MATH 25700 (Honors Basic Algebra I) Problem Sets

Steven Labalme

January 2, 2023

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

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

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

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

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:

$$\boxed{\text{Every permutation of 52 cards } \textit{cannot} \text{ be obtained by some combination of riffle shuffles.}}$$

□

[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. $\square$

(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

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

Therefore,

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

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 $MM^T = M^TM = I$, we know that

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

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. $\square$

(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 $\mathbf{u}_1, \mathbf{u}_2 \in \operatorname{span}(\mathbf{v}_1, \mathbf{v}_2)$. 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. $\square$

(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. $\square$

(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 $p_1, \dots, p_k$ 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 $1, \dots, 52$. 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 $a_1, \dots, a_{52}$, 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 $p_1, \dots, p_k$ 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 $\operatorname{lcm}(a_1, \dots, a_k)$ 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 $a_1, \dots, a_k$ is the final list, then

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

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

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

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

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

and that

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

but that

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

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

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

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

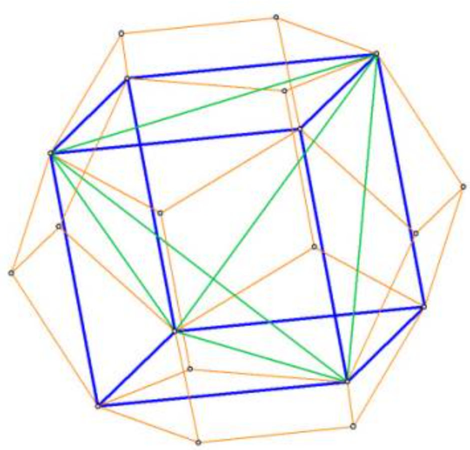
$$\begin{aligned}(i, i+1) = (i, i +_n 1, \dots, i +_n (k-1))^2 \\ \cdot (i, i +_n (k-1), i +_n (k-3), \dots, i +_n 3, i+1, i +_n (k-2), i +_n (k-4), \dots, i +_n 2)\end{aligned}$$

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

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

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 $(1, \dots, 8)^2$), 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

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

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

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

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 O(3) $\setminus$ SO(3), and $|S_5| = 120$, we know that the symmetry group of the dodecahedron is a subgroup (like SO(3) $\leq$ 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

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

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 $\sigma = (1,2,\dots,n)$ 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 $i = 1,\dots,n-1$. For the base case $n = 1$, we have by direct computation that

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

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

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

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., $\tau^i, \tau^k, \dots$) 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,

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

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. $\square$

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. $\square$

(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 $2^{26} \cdot 26! = 27064431817106664380040216576000000$.)

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 $S_{26} = \langle (1,2), (1,2,\dots,26) \rangle$, and note that $(1,2)(52,51)$ and $(1,2,\dots,26)(52,51,\dots,27)$ are generators of G. It follows that $(1,2)(52,51)$ and $(1,2,\dots,26)(52,51,\dots,27)$ 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. $\square$

(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. $\square$

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. $\square$

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. $\square$

5. Call a subgroup $H \subset G$ **cyclic** if $H = \langle g \rangle = \left\langle g, g^{-1} \right\rangle$ 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. $\square$

(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 $a, b, c, d \in \{0, 1, \dots, p-1\}$. 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 $b \in \{0, \dots, p-1\}$. 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 $d \in \{0, \dots, p-1\}$ 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. $\square$

4 Types of Subgroups

10/24: 1. Let H and K be normal subgroups of G such that $H \cap K$ is trivial. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. (Exercise 3.1.42 of Dummit and Foote (2004).)

Proof. Let $x \in H$ and $y \in K$ be arbitrary.

Since H is normal, $gxg^{-1} \in H$ for all $g \in G$. Choosing $g = y^{-1}$ reveals that $y^{-1}xy \in H$. Additionally, we know since H is a subgroup that $x^{-1} \in H$. It similarly follows that $x^{-1}y^{-1}xy \in H$.

Similarly, $x^{-1}y^{-1}x \in K$ and $y \in K$ imply that $x^{-1}y^{-1}xy \in K$.

Having proven that $x^{-1}y^{-1}xy \in H$ and $x^{-1}y^{-1}xy \in K$, we know that $x^{-1}y^{-1}xy \in H \cap K = \{e\}$. Therefore,

$$\begin{aligned} x^{-1}y^{-1}xy &= e \\ xy &= yx \end{aligned}$$

as desired. □

2. Show that S_4 does not have a normal subgroup of order 3 or order 8.

Proof. Suppose for the sake of contradiction that N be a normal subgroup of order 3 or 8. We know that N is a subgroup; thus, $e \in N$. We also know that N is a union of conjugacy classes. Thus, if we include any other cycle of a given shape in N, we know that all cycles of that shape are elements of N. Since there are 5 cycles of shape (xx), 8 cycles of shape (xxx), 6 cycles of shape $(xxxx)$, and 3 cycles of shape $(xx)(xx)$, and 1 plus the sum of any combination of these numbers does not equal 3 or 8, we have arrived at a contradiction. □

3. If H is a subgroup of G, define the **normalizer** of H to be

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

(a) Prove that $N_G(H) = G$ if and only if H is normal.

Proof. Suppose first that $N_G(H) = G$. Then $gHg^{-1} = H$ for all $g \in G$. It follows that $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$. Therefore, by the definition of normality, H is normal, as desired.

Now suppose that H is normal. Then $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. Additionally, if $h' \in H$, then $h = g^{-1}h'g \in H$ by hypothesis, so $h' = ghg^{-1} \in gHg^{-1}$. It follows by the definition of set equality that $gHg^{-1} = H$ for all $g \in G$. But by the definition of $N_G(H)$, this means that $N_G(H) = G$, as desired. □

(b) Prove that $N_G(H)$ contains H.

Proof. Let $h \in H$ be arbitrary. To prove that $h \in N_G(H)$, it will suffice to show that $hHh^{-1} = H$. We will do this with a bidirectional inclusion argument. Suppose first that $hh'h^{-1} \in hHh^{-1}$. Then since $h, h' \in H$ by hypothesis and H is a subgroup (i.e., is closed under multiplication), we have that $hh'h^{-1} \in H$, as desired. Now let $h'' \in H$. Then choosing $h' = h^{-1}h''h \in H$, we have that $h'' = hh'h^{-1} \in hHh^{-1}$, as desired. □

(c) Prove that H is a **normal** subgroup of $N_G(H)$.

