MATH 25700 (Honors Basic Algebra I) Problem Sets

Steven Labalme

October 17, 2022

Contents

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.

2 Cycles, Cubes, and the Dodecahedron

10/10: 1. If σ is an element of S_n, then σ has a cycle decomposition into disjoint cycles of various lengths (let us include 1-cycles). Since disjoint cycles commute, the shape of the element is determined by the lengths of the various cycles, which we can assume are put in decreasing order. Any two elements with the same cycle shape are conjugate, so the conjugacy classes are determined by writing n ($= 52$, say) as a sum of decreasing integers.

(a) Find the conjugacy class in S_{52} with the largest number of elements.

Proof. Let $52 = \sum_{i=1}^{k} c_i p_i$, where $p_1, \ldots, p_k$ is a decreasing sequence of natural numbers describing the cycle lengths present in the conjugacy class and the $c_i \in \mathbb{N}$ are their multiplicities.

There are 52! permutations of the numbers $1, \ldots, 52$. We can partition every permutation up into p_i-cycles, but in doing so, we will realize that we have overcounted in two ways.

First off, every p_i-cycle can be written in p_i equivalent ways. Thus, for every permutation $a_1, \ldots, a_{52}$, there are p_i permutations written differently that mean the same thing, so we need to divide through by p_i. Doing this for all p_i (and counting multiplicities), we need to divide through by $\prod_{i=1}^{k} p_i^{c_i}$.

Additionally, disjoint cycles commute. This means that the order in which we write the c_i p_i-cycles doesn't matter. Since there are $c_i!$ orders in which we can write the c_i p_i-cycles, we also need to divide through by $\prod_{i=1}^{k} c_i!$.

Therefore, the total number of elements in the conjugacy class $\sum_{i=1}^{k} c_i p_i$ is

$$\frac{n!}{\prod_{i=1}^{k} p_i^{c_i} \cdot c_i!}$$

This is the functional whose value we want to maximize.

To maximize the above functional, we can seek to minimize its denominator. To do so, we'll justify a couple of rules.

First, note that if $p, c \geq 2$, then

$$p^c \cdot c! > cp \cdot 1!$$

We can prove this by inducting on p and c in turn, keeping the other fixed. This rule tells us that if we want to minimize the above functional, it is to our benefit to reduce all multiplicities to 1 by combining cycles of the same length (as long as that length is greater than 1).

We are now down to only classes of the form $\sum_{i=1}^{k} x_i = \sum_{i=1}^{k} c_i p_i$. Thus, the problem becomes one of minimizing one of the two equations below, depending on whether or not $p_k = 1$ (remember that $p_1, \ldots, p_k$ is *decreasing*, so 1, if present, will be p_k).

$$\prod_{i=1}^{k} c_i p_i = \prod_{i=1}^{k} x_i \qquad\qquad \prod_{i=1}^{k-1} c_i p_i \cdot 1^{c_k} c_k! = c_k! \prod_{i=1}^{k-1} x_i$$

With respect to this kind of product, we can note that if $a, b \geq 2$, then

$$ab \geq a + b$$

Thus, it is to our benefit to combine all cycles of length greater than 1. Thus, we have reduced to the cases

$$52 \qquad\qquad c_k!(52 - c_k)$$

respectively from the above. Since the right equation above is minimized for $c_k = 1$ and, with this value, evaluates to $51 < 52$, we know that the conjugacy class in S_{52} with the largest number of elements is:

$$\boxed{\text{The conjugacy class } 52 = 51 + 1.}$$

□

(b) Find the conjugacy class in S_{52} which contains the element of largest order. (This question is somewhat computational, so an explanation of your strategy plus the answer is sufficient.)

Proof. Let $52 = \sum_{i=1}^{k} a_i$. By Exercise 1.3.15 of Dummit and Foote (2004) (and from class), the order of an element of S_n equals the least common multiple (lcm) of the lengths of the cycles in its cycle decomposition. Thus, all elements in a conjugacy class have the same order.

We now must optimize $\text{lcm}(a_1, \ldots, a_k)$ over all such decompositions. To do so, we will start with a guess based on some observations and then progressively refine according to two rules.

Observations:

(1) Rely (primarily) on relatively prime numbers. For example, the list $2, 4, 8$ has lcm $= 8$, but the list $2, 3, 5$ has lcm $= 30$, and a smaller sum.

(2) 1 should not be in the list because it does not contribute anything to the lcm but does add to the sum.

(3) Rely (primarily) on small numbers — remember the $ab \geq a + b$ rule for $a, b \geq 2$ from part (a). This means that it is often beneficial to split larger numbers into smaller numbers.

With these observations in hand, we'll use as our starting list

$$2, 3, 5, 7, 11, 13, 11$$

where we include the last 11 because $2 + \cdots + 13 = 41$ and $52 - 41 = 11$, i.e., we cannot include the first six numbers and the next prime (17) without the sum exceeding 52.

We now give the two rules for progressive refinement of the above list. The first one is that if $a_1, \ldots, a_k$ is the final list, then

$$\text{lcm}(a_1, \ldots, a_k) \geq \text{lcm}(a_1, \ldots, a_{i-1}, n, (a_i - n), a_{i+1}, \ldots, a_k)$$

for all $n < a_i$ and all $i \leq k$. The second one is that if $a_1, \ldots, a_k$ is the final list, then

$$\text{lcm}(a_1, \ldots, a_k) \geq \text{lcm}(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{j-1}, a_{j+1}, \ldots, a_k, a_i + a_j)$$

for all $i \neq j \leq k$. In particular, if we ever come across a case in which either of the above two inequalities is not satisfied, then we should redefine our list on the LHS with the list on the RHS.

