^{-1}M\mathbf{x}$$

as desired.

The proof of the second statement is symmetric to that of the first. □

(i) Deduce that if $M \in \mathrm{SO}(3)$, then $M^{-1} = M^T$, and then use part (h) to deduce that 1 is an eigenvalue of M.

Proof. The proof that $M^{-1} = M^T$ is given for the general special orthogonal group $\mathrm{SO}(n)$ in part (a). Clearly, the special case $n = 3$ holds as well.

If $M^{-1} = M^T$, then $\sigma(M^{-1}) = \sigma(M^T)$[3]. Additionally, by part (h), $\sigma(M) = \sigma(M^T)$, so in this case, transitivity implies that $\sigma(M) = \sigma(M^{-1})$. Furthermore, part (h) asserts that for every $\lambda \in \sigma(M)$, we have that $\lambda^{-1} \in \sigma(M^{-1})$. Combining this with the above, we have that $\lambda \in \sigma(M)$ implies that $\lambda^{-1} \in \sigma(M)$.

Now suppose $\lambda_1, \lambda_2, \lambda_3$ are eigenvalues of M. Note that these eigenvalues need not be distinct, but they do exist (every linear transformation has at least one [possibly complex] eigenvalue). Since the inverses of each of these eigenvalues are amongst the set, too, WLOG let $\lambda_2 = \lambda_1^{-1}$. It follows that

$$1 = \det(M) = \lambda_1\lambda_2\lambda_3 = \lambda_1\lambda_1^{-1}\lambda_3 = \lambda_3$$

as desired. □

(j) Deduce that every $M \in \mathrm{SO}(3)$ is a rotation about some line $\mathbf{u}$ passing through the origin. Deduce that the composition of a rotation in $\mathbb{R}^3$ about some line $\mathbf{u}$ passing through the origin with a rotation about any second line $\mathbf{v}$ also passing through the origin is also a rotation about some third line $\mathbf{w}$ passing through the origin. Note that $\mathbf{u}, \mathbf{v}, \mathbf{w}$ need not be distinct.

Proof. Let $M \in \mathrm{SO}(3)$ be arbitrary. By part (i), 1 is an eigenvalue of M. Let $\mathbf{u}$ be the normalized corresponding eigenvector. Then $M\mathbf{u} = \mathbf{u}$, so by part (e), M is a rotation about the line $\mathbf{u}$ passing through the origin by some angle θ.

It follows since $\mathrm{SO}(3)$ is a group by part (b) (and hence closed) that for any $M, N \in \mathrm{SO}(3)$, $MN \in \mathrm{SO}(3)$ as well. In effect, the composition of a rotation in $\mathbb{R}^3$ about some line $\mathbf{u}$ passing through the origin with a rotation about any second line $\mathbf{v}$ also passing through the origin is also a rotation about some third line $\mathbf{w}$ passing through the origin, as desired. □

[3] $\sigma(A)$ denotes the **spectrum** of A, i.e., the set of all eigenvalues of the matrix A.