Proof. H is a clearly a subgroup of $N_G(H)$: H is a subset of $N_G(H)$ by part (b) and H is nonempty, closed under multiplication, closed under inverses, and associative as a subgroup of G. All that remains now is to prove that H is normal.

To prove that $H \triangleleft N_G(H)$, it will suffice to show that for all $g \in N_G(H)$, $gHg^{-1} \subset H$. But we have this by the definition of $N_G(H)$, as desired. □

(d) Compute $N_G(H)$ for the following pairs (G, H).

i. $(S_4, \langle(1,2,3,4)\rangle)$.

Proof. We will first prove a lemma.

Lemma: Let $H = \langle x\rangle = \langle y\rangle$ be a subgroup of G. If $gxg^{-1} = y$, then $gHg^{-1} = H$.
Proof: We proceed via a bidirectional inclusion argument. Suppose first that $ghg^{-1} \in gHg^{-1}$. Since $h \in H$ by hypothesis, $h = x^n$ for some $n \in \mathbb{N}$. Therefore, since $gxg^{-1} = y \in H$ and by the closure of H, $ghg^{-1} = gx^n g^{-1} = (gxg^{-1})^n \in H$, as desired. Now suppose that $h' \in H$. Then $h' = y^n = gx^n g^{-1} \in gHg^{-1}$, as desired. Q.E.D.

Let $x = (1,2,3,4)$. We know that

$$gxg^{-1} = (g(1), g(2), g(3), g(4))$$

There are two 4-cycles in H, each of which can be written in four ways:

$$\begin{array}{cc} (1,2,3,4) & (1,4,3,2) \\ (2,3,4,1) & (2,1,4,3) \\ (3,4,1,2) & (3,2,1,4) \\ (4,1,2,3) & (4,3,2,1) \end{array}$$

Thus, the values of g that make gxg^{-1} equal to one of the above are

$$\begin{array}{rr} e & (2,4) \\ (1,2,3,4) & (1,2)(3,4) \\ (1,3)(2,4) & (1,3) \\ (1,4,3,2) & (1,4)(2,3) \end{array}$$

Letting $y = (4,3,2,1)$, we have $H = \langle x\rangle = \langle y\rangle$ and $gxg^{-1} \in \{x, y\}$ for all of the above g and our chosen x. Thus, by the lemma, $gHg^{-1} = H$ for all of the above g. It follows that they are all elements of $N_G(H)$.
Moreover, any value of g that would make $g(1,3)(2,4)g^{-1}$ equal to some other value of H has already been included in the above list, so we have no additional cases to check from there.
Of course, all $g \in G$ satisfy $geg^{-1} \in H$, the g there that have not already been mentioned would take gxg^{-1} outside of H.
Therefore,

$$\boxed{N_G(H) = \{e, (2,4), (1,2,3,4), (1,2)(3,4), (1,3)(2,4), (1,3), (1,4,3,2), (1,4)(2,3)\}}$$

□

ii. $(S_5, \langle(1,2,3,4,5)\rangle)$.

Proof. Let $x = (1,2,3,4,5)$. As before, we know that

$$gxg^{-1} = (g(1), g(2), g(3), g(4), g(5))$$

There are four 5-cycles in H, each of which can be written in five ways:

$$\begin{array}{cccc} (1,2,3,4,5) & (1,3,5,2,4) & (1,4,2,5,3) & (1,5,4,3,2) \\ (2,3,4,5,1) & (2,4,1,3,5) & (2,5,3,1,4) & (2,1,5,4,3) \\ (3,4,5,1,2) & (3,5,2,4,1) & (3,1,4,2,5) & (3,2,1,5,4) \\ (4,5,1,2,3) & (4,1,3,5,2) & (4,2,5,3,1) & (4,3,2,1,5) \\ (5,1,2,3,4) & (5,2,4,1,3) & (5,3,1,4,2) & (5,4,3,2,1) \end{array}$$

Thus, the values of g that make gxg^{-1} equal to one of the following are

$$\begin{array}{cccc}
e & (2,3,5,4) & (2,4,5,3) & (2,5)(3,4) \\
(1,2,3,4,5) & (1,2,4,3) & (1,2,5,4) & (1,2)(3,5) \\
(1,3,5,2,4) & (1,3,2,5) & (1,3,4,2) & (1,3)(4,5) \\
(1,4,2,5,3) & (1,4,5,2) & (1,4,3,5) & (1,4)(2,3) \\
(1,5,4,3,2) & (1,5,3,4) & (1,5,2,3) & (1,5)(2,4)
\end{array}$$

Since each of the four 5-cycles generates H, we have by the lemma to part (d)i that gHg^{-1} for all of the above g. It follows that they are all elements of $N_G(H)$. Therefore,

$$\boxed{\begin{aligned}
N_G(H) = \{&e, (2,3,5,4), (2,4,5,3), (2,5)(3,4), \\
&(1,2,3,4,5), (1,2,4,3), (1,2,5,4), (1,2)(3,5) \\
&(1,3,5,2,4), (1,3,2,5), (1,3,4,2), (1,3)(4,5) \\
&(1,4,2,5,3), (1,4,5,2), (1,4,3,5), (1,4)(2,3) \\
&(1,5,4,3,2), (1,5,3,4), (1,5,2,3), (1,5)(2,4)\}
\end{aligned}}$$

□

4. Prove that the subgroup N generated by elements of the form $x^{-1}y^{-1}xy$ for all $x, y \in G$ is normal. (Exercise 3.1.41 of Dummit and Foote (2004).)

Proof. To prove that N is normal, it will suffice to show that for all $z \in N$ and $g \in G$, $gzg^{-1} \in N$. Let $x^{-1}y^{-1}xy \in N$ and $g \in G$ be arbitrary. Then

$$\begin{aligned}
gx^{-1}y^{-1}xyg^{-1} &= gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} \\
&= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\
&= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\
&\in N
\end{aligned}$$

as desired. □

5. Prove that if $G/Z(G)$ is cyclic, then G is abelian. (For a hint, see Exercise 3.1.36 of Dummit and Foote (2004).)

Proof. We first prove the hint. Let $G/Z(G) = \langle xZ(G) \rangle$ and let $\sigma \in G$ be arbitrary. Then $\sigma \in [xZ(G)]^a$ for some $a \in \mathbb{Z}$. It follows by the rules of coset multiplication that $\sigma \in x^aZ(G)$. Therefore, $\sigma = x^az$ for some $a \in \mathbb{Z}$ and $z \in Z(G)$, as desired.