Using these rules, we will first attack the second 11 in the above list. We can compute that

$$\text{lcm}(2, 3, 5, 7, 11, 13, 11) = 30030$$

and that

$$\text{lcm}(2, 3, 5, 7, 11, 13, 1, 10) = 30030$$

but that

$$\text{lcm}(2, 3, 5, 7, 11, 13, 2, 9) = 90090$$

Thus, we redefine our list to be $2, 2, 3, 5, 7, 9, 11, 13$. If we run through and check all of the cases by the first rule, we will find that there is no more splitting we can do to increase the value of this list. However, by the second rule, there is some combining: If we combine $2, 2 \mapsto 4$, then

$$\text{lcm}(3, 4, 5, 7, 9, 11, 13) = 180180$$

Running both rules, we will find that we cannot progressively refine any further from here. Therefore, the conjugacy class in S_{52} which contains the element of the largest order is:

$$\boxed{\text{The conjugacy class } 52 = 13 + 11 + 9 + 7 + 5 + 4 + 3.}$$

□

2. Let $k \leq n$ be even. Prove that every element in S_n can be written as a product of k-cycles.

Proof. Every element in S_n can be written in terms of elementary transpositions. Thus, the problem becomes one of showing that every elementary transposition can be written as a product of k-cycles.

Let $(i, i+1) \in S_n$ be an elementary transposition. We will prove that

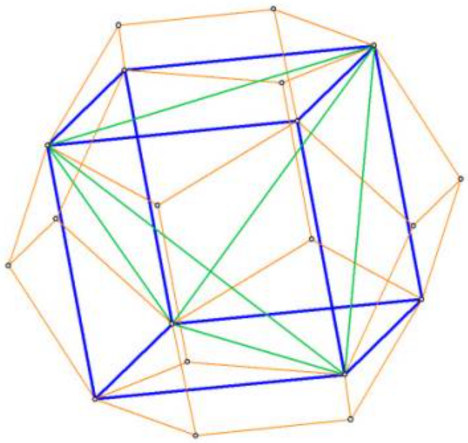
$$\begin{aligned}(i, i+1) = (i, i +_n 1, \ldots, i +_n (k-1))^2 \\ \cdot (i, i +_n (k-1), i +_n (k-3), \ldots, i +_n 3, i+1, i +_n (k-2), i +_n (k-4), \ldots, i +_n 2)\end{aligned}$$

where $+_n$ denotes addition modulo n[4]. Indeed, we have that

$$\begin{aligned}&(i, i +_n 1, \ldots, i +_n (k-1)) \\ &\cdot (i, i +_n 1, \ldots, i +_n (k-1)) \\ &\cdot (i, i +_n (k-1), i +_n (k-3), \ldots, i +_n 3, i+1, i +_n (k-2), i +_n (k-4), \ldots, i +_n 2) \\ &= (i, i +_n 1, \ldots, i +_n (k-1)) \\ &\cdot (i)(i+1, i +_n (k-1), i +_n (k-2), \ldots, i +_n 2) \\ &= (i, i +_n 1, \ldots, i +_n (k-1)) \\ &\cdot (i+1, i +_n (k-1), i +_n (k-2), \ldots, i +_n 2) \\ &= (i, i+1)\end{aligned}$$

as desired. □

3. Let D be a regular dodecahedron. You may assume for this question that it is possible to inscribe a cube C on the vertices of D as shown below.



Remember the following distinction: An object X in $\mathbb{R}^3$ is **fixed pointwise** by g if every point on X is fixed by g, that is, if $gx = x$ for all $x \in X$. An object $X \in \mathbb{R}^3$ is **preserved** by g if every point on X maps to another (possibly different) point on X, i.e., for all $x \in X$, there exists $y \in X$ such that $gx = y$. As an example, the circle centered at the origin is preserved by any rotation through the origin, but is not fixed pointwise unless the rotation is trivial.

- If F is a face, call a line between two vertices of F an **internal line** if the vertices are not adjacent. That is, an internal line is a line between two vertices of a pentagonal face which is not an edge of the pentagon.

[4]Motivation: We have, for example, that $(1,2) \in S_n$ with $k = 8$ can be given by $(1,2,3,4,5,6,7,8)^2(1,8,6,4,2,7,5,3)$. Essentially, what we are doing here is sending $1 \mapsto 8$ and $2 \mapsto 7$ so that when we rotate all of the numbers twice (with $(1,\ldots,8)^2$), 1 and 2 land in the 2 and 1 positions. The "decreasing by 2 at a time" part is a necessary consequence of writing an 8-cycle that sends $1 \mapsto 8$ and $2 \mapsto 7$ and can be more easily understood by drawing out a function diagram and tracing the cycle.

- Observe that the cube C has 12 edges, and that each edge lies on exactly one of the 12 faces of D as an internal line.
- Choose a face F of D and let g be the symmetry of D of order 5 which is a rotation by $2\pi/5$ through the line passing through the middle of F and the middle of the opposite face $-F$.
- Label the vertices of a face F from 1 to 5. Suppose that $C = C_{(1,3)}$ intersects F in the internal edge from 1 to 3.

(b) Show that for any such g, the five cubes $C_{(1,3)}$, $C_{(2,4)}$, $C_{(3,5)}$, $C_{(1,4)}$, and $C_{(2,5)}$ obtained by applying the powers of g to each cube are distinct because they intersect F in different internal lines (which are the lines between vertices indicated by the notation).