To prove that G is abelian, it will suffice to show that for all $\sigma, \tau \in G$, $\sigma\tau = \tau\sigma$. Let $\sigma, \tau \in G$ be arbitrary. Let $\sigma = x^az$ and $\tau = x^bz'$. Then since elements of $Z(G)$ — such as z, z' — commute with any $g \in G$ and exponents commute with each other, we have that

$$\sigma\tau = x^azx^bz' = zx^ax^bz' = zx^bx^az' = x^bz'x^az = \tau\sigma$$

as desired. □

6. Let G be a finite group, and let $H \subset G$ be a subgroup of index two — i.e., $|G|/|H| = 2$. Prove that H is normal.

Proof. To prove that H is normal, it will suffice to show that $gH = Hg$ for all $g \in G$. Let $g \in G$ be arbitrary. We divide into two cases ($g \in H$ and $g \notin H$).

Suppose first that $g \in H$. Let $gh \in gH$ be arbitrary. Then by closure under multiplication, $gh \in H$. Choosing $h' = ghg^{-1} \in H$, it follows that $gh = h'g \in Hg$, as desired. The proof that $gH \supset Hg$ is analogous.

Now suppose that $g \notin H$. Since $[G : H] = 2$, G can be partitioned into the disjoint union of H and the coset gH or, symmetrically, H and the coset Hg. It follows that

$$gH = G \setminus H = Hg$$

as desired. $\square$

7. Let G be a finite group, and let $H \subset G$ be a subgroup of index three — i.e., $|G|/|H| = 3$. Show that H is not necessarily normal.

Proof. Let $G = S_3$, $H = \langle (1,2) \rangle$, $h = (1,2)$, and $g = (1,3)$. Since $|G| = 6$ and $|H| = 2$, $[G : H] = 6/2 = 3$. Additionally, $ghg^{-1} = (2,3) \notin H$, so H is not normal, as desired. $\square$

8. **Automorphism Groups**. Define an automorphism of a group G to be an isomorphism $\phi : G \to G$ from G to itself. (See §4.4 of Dummit and Foote (2004).)

   (a) Prove that the identity map is an automorphism.

   Proof. To prove that the identity map ι on an arbitrary group G is an automorphism, it will suffice to show that ι is a homomorphism, injective, surjective, and sends $G \mapsto G$.
   Homomorphism:
   $$\iota(xy) = xy = \iota(x)\iota(y)$$
   Injective:
   $$\iota(x) = \iota(x') \quad \Longleftrightarrow \quad x = x'$$
   Surjective: If $x \in G$, $\iota(x) = x$.
   Naturally, $\iota : G \to G$. $\square$

   (b) Prove that the composition of two automorphisms is an automorphism.

   Proof. Suppose ϕ, ψ are automorphisms on a group G; we seek to prove that $\phi \circ \psi$ is an automorphism. To do so, it will suffice to show that $\phi \circ \psi$ is a homomorphism, injective, surjective, and sends $G \to G$.
   Homorphism:
   $$[\phi \circ \psi](xy) = \phi(\psi(xy)) = \phi(\psi(x)\psi(y)) = \phi(\psi(x))\phi(\psi(y)) = [\phi \circ \psi](x) \cdot [\phi \circ \psi](y)$$
   Injective:
   $$\begin{aligned} [\phi \circ \psi](x) &= [\phi \circ \psi](x') \\ \phi(\psi(x)) &= \phi(\psi(x')) \\ \psi(x) &= \psi(x') \\ x &= x' \end{aligned}$$
   Surjective: If $z \in G$, then the surjectivity of ϕ implies that there exists $y \in G$ such that $\phi(y) = x$. Similarly, there exists $x \in G$ such that $\psi(x) = y$. It follows that
   $$z = \phi(\psi(x)) = [\phi \circ \psi](x)$$
   $\psi(G) = G$ and $\phi(G) = G$, so
   $$[\phi \circ \psi](G) = \phi(\psi(G)) = \phi(G) = G$$
   as desired. $\square$

(c) Prove that the set of automorphisms forms a group under composition. We will call this group $\text{Aut}(G)$.

Proof. To prove that $\text{Aut}(G)$ is a group, it will suffice to show that $\text{Aut}(G)$ contains an identity element, is closed under inverses, and is associative.
Identity: Per part (a), we may choose ι to be the identity element of $\text{Aut}(G)$. Indeed, if $\phi \in \text{Aut}(G)$ and $g \in G$ are arbitrary, then

$$[\phi \circ \iota](g) = \phi(\iota(g)) = \phi(g) = \iota(\phi(g)) = [\iota \circ \phi](g)$$

Inverses: Since ϕ is a bijection, $\phi^{-1} : G \to G$ is a well-defined automorphism in its own right. We can prove in an analogous manner to the above that $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = e$.
Associativity: Let $f, g, h \in \text{Aut}(G)$ and $x \in G$ be arbitrary. Then

$$[(f \circ g) \circ h](x) = [f \circ g](h(x)) = f(g(h(x))) = f([g \circ h](x)) = [f \circ (g \circ h)](x)$$

□

(d) If $g \in G$ is a fixed element, prove that the map $\phi_g : G \to G$ given by $\phi_g(x) = gxg^{-1}$ is an isomorphism.

Proof. To prove that ϕ_g is an isomorphism, it will suffice to show that it is a homomorphism, injective, and surjective.
Homomorphism:

$$\phi_g(xy) = gxyg^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$$

Injective:

$$\begin{aligned} \phi_g(x) &= \phi_g(x') \\ gxg^{-1} &= gx'g^{-1} \\ x &= x' && \text{Cancellation Lemma} \end{aligned}$$

Surjective: Let $y \in G$ be arbitrary. Choose $x = g^{-1}yg$. Then

$$y = (gg^{-1})y(gg^{-1}) = g(g^{-1}yg)g^{-1} = gxg^{-1} = \phi_g(x)$$

□

(e) Prove that the map $\psi : G \to \text{Aut}(G)$ given by $\psi(g) = \phi_g$ (sending the element g to the automorphism ϕ_g) is a homomorphism of groups.