Proof. Let g be arbitrary. Choose the z-axis to be the axis about which g rotates the dodecahedron/cube. Adopt a cylindrical coordinate system (r, θ, z). Orient the remaining coordinate axes so that vertex 1 of face F lies at $(r, 0, z)$; it follows that vertices 2-5 lie at $(r, 2\pi/5, z)$, $(r, 4\pi/5, z)$, $(r, 6\pi/5, z)$, and $(r, 8\pi/5, z)$, respectively. In this coordinate system, g^n is the orthogonal transformation that sends

$$(r, \theta, z) \mapsto \left(r, \theta + \frac{2\pi n}{5}, z\right)$$

Consider $C_{(1,3)}$, which intersects F at the internal line from vertex 1 to vertex 3. Applying the powers of g sends

$$\begin{aligned}
g(1) &= g(r,0,z) = (r, 2\pi/5, z) = 2 & \qquad g(3) &= g(r, 4\pi/5, z) = (r, 6\pi/5, z) = 4 \\
g^2(1) &= g^2(r,0,z) = (r, 4\pi/5, z) = 3 & \qquad g^2(3) &= g^2(r, 4\pi/5, z) = (r, 8\pi/5, z) = 5 \\
g^3(1) &= g^3(r,0,z) = (r, 6\pi/5, z) = 4 & \qquad g^3(3) &= g^3(r, 4\pi/5, z) = (r, 2\pi, z) = (r, 0, z) = 1 \\
g^4(1) &= g^4(r,0,z) = (r, 8\pi/5, z) = 5 & \qquad g^4(3) &= g^4(r, 4\pi/5, z) = (r, 2\pi/5, z) = 2 \\
g^5(1) &= e(r,0,z) = 1 & \qquad g^5(3) &= e(r, 4\pi/5, z) = 3
\end{aligned}$$

Thus, we know that the cube $g(C_{(1,3)})$ — remember that g, as an orthogonal transformation, preserves lengths, angles, and lines, so the image of a cube under g will still be a cube — intersects F at the internal line from vertex 2 to vertex 4, the cube $g^2(C_{(1,3)})$ intersects F at the internal line from vertex 3 to vertex 5, the cube $g^3(C_{(1,3)})$ intersects F at the internal line from vertex 4 to vertex 1, the cube $g^4(C_{(1,3)})$ intersects F at the internal line from vertex 5 to vertex 2, and the cube $g^5(C_{(1,3)}) = e(C_{(1,3)}) = C_{(1,3)}$ since g is of order 5 by definition. Naturally, continuing onto higher natural numbers will just get us back to these same cubes. It follows that these cubes — which are equal to $C_{(2,4)}$, $C_{(3,5)}$, $C_{(4,1)} = C_{(1,4)}$, $C_{(5,2)} = C_{(2,5)}$, and $C_{(1,3)}$, respectively — are all distinct because they intersect F in different internal lines. □

(c) Show that *any* symmetry of D takes C to one of these five cubes. Hint: Any pair of cubes share two vertices $\mathbf{v}, \mathbf{w}$ on F lying on an internal line of F which are connected by an edge of the cube. Given a cube centered at the origin with vertices $\mathbf{v}, \mathbf{w}$ and $|\mathbf{v}| = |\mathbf{w}|$ connected by an edge, show that the eight vertices of the cube are

$$\pm\mathbf{v},\ \pm\mathbf{w},\ \pm\mathbf{u} \pm \left(\frac{\mathbf{v} - \mathbf{w}}{2}\right)$$

where $\mathbf{u}$ is the (unique up to a $\pm$ sign) vector with $3|\mathbf{u}|^2 = 2|\mathbf{v}|^2 = 2|\mathbf{w}|^2$ and $\mathbf{u} \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{w} = 0$.

Proof.

Setup: Let C be an arbitrary cube inscribed on the vertices of D, and let F be a face of D. By the second bullet point above, C intersects F at exactly one of its internal lines. Let $\mathbf{v}, \mathbf{w}$ be the vertices of F which are connected by said internal line. Define

$$\mathbf{u} = \sqrt{\frac{2}{3}}|\mathbf{v}| \cdot \frac{\mathbf{v} \times \mathbf{w}}{|\mathbf{v} \times \mathbf{w}|}$$

By the definition of the cross product, $\mathbf{u}$ is orthogonal to $\mathbf{v}, \mathbf{w}$. Additionally, the way it is defined guarantees that it satisfies the magnitude relation.

Proving the hint: We now prove that the eight vertices of C are

$$\pm\mathbf{v},\ \pm\mathbf{w},\ \pm\mathbf{u} \pm \left(\frac{\mathbf{v}-\mathbf{w}}{2}\right)$$

Let A be the determinant 1, orthogonal transformation which sends $\mathbf{v} \mapsto (a,a,a)$ and $\mathbf{w} \mapsto (-a,a,a)$ for some $a \in \mathbb{R}$. We know that such a transformation exists since it is equivalent to redrawing the basis of $\mathbb{R}^3$ such that the three axes go through the center of three adjacent faces of the cube. Since orthogonal transformations preserve the cross product, we know that

$$\begin{aligned}
A\mathbf{u} &= \frac{\sqrt{2/3}|\mathbf{v}|}{|\mathbf{v}\times\mathbf{w}|} \cdot A\mathbf{v} \times A\mathbf{w} \\
&= \frac{\sqrt{2/3}|A\mathbf{v}|}{|A\mathbf{v}\times A\mathbf{w}|} \cdot \begin{pmatrix} 0 \\ -2a^2 \\ 2a^2 \end{pmatrix} \\
&= \frac{\sqrt{2/3}\cdot\sqrt{3a^2}}{\sqrt{8a^4}} \cdot \begin{pmatrix} 0 \\ -2a^2 \\ 2a^2 \end{pmatrix} \\
&= \frac{1}{2a} \cdot \begin{pmatrix} 0 \\ -2a^2 \\ 2a^2 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ -a \\ a \end{pmatrix}
\end{aligned}$$

It follows that the full set of vertices of this cube can be expressed in terms of $\mathbf{u}, \mathbf{v}, \mathbf{w}$ as follows.

$$\begin{aligned}
(a,a,a) &= A(\mathbf{v}) \\
(-a,-a,-a) &= A(-\mathbf{v}) \\
(-a,a,a) &= A(\mathbf{w}) \\
(a,-a,-a) &= A(-\mathbf{w}) \\
(a,-a,a) &= (0,-a,a) + \left(\frac{a-(-a)}{2}, a-a, a-a\right) = A\left(\mathbf{u} + \frac{\mathbf{v}-\mathbf{w}}{2}\right) \\
(-a,-a,a) &= A\left(\mathbf{u} - \frac{\mathbf{v}-\mathbf{w}}{2}\right) \\
(a,a,-a) &= A\left(-\mathbf{u} + \frac{\mathbf{v}-\mathbf{w}}{2}\right) \\
(-a,a,-a) &= A\left(-\mathbf{u} - \frac{\mathbf{v}-\mathbf{w}}{2}\right)
\end{aligned}$$

Thus, the vertices of C are given by the arguments of A, above, as desired.

Proving the claim: To prove that any symmetry of D takes C to one of the five cubes from part (b), we will let h be an arbitrary symmetry of D and prove that h maps the eight vertices of C to the eight vertices of $C_{(1,3)}$, $C_{(2,4)}$, $C_{(3,5)}$, $C_{(1,4)}$, or $C_{(2,5)}$. Per the hint, we know that $\mathbf{v}, \mathbf{w}$ uniquely determine the remainder of the vertices of an inscribed cube. In particular, for each of the five cubes just listed, they are the unique cube which intersects F at the internal line that they do. Thus, since h will send C to some other inscribed cube, which must by observation 2 intersect F in one of the above internal lines, we know that h sends C to one of the five desired cubes. □

(d) Let $\mathbf{v}_i$ indicate the vector corresponding to vertex i of F. Deduce that there are exactly two cubes which have $\mathbf{v}_i$ as a vertex, and that the only vertices that these two cubes have in common are $\pm\mathbf{v}_i$.

Proof. We will first prove that exactly two cubes have $\mathbf{v}_i$ as a vertex. By parts (b-c), there are exactly 5 distinct cubes inscribed in D: $C_{(1,3)}$, $C_{(2,4)}$, $C_{(3,5)}$, $C_{(1,4)}$, and $C_{(2,5)}$. Since each vertex from 1-5 appears exactly twice and in exactly two different cubes according to the above list, we have the desired result for all i.

We now prove that two cubes that both have $\mathbf{v}_i$ as a vertex only share $\pm\mathbf{v}_i$. In particular, we will prove the claim for $\mathbf{v}_1$; the argument is analogous for $\mathbf{v}_2$-$\mathbf{v}_5$. Let's begin. We know that $C_{(1,3)}$ and $C_{(1,4)}$ both have $\mathbf{v}_1$ as a vertex. We also know that the two vertices these cubes have on F are $\mathbf{v}_1, \mathbf{v}_3$ and $\mathbf{v}_1, \mathbf{v}_4$, respectively. Thus, we have by part (c) that the eight vertices of the respective cubes are

$$\pm\mathbf{v}_1,\ \pm\mathbf{v}_3,\ \pm\mathbf{u}_{13} \pm \left(\frac{\mathbf{v}_1 - \mathbf{v}_3}{2}\right) \qquad \pm\mathbf{v}_1,\ \pm\mathbf{v}_4,\ \pm\mathbf{u}_{14} \pm \left(\frac{\mathbf{v}_1 - \mathbf{v}_4}{2}\right)$$

Evidently, the only overlap is at $\pm\mathbf{v}_1$ for $\mathbf{v}_3, \mathbf{v}_4$ distinct, as desired. □

(e) (*) Show that any rigid motion of D (i.e., any element of SO(3) preserving D) permutes the 5 cubes. Hint: Show that if a symmetry σ preserves the two cubes passing through $\mathbf{v}_i$, then it preserves their intersection and deduce that

$$\sigma\mathbf{v}_i = \pm\mathbf{v}_i$$

Deduce that this identity must hold for every i, and use this (and HW1) to show that this implies that σ is the identity.

Proof. We will first prove the hint. Let's begin.

Suppose σ preserves the two cubes C, C' passing through $\mathbf{v}_i$. To prove that σ preserves $C \cap C'$, it will suffice to show that σ maps every element in that set to another element of that set. Since $C \cap C' = \{\pm\mathbf{v}_i\}$ by part (d), we confirm this with two cases. For $\mathbf{v}_i$, since $\mathbf{v}_i \in C$ and σ preserves C, we know that $\sigma\mathbf{v}_i \in C$. Similarly, we know that $\sigma\mathbf{v}_i \in C'$. Thus, by the definition of a set union, $\sigma\mathbf{v}_i \in C \cap C'$, as desired. An analogous argument treats the other case.

It follows from the above that $\sigma\mathbf{v}_i \in \{\pm\mathbf{v}_i\}$. Therefore,

$$\sigma\mathbf{v}_i = \pm\mathbf{v}_i$$

as desired.

Now suppose for the sake of contradiction that $\sigma\mathbf{v}_1 = -\mathbf{v}_1$. Then for σ to be orthogonal, we must necessarily have $\sigma\mathbf{v}_i = -\mathbf{v}_i$ for all i. But then σ is an inversion with determinant -1, and is thus not a rigid motion, a contradiction. Therefore, we must have that $\sigma\mathbf{v}_i = \mathbf{v}_i$ for all i. It follows by HW1, Q2f since σ fixes (at least) two linearly independent vectors that σ is the identity. □

(f) Deduce that the symmetry group of the dodecahedron is a subgroup of S_5 of order 60.