Proof. Let $x, y, g \in G$ be arbitrary. Then we have that

$$[\psi(xy)](g) = \phi_{xy}(g) = (xy)g(xy)^{-1} = xygy^{-1}x^{-1} = x\phi_y(g)x^{-1} = \phi_x(\phi_y(g)) = [\phi_x \circ \phi_y](g)$$

as desired. □

(f) Prove that the kernel of the map $\psi : G \to \text{Aut}(G)$ is the center

$$Z(G) = \{g \in G \mid gx = xg,\ \forall x \in G\}$$

Proof. To prove that $\ker\psi = Z(G)$, we will use a bidirectional inclusion argument.
Suppose first that $g \in \ker\psi$. Then $\iota = \psi(g) = \phi_g$. It follows that $gxg^{-1} = \phi_g(x) = \iota(x) = x$ for all $x \in X$, but this directly implies that $gx = xg$ for all $x \in G$.
The proof is symmetric in the reverse direction. □

(g) Define the inner automorphism group $\text{Inn}(G)$ of G to be the subgroup of $\text{Aut}(G)$ given by the image of G under ψ. Prove that $\text{Inn}(G)$ is a normal subgroup of $\text{Aut}(G)$.

Proof. We have from the lemma in class that $\operatorname{Inn}(G) = \operatorname{im}\psi$ is a subgroup of $\operatorname{Aut}(G)$ since ψ is a homomorphism.

To prove that $\operatorname{Inn}(G)$ is normal, it will suffice to show that if $\phi_g = \psi(g) \in \operatorname{Inn}(G)$ and $\varphi \in \operatorname{Aut}(G)$, then $\varphi\phi_g\varphi^{-1} \in \operatorname{Inn}(G)$. Let $\phi_g \in \operatorname{Inn}(G)$, $\varphi \in \operatorname{Aut}(G)$, and $x \in G$ be arbitrary. Then we have that

$$\begin{aligned}
[\varphi\phi_g\varphi^{-1}](x) &= \varphi(\phi_g(\varphi^{-1}(x))) \\
&= \varphi(g\varphi^{-1}(x)g^{-1}) \\
&= \varphi(g)\varphi(\varphi^{-1}(x))\varphi(g^{-1}) \\
&= \varphi(g)x\varphi(g)^{-1} \\
&= \phi_{\varphi(g)}(x) \\
&\in \operatorname{Inn}(G)
\end{aligned}$$

as desired. $\square$

(h) Show that if G is abelian, then $\operatorname{Inn}(G)$ is trivial.

Proof. Suppose G is abelian. Then $gx = xg$ for all $g, x \in G$. It follows that $Z(G) = G$. Thus, by part (f), $\ker\phi = Z(G) = G$, meaning that $\operatorname{Inn}(G) = \operatorname{im}\psi = \{\iota\}$, as desired. $\square$

(i) Let $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$. Prove that...

i. $\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z}) = \operatorname{Out}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$;

Proof. $\mathbb{Z}/3\mathbb{Z}$ is abelian. Thus, by part (h), $\operatorname{Inn}(\mathbb{Z}/3\mathbb{Z})$ is trivial. It follows that $\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z}) = \operatorname{Out}(\mathbb{Z}/3\mathbb{Z})$ as desired.

Constructing ψ: Let $\psi : \operatorname{Aut}(G) \to \mathbb{Z}/2\mathbb{Z}$ be the isomorphism we seek to construct. First notice that since $\mathbb{Z}/3\mathbb{Z}$ is cyclic, any homomorphism $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ is uniquely determined by $\phi(1)$. Indeed, if we know $\phi(1)$, then $\phi(n) = n\phi(1)$. Since $\phi(1)$ can have three possible values, we divide into three cases. If $\phi_1(1) = 0$, then ϕ_1 sends every element of $\mathbb{Z}/3\mathbb{Z}$ to zero. Thus, ϕ_1 is not surjective, so $\phi_1 \notin \operatorname{Aut}(G)$. If $\phi_2(1) = 1$, then $\phi_2(n) = n$, i.e., $\phi_2 = \iota$. Thus, take $\psi(\phi_2) = 0$. It follows that ϕ_3 defined by

$$1 \mapsto 2 \qquad 2 \mapsto 1 \qquad 0 \mapsto 0$$

must be sent by ψ to $1 \in \mathbb{Z}/2\mathbb{Z}$.

Verifying that ψ is an isomorphism: We have mapped the two distinct elements of $\operatorname{Aut}(G)$ to the two distinct elements of $\mathbb{Z}/2\mathbb{Z}$. Therefore, ψ is injective and surjective. Moreover, ψ is a homomorphism since

$$\begin{aligned}
\psi(\phi_2 \circ \phi_2) = \psi(\phi_2) = 0 = 0 + 0 = \psi(\phi_2) + \psi(\phi_2) \\
\psi(\phi_2 \circ \phi_3) = \psi(\phi_3) = 1 = 0 + 1 = \psi(\phi_2) + \psi(\phi_3) \\
\psi(\phi_3 \circ \phi_2) = \psi(\phi_3) = 1 = 1 + 0 = \psi(\phi_3) + \psi(\phi_2) \\
\psi(\phi_3 \circ \phi_3) = \psi(\phi_2) = 0 = 1 + 1 = \psi(\phi_3) + \psi(\phi_3)
\end{aligned}$$

$\square$

ii. $\operatorname{Out}(S_3) = \{1\}$;

Proof. S_3 is not abelian. In fact, it contains no nontrivial elements which commute: We know that disjoint cycles commute, but in S_3, any nontrivial cycle is of length at least 2 and thus must share an element with another cycle of length at least 2. Thus $Z(S_3) = \{e\}$. It follows by part (f) that $\psi : S_3 \to \operatorname{Aut}(S_3)$ is an isomorphism. Thus, $\operatorname{Inn}(G) = \operatorname{Aut}(G)$. It follows that $\operatorname{Out}(G) = \{1\}$, as desired. $\square$

iii. $\operatorname{Aut}(K) \cong \operatorname{Out}(K) \cong S_3$, where $K = (\mathbb{Z}/2\mathbb{Z})^2$ is the Klein 4-group.