Proof. By part (f), any rigid motion of D permutes the 5 cubes, and is thus an element of S_5. Moreover, said rigid motion must correspond to a positive-determinant matrix element of SO(3). Thus, since half of S_5 maps to SO(3) and the other half maps to $\mathrm{O}(3) \setminus \mathrm{SO}(3)$, and $|S_5| = 120$, we know that the symmetry group of the dodecahedron is a subgroup (like $\mathrm{SO}(3) \leq \mathrm{O}(3)$) of S_5 of order $120/2 = 60$. □

4. Embed the cube inside $\mathbb{R}^3$ so that the centers of each face are at

$$A = (1,0,0) \quad B = (-1,0,0) \quad C = (0,1,0) \quad D = (0,-1,0) \quad E = (0,0,1) \quad F = (0,0,-1)$$

Considering the symmetry group of C as a subgroup of SO(3), write down the matrix of SO(3) corresponding to the following elements.

(a) $\sigma = (A, C, E)(B, D, F)$.

Proof. To send $A, B \mapsto C, D \mapsto E, F \mapsto A, B$, we need to move the nonzero index in the matrix of the vector "down" by one each time. Thus, a permutation matrix will accomplish the job.

$$\boxed{\mathcal{M}(\sigma) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}}$$

□

(b) $\tau = (C, E, D, F)$.

Proof. Here, we need to (between the two indices that change) move the nonzero index down, and then up and flip the sign, and then move it down, and then up and flip the sign again. The following matrix accomplishes this.

$$\boxed{\mathcal{M}(\tau) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}}$$

□

(c) $\sigma\tau = (A, C, E)(B, D, F)(C, E, D, F) = (A, C)(B, D)(E, F)$.

Proof. Taking the product $\mathcal{M}(\sigma) \circ \mathcal{M}(\tau)$ gives us the desired matrix.

$$\boxed{\mathcal{M}(\sigma\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}}$$

□

3 Subgroups and Group Functions

10/17: 1. Let $\sigma \in S_n$ be an n-cycle, and let $\tau \in S_n$ be a 2-cycle. Show by constructing a counterexample that there exists a choice σ, τ, n such that $\langle \sigma, \tau \rangle \neq S_n$. Bonus Question: Determine for which n such an example exists.

Proof. As a particular counterexample, we may pick

$$\boxed{n = 4 \qquad \sigma = (1,2,3,4) \qquad \tau = (2,4)}$$

Notice that $\langle \sigma, \tau \rangle \cong D_4$ with $\sigma \sim r$ and $\tau \sim s$; this observation will motivate the remainder of our proof. We withhold a proof that $\langle (1,2,3,4), (2,4) \rangle \neq S_4$ in favor of proving the more general fact that for any

$$\boxed{n \geq 4}$$

we may use the n-cycle $\sigma = (1, 2, \ldots, n)$ and the 2-cycle $\tau = (2, n)$ to generate a subgroup of S_n of order $2n$. This fact will imply the desired result, as explained below. Let's begin.

We will first show that $\sigma^i \tau = \tau \sigma^{-i}$ for $i = 1, \ldots, n-1$. For the base case $n = 1$, we have by direct computation that

$$\sigma\tau = (1,2)(3,4,\ldots,n) = \tau\sigma^{-1}$$

Now suppose inductively that we have proven the claim for i. Then

$$\sigma^{i+1}\tau = \sigma(\sigma^i\tau) = \sigma(\tau\sigma^{-i}) = (\sigma\tau)\sigma^{-i} = (\tau\sigma^{-1})\sigma^{-i} = \tau\sigma^{-(i+1)}$$

as desired.

We will now prove that

$$\langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$$

via a bidirectional inclusion proof. This will imply our desired result by inspection. The right-to-left case follows directly from the definition of generators. For the left-to-right case, let $x \in \langle \sigma, \tau \rangle$ be arbitrary. Then x is equal to a finite product of σ's and τ's, i.e., $x = \tau^i \sigma^j \tau^k \sigma^\ell \cdots$. With respect to i, k, and other exponents of the τ's: If these numbers are not congruent to 1 mod 2, then that term (e.g., $\tau^i, \tau^k, \ldots$) is equal to the identity (because $|\tau| = 2$). Thus, we may rewrite $x = \tau\sigma^i\tau\sigma^j \cdots$. Invoking the above rule, we can combine that τ's further:

$$x = \tau\tau\sigma^{-i}\sigma^j \cdots = \sigma^{j-i} \cdots$$

It should not be hard to see that τ only appears in the fully condensed decomposition of x iff τ appears an odd number of times in the expanded decomposition. In other words, τ appears at most once (and when it does show up, we can make it appear on the leftmost side of the equation). Moreover, the other term will be composed entirely of σ raised to some power, which we can take mod n since $|\sigma| = n$. Thus, $x = \tau^k\sigma^i$ for some $k = 0, 1$ and $0 \leq i \leq n-1$. Therefore,

$$x \in \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$$

so we have the desired set equality. As stated above, it follows by inspection that $|\langle \sigma, \tau \rangle| = 2n$, as desired.

To have $\langle \sigma, \tau \rangle \neq S_n$, we want $2n < n!$ (recall that $|S_n| = n!$). This inequality is satisfied for $n \geq 4$, proving our result. Note that we can confirm by casework that there are no two elements $\sigma, \tau \in S_n$ for $n = 1, 2, 3$ satisfying the desired conditions:

S_1: We cannot pick a 2-cycle in S_1.

S_2: The only 2-cycle in S_2 generates the entire set.

S_3: S_3 is generated by $\langle (1,2), (2,3) \rangle$. Any 2- and 3-cycles we pick will generate these two transpositions. □

2. Shuffling Redux. Let G be the subgroup generated by the union of the following elements.

   - $(n, 53-n)$ for all n;
   - The element $(1, 2, \ldots, 26)(52, 51, \ldots, 27)$ of order 26;
   - The element $(1, 2)(51, 52)$.