Proof. K is abelian; hence, by part (h), $\mathrm{Aut}(K) \cong \mathrm{Out}(K)$.
$K = \langle (0,1), (1,0) \rangle$; hence, any $\phi \in \mathrm{Aut}(K)$ is uniquely defined by its action on $(0,1)$ and $(1,0)$. In particular, since ϕ is a homomorphism, we know $\phi(0,0) = (0,0)$. Additionally, whichever element of $\{(0,1),(1,0),(1,1)\}$ is not in $\phi(\{(0,1),(1,0)\})$ is the element to which ϕ maps $(1,1)$. Thus, we can define an isomorphism from $\psi : \mathrm{Aut}(G) \to S_3$ as follows. Let $f : K \setminus \{(0,0)\} \to [3]$ be defined by

$$(0,1) \mapsto 1 \qquad (1,0) \mapsto 2 \qquad (1,1) \mapsto 3$$

Then define ψ by

$$\psi(\phi) = f \circ \phi \circ f^{-1}$$

It follows by an analogous argument to that used in part (d) that ψ is an isomorphism. $\square$

9. Let p be an odd prime number. Prove that there are no surjective homomorphisms from S_n to $\mathbb{Z}/p\mathbb{Z}$ for any prime p. (Hint: Consider the image of the two-cycles).

Proof. Let $\phi : S_n \to \mathbb{Z}/p\mathbb{Z}$ be an arbitrary homomorphism. Let $(a,b) \in S_n$ be an arbitrary 2-cycle. By Lagrange's theorem, $|\phi(a,b)|$ divides $|\mathbb{Z}/p\mathbb{Z}|$, i.e, $|\phi(a,b)| \in \{1,p\}$. Additionally, we have that

$$2\phi(a,b) = \phi[(a,b) \circ (a,b)] = \phi(e) = 0$$

i.e., $|\phi(a,b)| \leq 2$. Thus, $|\phi(a,b)| = 1$. It follows that $\phi(a,b) = 0$ for all $(a,b) \in S_n$. But since a homomorphism is uniquely defined by its action on the generators and the 2-cycles generate S_n, this means that ϕ is the trivial homomorphism. Therefore, since all homomorphisms from S_n to $\mathbb{Z}/p\mathbb{Z}$ are equal to the trivial one (which is not surjective), we know that there are no surjective homomorphisms from S_n to $\mathbb{Z}/p\mathbb{Z}$, as desired. $\square$

5 Group Structure Applications

11/7: 1. Automorphisms of S_n.

(a) Let $\psi : G \to G$ be an isomorphism. If $\{c\}$ is a conjugacy class of G, prove that the image $\psi(\{c\})$ of $\{c\}$ under ψ is the conjugacy class $\{\psi(c)\}$.

(b) Deduce that $|\{c\}| = |\{\psi(c)\}|$.

(c) Let $G = S_n$. Prove that $|\{(1,2)\}| = n(n-1)/2$.

(d) If $n \neq 6$ and $\sigma \in S_n$ has order 2, prove that $|\{\sigma\}| = |\{(1,2)\}|$ if and only if σ is a 2-cycle.

(e) Deduce that if $\psi : S_n \to S_n$ is an isomorphism and $n \neq 6$, then ψ takes 2-cycles to 2-cycles.

(f) Suppose that $\psi[(1,2)] = (i,j)$. Prove that, after possibly swapping i and j, $\psi[(1,3)] = (i,k)$ for some $k \notin \{i,j\}$.

(g) Let $g \in S_n$ denote any element with $g(i) = 1$, $g(j) = 2$, and $g(k) = 3$. Let ϕ_g be the (inner) automorphism of S_n given by conjugation by g. After replacing ψ by $\phi_g \circ \psi$, deduce that one can assume that $\psi[(1,2)] = (1,2)$ and $\psi[(1,3)] = (1,3)$.

(h) Assume that $\psi(1,i) = (1,i)$ for all $i < k$ with $k > 3$. Prove that $\psi(1,k) = (1,j)$ for some $j \geq k$. As in part (g), show that after replacing ψ by $\phi_h \circ \psi$ for some h, one can assume in addition that $\psi[(1,k)] = (1,k)$.

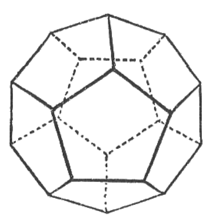
(i) Deduce that ψ is the identity, and hence that any automorphism of S_n (for $n \neq 6$) is given by conjugation, i.e., $\text{Out}(S_n) = 1$ for $n \neq 6$.

2. Let H be a finite subgroup of G of index n. Let A be the set of left cosets G/H, and consider the left action of G on A. (See Exercise 4.2.8 of Dummit and Foote (2004).)

(a) Let $n = |G/H|$, and consider the associated homomorphism $G \to S_{G/H} \cong S_n$. Prove that the kernel of this map is a subgroup of H.

(b) By considering the kernel of the map $G \to S_n$, deduce that G contains a normal subgroup N contained in H of index dividing $n!$ and divisible by n.

3. Let Do $\cong A_5$ denote the symmetry group of the dodecahedron. Fill out the missing entries in the table below for various sets X on which Do acts transitively. Since the action of Do is transitive for each X, all stabilizers S for any point $x \in X$ are conjugate to the stabilizers of any other point. Hence, they are isomorphic as subgroups; simply list a group (from our known list of groups: symmetric, alternating, dihedral, cyclic, quaternion, etc.) isomorphic to any of the stabilizers.



Dodecahedron.

Proof.

X	$\lvert X\rvert$	Faithful?	Stab(x)	$\lvert S\rvert$
Dodecahedra	1	No	$S = \text{Do} \cong A_5$	60
Inscribed cubes				
Pairs of opposite faces				
Faces				
Vertices				
Edges				

□

6 Theory of Group Actions

11/14: You should think about and try to solve the starred questions, but several of them are quite messy and some are difficult, so only submit the ones without stars.

1. Exercises 4.1.7-4.1.8 of Dummit and Foote (2004).

7. Let G be a transitive permutation group on the finite set A. A **block** is a nonempty subset B of A such that for all $\sigma \in G$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B)$ is the set $\{\sigma(b) \mid b \in B\}$).

(a) Prove that if B is a block containing the element $a \in A$, then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.

Proof. To prove that G_B is a subgroup, it will suffice to show that G_B is nonempty, closed under multiplication, and closed under inverses. Since we naturally have $e(B) = B$, G_B is nonempty. Suppose $\sigma, \tau \in G_B$. Then $\sigma(B) = B$ and $\tau(B) = B$. It follows that $[\sigma \cdot \tau](B) = \sigma(\tau(B)) = \sigma(B) = B$, so $\sigma \cdot \tau \in G_B$ as well. Thus, G_B is closed under multiplication. Now suppose $\sigma \in G_B$. Then $\sigma(B) = B$. It follows since σ is bijective that $\sigma^{-1}(B) = B$ as well. Thus, $\sigma^{-1} \in G_B$, and hence G_B is closed under inverses.