   With this definition in mind, respond to the following.

   (a) Let $H = \langle (n, 53-n) \mid n \in [52] \rangle$. Prove that $H \cong (\mathbb{Z}/2\mathbb{Z})^{26}$ inside S_{52}.

   Proof. Let $a = (a_1, \ldots, a_{26})$ be a 26-tuple, every entry of which is either 1 or 0. Define $\psi : (\mathbb{Z}/2\mathbb{Z})^{26} \to H$ by

   $$\psi(a) = \bigcirc_{i=1}^{26} (i, 53-i)^{a_i}$$

   To prove that ψ is a homomorphism, it will suffice to show that $\psi(a +_2 b) = \psi(a)\psi(b)$. But we have that

   $$\begin{aligned} \psi(a +_2 b) &= \bigcirc_{i=1}^{26} (i, 53-i)^{a_i +_2 b_i} \\ &= \bigcirc_{i=1}^{26} (i, 53-i)^{a_i} \circ (i, 53-i)^{b_i} \\ &= \left[\bigcirc_{i=1}^{26} (i, 53-i)^{a_i}\right] \circ \left[\bigcirc_{i=1}^{26} (i, 53-i)^{b_i}\right] \\ &= \psi(a)\psi(b) \end{aligned}$$

   where we get from the first to the second line via: If $a_i + b_i \leq 1$, regular exponent rules hold; if $a_i, b_i = 1$, then $a_i +_2 b_i = 0$ and $(i, 53-i)^{a_i +_2 b_i} = e$ just the same as $(i, 53-i)^1 \circ (i, 53-i)^1 = (i, 53-i)^2 = e$. We get from the second to the third line since disjoint cycles commute.
   We verify bijectivity by noting that since the generators of H are disjoint 2-cycles, every element of H can be written in the form

   $$\bigcirc_{i=1}^{26} (i, 53-i)^{a_i}$$

   with every $a_i \in \{0, 1\}$. Thus, ψ^{-1} can be defined by sending each a_i to the i^{th} slot in the 26-tuple a. It will naturally follow that $\psi \circ \psi^{-1} = I = \psi^{-1} \circ \psi$, proving bijectivity. □

   (b) Show that there is a homomorphism $\phi : G \to S_{26}$ such that...

   i. ϕ is surjective;
   ii. $\ker \phi = H$.

   (It follows from this that G has order $2^{26} \cdot 26! = 2706443181710666438004021657600000$0.)

   Proof. Define $w : [52] \to [26]$ by

   $$w(i) = \begin{cases} i & i \in [26] \\ 53 - i & i \in [27:52] \end{cases}$$

   Define $\phi : G \to S_{26}$ by

   $$\phi(g) = w \circ g|_{[26]}$$

   We now prove two lemmas.

   Lemma 1: Any $f \in G$ obeys the functional rule $f(n) + f(53-n) = 53$. This follows from the facts that all generators of G obey said functional rule, f is a composition of the generators of G, and compositions of functions that obey said functional rule obey said function rule (as per HW1, Q1).
   Lemma 2: $w(i) = w(53-i)$. We divide into two cases ($i \in [26]$ and $i \in [27:52]$). If $i \in [26]$, then $53 - i \in [27:52]$, so $w(i) = i = 53 - (53-i) = w(53-i)$. If $i \in [27:52]$, then $53 - i \in [26]$, so $w(i) = 53 - i = w(53-i)$.

   To prove that ϕ actually maps elements of G to S_{26} as defined, it will suffice to show that for any $g \in G$, $\phi(g) : [26] \to [26]$ is a bijection.

Let $g \in G$ and $i \in [26]$ be arbitrary. We divide into two cases ($g(i) \in [26]$ and $g(i) \in [27:52]$). If $g(i) \in [26]$, then $w(g(i)) = g(i) \in [26]$. If $g(i) \in [27:52]$, then $w(g(i)) = 53 - g(i) \in [26]$. Therefore, $\phi(g) : [26] \to [26]$.

Now suppose $w(g(i)) = w(g(j))$. If either $g(i), g(j) \in [27:52]$, invoke Lemmas 1-2 to rewrite $w(g(x)) = w(53 - g(x)) = w(g(53 - x))$. Since g, itself, has mirror symmetry, what we are essentially doing here is guaranteeing that both $i, j \in [26]$ or $i, j \in [27:52]$; there may be distinct $i, j \in [52]$ such that $w(g(i)) = w(g(j))$ (namely, $i, 53 - i$), but we are going to show that there is only one $i, j \in [26]$ such that $w(g(i)) = w(g(j))$. Continuing, based on our rewrite, we may assume that $g(i), g(j) \in [26]$. Now let

$$w(i) = \begin{cases} w_1(i) & i \in [26] \\ w_2(i) & i \in [27:52] \end{cases}$$

where w_1, w_2 are naturally bijections. Since $g(i), g(j) \in [26]$, we have

$$\begin{aligned} w(g(i)) &= w(g(j)) \\ w_1(g(i)) &= w_1(g(j)) \\ g(i) &= g(j) \\ i &= j \end{aligned}$$

where the last line follows since $g \in S_{52}$ is a bijection by definition. Note that if $i, j \in [27:52]$, we may take $53 - i = 53 - j$ to be the unique desired element of $[26]$.

Lastly, let $j \in [26]$. It follows from the above that either $g^{-1}(w_1^{-1}(j))$ or $g^{-1}(w_2^{-1}(j))$ is an element of $[26]$, as desired.

To prove that ϕ is a homomorphism, it will suffice to show that $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$ for all $\sigma, \tau \in G$. Let $\sigma, \tau \in G$ be arbitrary. Now notice that

$$\phi(\sigma\tau) = w \circ (\sigma\tau)|_{[26]} = w(\sigma(\tau)) \qquad \phi(\sigma)\phi(\tau) = (w \circ \sigma|_{[26]}) \circ (w \circ \tau|_{[26]}) = w(\sigma(w(\tau)))$$

Thus, if we let $i \in [26]$ be arbitrary, it will suffice to show that $w(\sigma(\tau(i))) = w(\sigma(w(\tau(i))))$ to prove that ϕ is a homomorphism. We divide into two cases ($\tau(i) \in [26]$ and $\tau(i) \in [27:52]$). If $\tau(i) \in [26]$, then $w(\tau(i)) = \tau(i)$, implying the desired result. If $\tau(i) \in [27:52]$, then

$$\begin{aligned} w(\sigma(w(\tau(i)))) &= w(\sigma(53 - \tau(i))) && \text{Definition of } w \\ &= w(53 - \sigma(\tau(i))) && \text{Lemma 1} \\ &= w(\sigma(\tau(i))) && \text{Lemma 2} \end{aligned}$$

as desired.

To prove that ϕ is surjective, it will suffice to show that for all $\sigma \in S_{26}$, there exists $g \in G$ such that $\phi(g) = \sigma$. Note that this argument will be distinct (but closely related to) our earlier argument that $\phi(g)$ is surjective. Take

$$\begin{aligned} g(i) &= \begin{cases} w_1^{-1}(\sigma(w(i))) & i \in [26] \\ w_2^{-1}(\sigma(w(i))) & i \in [27:52] \end{cases} \\ &= \begin{cases} \sigma(i) & i \in [26] \\ 53 - \sigma(53 - i) & i \in [27:52] \end{cases} \end{aligned}$$

Now we must prove that $g \in G$. Recall from class that $S_{26} = \langle (1,2), (1,2,\ldots,26) \rangle$, and note that $(1,2)(52,51)$ and $(1,2,\ldots,26)(52,51,\ldots,27)$ are generators of G. It follows that $(1,2)(52,51)$ and $(1,2,\ldots,26)(52,51,\ldots,27)$ generate all elements of G that permute the elements of $[26]$, and do the same permutation symmetrically to $[27:52]$. This combined with the observations that $g : [26] \to [26]$, $g : [27:52] \to [27:52]$, and g has obeys the mirror symmetry equation

$f(n) + f(53-n) = 53$ (as is evident from its definition) proves that g is generated by these two generators, and is thus an element of G.

To prove that $\ker \phi = H$, it will suffice to show that $\phi(h) = e \in S_{26}$ for all $h \in H$. Let $h \in H$ be arbitrary. Then since h is the product of disjoint 2-cycles which are all mirror symmetric, we know that for every $i \in [26]$, h either sends $i \mapsto i$ or $i \mapsto 53 - i$. If $h : i \mapsto i$, then $w \circ h : i \mapsto i$. If $h : i \mapsto 53 - i$, then $w(h(i)) = w(53 - i) = 53 - (53 - i) = i$. Either way, $w \circ h$ is the identity on $[26]$, so $\phi(h) = e \in S_{26}$, as desired. □

(c) Prove that the group generated by the two riffle shuffles is a subgroup of G. (In fact, they are equal.)

Proof. To prove this, it will suffice to show that $A, B \in G$ because then, all products of them are naturally a subset of all products of the generators of G. Both A, B obey mirror symmetry; thus, $\phi(A), \phi(B) \in S_{26}$ because of the way ϕ is defined in part (b). It follows since ϕ is surjective that we can find, using the algorithm in part (b), elements $A', B' \in G$ such that $\phi(X') = \phi(X)$ and $X'|_{[26]} \in S_{26}$. Moreover, since A, B obey mirror symmetry, we can find $h, h' \in H$ such that $hA|_{[26]}, h'B_{[26]} \in S_{26}$. But this implies that $hA = A'$ and $hB = B'$, i.e., that $A = h^{-1}A' \in G$ and likewise for B, as desired. □

3. Let G be a finite group, and let $g, h \in G$ both have order 2. Determine the possible orders of gh.

Proof. We will prove that

$$\boxed{|gh| \text{ can be any natural number.}}$$

We divide into three cases ($|gh| = 1$, $|gh| = 2$, and $|gh| > 2$).

Suppose we want $|gh| = 1$. Consider S_2. Let $g = (1, 2)$ and $h = g^{-1} = (1, 2)$. Then clearly $|g| = |h| = 2$, but $|gh| = |e| = 1$.

Suppose we want $|gh| = 2$. Let G be some abelian group containing distinct elements of order 2 (for example, take $G = (\mathbb{Z}/2\mathbb{Z})^2$). Let g be one such element and h another. Then $(gh)^2 = ghgh = g^2h^2 = ee = e$, so $|gh| = 2$, as desired.

Suppose we want $|gh| = n$ for some $n > 2$. Consider the dihedral group D_{2n}. Let $g = rs$ and $h = s$. Then $g^2 = rsrs = rssr^{-1} = e$ and $h^2 = s^2 = e$, so $|g| = 2$ and $|h| = 2$. Moreover, $gh = rss = r$, so $|gh| = n$, as desired. □

4. Suppose that the map $\phi : G \to G$ given by $\phi(x) = x^2$ is a homomorphism. Prove that G is abelian.

Proof. To prove that G is abelian, it will suffice to show that $xy = yx$ for all $x, y \in G$. Let $x, y \in G$ be arbitrary. Then

$$xxyy = x^2y^2 = \phi(x)\phi(y) = \phi(xy) = (xy)^2 = xyxy$$

so by consecutive applications of the cancellation lemma, we have the desired result. □

5. Call a subgroup $H \subset G$ **cyclic** if $H = \langle g \rangle = \langle g, g^{-1} \rangle$ for some $g \in G$.

(a) Prove that any cyclic subgroup $H \subset G$ is abelian.