We know that $G_a = \{\sigma \in G \mid \sigma(a) = a\}$. To prove that $G_a \subset G_B$, it will suffice to show that every $\sigma \in G_a$ is an element of G_B. Let $\sigma \in G_a$ be arbitrary. Since B is a block, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. Suppose for the sake of contradiction that $\sigma(B) \cap B = \emptyset$. Since $\sigma(a) = a$, we have that $\sigma(a) \in B$ and $\sigma(a) \in \sigma(B)$. Consequently, $\sigma(a) \in \sigma(B) \cap B$, a contradiction. Therefore, $\sigma(B) = B$, and $\sigma \in G_B$, as desired. $\square$

(b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \dots, \sigma_n(B)$ are all the distinct images of B under the elements of G, then these form a partition of A.

Proof. To prove that the $\sigma_i(B)$ form a partition of A, it will suffice to show that they are pairwise disjoint and that all $a \in A$ lie in some $\sigma_i(B)$.

Suppose for the sake of contradiction that there exist $1 \leq i \neq j \leq n$ such that $\sigma_i(B) \cap \sigma_j(B) \neq \emptyset$. Then there exists an $a \in A$ such that $a = \sigma_i b = \sigma_j b'$ for some $b, b' \in B$. Since $\sigma_i b = \sigma_j b'$, $b = \sigma_i^{-1}\sigma_j b'$. It follows that $b \in \sigma_i^{-1}\sigma_j(B)$ and $b \in B$, so $b \in \sigma_i^{-1}\sigma_j(B) \cap B$, a contradiction.

Let $a \in A$ be arbitrary, and pick some $b \in B$. Since the action is transitive, there exists $\sigma \in G$ such that $\sigma(b) = a$. Thus, $a \in \sigma(B)$. But since $\sigma_1(B), \sigma_2(B), \dots, \sigma_n(B)$ encapsulates *all* distinct images of B under the elements of G, $\sigma(B) = \sigma_i(B)$ for some $1 \leq i \leq n$, as desired. $\square$

(c) A (transitive) group G on a set A is said to be **primitive** if the only blocks in A are the trivial ones: The sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.

Proof. To prove that S_4 is primitive on A, it will suffice to show that if $B \subset A$ contains 2 or 3 elements, then there exists $\sigma \in S_4$ such that $\emptyset \neq \sigma(B) \cap B \neq B$. Let $B \subset A$ contain 2 or 3 elements. Pick $a \in A \setminus B$ and $b \in B$. Then $\sigma = (a, b) \in S_4$ guarantees that at least one element of B is left in $\sigma(B)$ and one element is taken out, meaning that $\emptyset \neq \sigma(B) \cap B \neq B$, as desired.

To prove that D_8 is not primitive on A (where $1, 2, 3, 4$ denote the four vertices of a square going clockwise), it will suffice to find a block $B \subset A$ with cardinality not equal to 1 or 4. Choose $B = \{1, 3\}$. Then if r is a clockwise rotation by $90°$ and s is a reflection along the diagonal from vertex 1 to 3, $e, r^2, s, sr^2 : B \mapsto B$ and $r, r^3, sr, sr^3 : B \mapsto A \setminus B$. $\square$

(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a **maximal** subgroup of G). *Hint.* See Exercise 2.4.16. Use part (a).

Proof. Suppose first that G acts transitively and is primitive on A. Let $a \in A$ be arbitrary, and let $H \leq G$ contain G_a. Define $B = \{h(a) \mid h \in H\}$. We now seek to prove that B is a block.

To prove that B is a block, it will suffice to show that for all $\sigma \in G$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. Let $\sigma \in G$ be arbitrary. We divide into two cases ($\sigma \in H$ and $\sigma \notin H$).

If $\sigma \in H$, then every $\sigma h(a) \in \sigma(B)$ is an element of B since $\sigma, h \in H$ implies $\sigma h \in H$ implies $\sigma h(a) \in B$. Thus, $\sigma(B) = B$ in this case. If $\sigma \notin H$, then suppose for the sake of contradiction that $\sigma(B) \cap B \neq \emptyset$. Let $b \in \sigma(B) \cap B$. Then $b = \sigma(h(a))$ for some $h(a) \in B$ and $b = h'(a)$ for some $h'(a) \in B$. It follows that $\sigma h(a) = h'(a)$. Consequently, ${h'}^{-1}\sigma h \cdot a = a$, so ${h'}^{-1}\sigma h \in G_a \subset H$. But if ${h'}^{-1}\sigma h \in H$, then $\sigma \in h'Hh^{-1} = H$, a contradiction. Therefore, B is a block.
Having proven that B is a block, we complete the proof in this direction. Since G is primitive, $B = G$ or $|B| = 1$. If $B = G$, then $H = G$. If $|B| = 1$, then since $e \in H$ implies $e(a) = a \in B$, the definition of B implies that every $h \in H$ makes $h(a) = a$. But this means that $H \leq G_a$; this combined with the hypothesis that $G_a \leq H$ means that $H = G_a$.

Now suppose that for each $a \in A$, the G_a is a maximal subgroup of G. To prove that (the transitive group) G is primitive on A, it will suffice to show that the only blocks in A are the trivial ones. Let B be an arbitrary block in A. Pick an $a \in B$. By part (a), $G_a \leq G_B \leq G$. It follows by the hypothesis that G_a is maximal that $G_B = G_a$ or $G_B = G$. We now divide into two cases. If $G_B = G_a$, suppose for the sake of contradiction that there exists $b \neq a$ in B. Since $G \circlearrowright A$ is transitive, there exists $\sigma \in G$ such that $\sigma(a) = b$. It follows since B is a block that $\sigma(B) = B$, hence $\sigma \in G_B = G_a$. But this implies that $\sigma(a) = a$, a contradiction. Therefore, $B = \{a\}$. On the other hand, if $G_B = G$, then let $a \in A$ be arbitrary. By transitivity, there once again exists $\sigma \in G$ such that $\sigma \cdot b = a$ for some $b \in B$. But since $G = G_B$, $\sigma(B) = B$, so $a \in B$. Therefore, $A \subset B$, so $B = A$, as desired. $\square$

8. A transitive permutation group G on a set A is called **doubly transitive** if for any (hence all) $a \in A$, the subgroup G_a is transitive on the set $A \setminus \{a\}$.