Proof. Let H be cyclic. Then $H = \langle h \rangle$. Let $x, y \in H$ be arbitrary. Then $x = h^i$ and $y = h^j$. It follows that

$$xy = h^ih^j = h^{i+j} = h^{j+i} = h^jh^i = yx$$

as desired. □

(b) Prove that any cyclic subgroup $H \subset G$ is either isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$, and that the latter happens exactly when h has finite order n.

Proof. We divide into two cases (G is infinite and G is finite).
Let $G = \langle g \rangle$ be infinite. Then

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$$

Now suppose for the sake of contradiction that $g^a = g^b$ for some distinct $a, b \in \mathbb{Z}$. Then $g^{a-b} = e$, so $|G| \leq a - b$, a contradiction. Therefore, $G = \{G^{\mathbb{Z}}\}$. In particular, we may define $\phi : \mathbb{Z} \to G$ by $k \mapsto g^k$. This map has the property that $a + b \mapsto g^a g^b$, i.e., $\phi(a)\phi(b) = \phi(ab)$.
Let $G = \langle g \rangle$ be finite. Then

$$G = \{e, g, g^2, \dots, g^{n-1}\}$$

Now suppose for the sake of contradiction that $g^a = g^b$ for some distinct $0 \leq a, b < n$ with $a > b$ WLOG. Then $g^{a-b} = e$, so $|G| \leq a - b < n$, a contradiction. Therefore, we may once again define $\phi : \mathbb{Z}/n\mathbb{Z} \to G$ as above. Note that $a + b \mapsto g^{(a+b) \mod n}$. This is still a homomorphism, though. □

(c) Let G be any group. Prove that there is a bijection between the set of homomorphisms $\{\phi : \mathbb{Z} \to G\}$ and G given by

$$\phi \mapsto \phi(1)$$

(Exercise 2.3.19 of Dummit and Foote (2004).)

Proof. To prove that the given map is bijective, it will suffice to show that it is injective and surjective.
Suppose $\phi(1) = \psi(1)$. Then if $n \in \mathbb{Z}$ is arbitrary,

$$\phi(n) = \phi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\phi(1) \cdots \phi(1)}_{n \text{ times}} = \underbrace{\psi(1) \cdots \psi(1)}_{n \text{ times}} = \psi(\underbrace{1 + \cdots + 1}_{n \text{ times}}) = \psi(n)$$

so $\phi = \psi$, as desired.
Now let $g \in G$ be arbitrary. Define $\phi : Z \to G$ by

$$\phi(n) = g^n$$

Then $\phi(1) = g$, as desired, and ϕ is a homomorphism since

$$\phi(n + m) = g^{n+m} = g^n g^m = \phi(n)\phi(m)$$

as desired. □

(d) Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic. (Exercise 2.4.15 of Dummit and Foote (2004).)

Proof. Consider

$$\boxed{H = \left\langle 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots \right\rangle}$$

with addition as the group operation. H is a proper subgroup since every element of H will necessarily have 2^k in the denominator for some $k \in \mathbb{N}_0$. Moreover, H is not cyclic: Suppose for the sake of contradiction that $H = \langle g \rangle$. Then $g = n/2^k$ for some n, k. But then $1/2^{k+1}$, for instance, is unaccounted for. □

(e) Let G be a finite group. Prove that G is equal to the union of its proper subgroups if and only if it is not cyclic.

Proof. Suppose first that G is equal to the union of its proper subgroups. Each proper subgroup is generated by some proper subset of the generators of G. For there to be a nontrivial proper subset of the set of generators, the set of generators must have cardinality greater than or equal to 2. In particular, if the cardinality of this set is not 1, then G cannot be cyclic, as desired.
Now suppose that G is not cyclic. Then $\langle g \rangle$ is a proper subgroup of G for all $g \in G$; clearly, G is equal to the union of all of these subgroups. □

6. Let p be prime, and let $G = \mathrm{GL}_2(\mathbb{F}_p)$ be the group of invertible 2×2 matrices modulo p. Prove that $|G| = (p^2 - 1)(p^2 - p)$. (See §1.4 of Dummit and Foote (2004).)

Proof. First off, note that in general, we can assume the facts of the determinant that we know over $\mathbb{R}^n, \mathbb{C}^n$ hold true independent of field.

Let

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

be a 2×2 matrix modulo p. Then $a, b, c, d \in \{0, 1, \ldots, p-1\}$. We know that A is invertible iff

$$\det(A) = ad - bc \neq 0$$

and iff the two columns $(a, c)^T, (b, d)^T$ are linearly independent.

Let's begin by counting the possible values of $(a, c)^T$. a can take on p values and c can take on p values, but in the specific case that $a = 0$, we do not want to choose $c = 0$ as well (because then $\det(A) = 0$). Thus, there are $p^2 - 1$ choices of $(a, c)^T$.

Now let's count the possible values of $(b, d)^T$ corresponding to each $(a, c)^T$. Let $(a, c)^T$ be arbitrary. WLOG assume that $a \neq 0$. We want $(b, d)^T$ to be linearly independent, but since linear independence is a requirement of both variables, we can let b be any of the p values and fix our constraint on d. We will do this. Suppose we have chosen $b \in \{0, \ldots, p-1\}$. Then $bc \in \mathbb{Z}/p\mathbb{Z}$. Moreover, since p is prime, every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a generator of the group of order p. Thus, there exists exactly one $d \in \{0, \ldots, p-1\}$ such that $ad = bc$, i.e., $ad - bc = 0$. Therefore, for any choice of b, there are $p - 1$ choice for d that preserve linear independence.

It follows that the total order of the group is

$$|G| = (p^2 - 1)p(p - 1) = (p^2 - 1)(p^2 - p)$$

as desired. □

References

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (third). John Wiley and Sons.