(a) Prove that S_n is doubly transitive on $\{1, 2, \dots, n\}$ for all $n \geq 2$.

Proof. Let $\Sigma = \{1, 2, \dots, n\}$. It follows from the definition of S_n that $S_n \circlearrowright \Sigma$ is transitive. Now let $k \in \Sigma$ be arbitrary, and let $G = S_n$ (for ease of writing G_a instead of S_{n_a} or something). Then G_a is the set of all permutations of Σ that fix k, which is naturally transitive on $\Sigma \setminus \{a\}$ for $n \geq 2$. (The $n \geq 2$ condition helps us avoid the case where $\Sigma = \emptyset$.) Therefore, S_n is doubly transitive on Σ, as desired. $\square$

(b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the four vertices of a square.

Proof. Let G a transitive permutation group on A be doubly transitive. To prove that G is primitive, it will suffice to show that the only blocks in A are the trivial ones. Let $B \subset A$ be an arbitrary block. We divide into two cases ($B = A$ and $B \neq A$). If $B = A$, then we are done. If $B \neq A$, then we can pick $c \in A \setminus B$. Additionally, since B (as a block) is nonempty, we may pick an $a \in B$. Now suppose for the sake of contradiction that there exists $b \in B$ such that $b \neq a$. Then since G_a is transitive on $A \setminus \{a\}$, there exists $\sigma \in G_a$ such that $\sigma(b) = c$. This implies that $\sigma(B) \supsetneq B$. However, since $G_a \leq G_B$ by Exercise 7a, $\sigma(B) = B$, a contradiction. Therefore, $B = \{a\}$, as desired.
Since D_8 acting on the four vertices of a square is not primitive by Exercise 7c, we have by the above argument that it cannot be doubly transitive in action on this set either, as desired. $\square$

2. Exercise 4.2.9 of Dummit and Foote (2004).

9. Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

3. Suppose that G acts transitively and faithfully on a finite set X, and that G is abelian. Prove that $|G| = |X|$. Show that the equality need not hold if G is not abelian.

Proof. We approach this proof from the perspective of the Orbit-Stabilizer Theorem. According to it,

$$|G| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$$

for all $x \in X$. Since $G \circlearrowright X$ is transitive, $\mathrm{Orb}(x) = X$, and we can further refine the above to

$$|G| = |X| \cdot |\operatorname{Stab}(x)|$$

Thus, to prove that $|G| = |X|$, it will suffice to show that $|\operatorname{Stab}(x)| = 1$ for all $x \in X$. To do so, we will show that $\operatorname{Stab}(x) = \operatorname{Stab}(y)$ for all $x, y \in X$, from which it will follow that $\operatorname{Stab}(x) = \bigcap_{y \in X} \operatorname{Stab}(y) = \{e\}$ for all $x \in X$, as desired. Let $x, y \in X$ be arbitrary. Since G is transitive, there exists $g \in G$ such that $g \cdot x = y$. Now suppose $h \in \operatorname{Stab}(y)$. Then since G is abelian,

$$\begin{aligned}
g \cdot x &= y \\
&= h \cdot y \\
&= h \cdot (g \cdot x) \\
&= hg \cdot x \\
&= gh \cdot x \\
&= g \cdot (h \cdot x)
\end{aligned}$$

It follows by the cancellation lemma that $h \cdot x = x$, i.e., $h \in \operatorname{Stab}(x)$. Having shown that an arbitrary element of one stabilizer is necessarily in another, we know that all stabilizers are equal, and thus have the desired result.

Let $G = D_6$ and X be the a set of three points in the plane that D_6 can shuffle around. There are elements of D_6 that move every point to every other point, so the action is transitive, and the only element that fixes every point is the identity, so the action is faithful. Additionally, D_6 is not abelian: recall our special rule for commuting in D_6 as $rs = sr^{-1}$. And lastly, note that $|G| = 6 \neq 3 = |X|$, as desired. □

4. Let G be a finite group and let H be any subgroup.

(a) Prove that the left action of G on the coset space G/H has kernel $N = \bigcap_{g \in G} gHg^{-1}$.

Proof. Let $gH \in G/H$ be arbitrary. We seek to show that $\operatorname{Stab}(gH) = gHg^{-1}$. Suppose $\sigma \in \operatorname{Stab}(gH)$ is such that $\sigma \cdot gH = gH$. Then $\sigma gH = gH$, i.e., for every $h \in H$, there exists $h' \in H$ such that $\sigma gh = gh'$. It follows that $\sigma = gh'h^{-1}g^{-1} \in gHg^{-1}$.

Therefore, we have that

$$\ker = \bigcap_{gH \in G/H} \operatorname{Stab}(gH) = \bigcap_{g \in G} \operatorname{Stab}(gH) = \bigcap_{g \in G} gHg^{-1}$$

as desired. □

(b) Prove that $N = \bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup of G contained in H.

Proof. Suppose for the sake of contradiction that there exists $M \lhd G$ such that $M \subset H$ and $M \supsetneq N$. □

5. **The Quaternions.** Let $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ be a 4-dimensional vector space over $\mathbb{R}$. Define a non-commutative associative multiplication structure on $\mathbb{H}$ by the formulae

$$ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j \qquad i^2 = j^2 = k^2 = -1$$

(a) ($\star$) Show that there is a map $\phi : \mathbb{H} \to M_2(\mathbb{C})$, where $M_2(\mathbb{C})$ is the vector space of 2×2 matrices over $\mathbb{C}$, defined by sending

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad k \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

for which

i. ϕ is injective as a map of vector spaces over $\mathbb{R}$.

ii. ϕ respects multiplication; if q_1, q_2 are two quaternions, then $\phi(q_1q_2) = \phi(q_1)\phi(q_2)$. This should reduce easily enough to the case where q_i, q_j are elements of the set $\phi(1), \phi(i), \phi(j), \phi(k)$. The map ϕ is not a group homomorphism since 0 is not an invertible quaternion, but we shall see below in part (c) that non-zero quaternions form a group, so ϕ restricted to $\mathbb{H}^\times$ is actually a homomorphism from $\mathbb{H}^\times$ to $\mathrm{GL}_2(\mathbb{C})$.

(b) Define the conjugate of a quaternion $q = a + bi + cj + dk$ by $\bar{q} := a - bi - cj - dk$. Prove that $N(q) := q\bar{q} = a^2 + b^2 + c^2 + d^2$.

Proof. We have that

$$\begin{aligned}
N(q) &= q\bar{q} \\
&= (a + bi + cj + dk)(a - bi - cj - dk) \\
&= a^2 - abi - acj - adk + abi - b^2i^2 - bcij - bdik + acj - bcji - c^2j^2 - cdjk + adk - bdki - cdkj - d^2k^2 \\
&= a^2 - b^2i^2 - bcij - bdik - bcji - c^2j^2 - cdjk - bdki - cdkj - d^2k^2 \\
&= a^2 - b^2i^2 - bcij - bdik + bcij - c^2j^2 - cdjk + bdik + cdjk - d^2k^2 \\
&= a^2 - b^2i^2 - c^2j^2 - d^2k^2 \\
&= a^2 + b^2 + c^2 + d^2
\end{aligned}$$

as desired. □

(c) Prove that non-zero quaternions $\mathbb{H}^\times$ form a group under multiplication.

Proof. To prove that $(\mathbb{H}^\times, \cdot)$ is a group, it will suffice to show that there exists an identity element e, there exist inverses for every element, and associativity holds. Pick 1 to be the identity element; we clearly have that

$$1 \cdot (a + bi + cj + dk) = (a + bi + cj + dk) \cdot 1 = a + bi + cj + dk$$

where $a + bi + cj + dk \in \mathbb{H}^\times$ is arbitrary. For every $q \in \mathbb{H}^\times$, pick $\bar{q}/N(q)$ to be its inverse; by part (a), we have that

$$q \cdot \frac{\bar{q}}{N(q)} = \frac{N(q)}{N(q)} = 1 = \frac{N(q)}{N(q)} = \frac{\bar{q}}{N(q)} \cdot q$$

Associativity holds by hypothesis. Therefore, $\mathbb{H}^\times$ is a group, as desired. □

(d) Let $Q = \langle i, j \rangle$ be the subgroup of $\mathbb{H}^\times$ generated by i, j. Prove that Q is a group of order 8. (Q is known as the "quaternion group.")

Proof. The elements of Q are

$$Q = \{1 = i^4, -1 = i^2, i, j, -i = i^3, -j = j^3, k = ij, -k = ji\}$$

We can confirm by manual computation that the product of any two of these elements is in Q. The rest of the group axioms are satisfied since any set defined in terms of group generators is a group. □

(e) Prove that every subgroup of Q is normal.

Proof. Let $H \leq Q$, and let $h \in H$. We want to show that $qhq^{-1} \in H$ for all $q \in Q$. We divide into two cases ($q = 1, -1$, and $q \neq 1, -1$). If $q = 1, -1$, then both q, q^{-1} commute with h, so $qhq^{-1} = qq^{-1}h = h \in H$. If $q \neq 1, -1$, then □

(f) Let $N = \pm 1 \subset Q$. Prove that $Q/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ and that Q/N is not isomorphic to a subgroup of Q.

(g) ($\star$) Let Γ be the subgroup of $\mathbb{H}^\times$ generated by the elements of Q together with $\frac{1}{2}(1+i+j+k)$. Prove that Γ is a group of order 24.

(h) Prove that Γ is *not* isomorphic to S_4, and Q is *not* isomorphic to D_8. In fact, $\Gamma = \mathrm{SL}_2(\mathbb{F}_3)$.

(i) ($\star$) Construct a surjective homomorphism from Γ to A_4.

(j) Prove that the subgroup $\mathbb{H}^1$ of quaternions q with $N(q) = 1$ is a subgroup of $\mathbb{H}^\times$. Deduce that the 3-sphere $S^3 \subset \mathbb{R}^4$ defined by $a^2+b^2+c^2+d^2 = 1$ has a natural structure of a group. Note that S^1 also has a natural group structure given by rotations in $\mathrm{SO}(2)$. It turns out that S^n has a natural (i.e., continuous) group structure only for $n = 1$ and $n = 3$.

(k) ($\star$) Say that a quaternion is **pure** if it is of the form $bi+cj+dk$, i.e., $a = 0$. We may identify pure quaternions with $\mathbb{R}^3$. Show that if u is a pure quaternion, then quq^{-1} is still a pure quaternion for any $q \in \mathbb{H}^\times$.

(l) ($\star$) Prove that the action of q on $\mathbb{R}^3$ by $q \cdot u = quq^{-1}$ is via elements of $\mathrm{SO}(3)$, and deduce that there is a homomorphism $\mathbb{H}^\times \to \mathrm{SO}(3)$.

(m) ($\star$) Prove that the restriction of this homomorphism to $\mathbb{H}^1 \to \mathrm{SO}(3)$ is surjective and has kernel of order 2.

7 Broader Classes of Groups

11/28: 1. Suppose that $\mathbb{Z}/m\mathbb{Z}$ is a subgroup of S_n for some $n, m > 2$. Prove that D_{2m} is also a subgroup of S_n.

Proof. m divides $n!$. $n!/m$ is still divisible by 2? $1 \in \mathbb{Z}/m\mathbb{Z}$ functions as r; we just need to prove the existence of an order 2 element in $S_n \setminus \mathbb{Z}/m\mathbb{Z}$.

Take a 2-Sylow of S_n? Characterize that.

Since $n > 2$ and $|S_n| = n!$, $2\big||S_n|$. Thus, by Sylow I, there exists a 2-Sylow $P \in S_n$. Suppose $P = \langle x \rangle$. ☐

2. Let $G = \mathrm{SL}_2(\mathbb{F}_3)$. Prove that the subgroup

$$H = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \right\rangle$$

is isomorphic to the quaternion group Q (where i, j, k map to the given matrices). Deduce that $\mathrm{SL}_2(\mathbb{F}_3)$ and S_4 are not isomorphic.

Proof. Define $\phi : Q \to H$ by

$$i \mapsto \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad k \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

We need not explicitly define matrix images for entries beyond i, j, k since these three elements generate Q. Thus, ϕ is bijective; it only remains to be seen that it is a homomorphism. Fortunately, we can verify the multiplication table as follows (remember that addition everything is mod 2 here in a sense!).

$$\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)}\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)} = -\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)}\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)} = \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)}$$

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)}\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)} = -\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)}\underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)} = \underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)}$$

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)}\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)} = -\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}}_{\phi(i)}\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\phi(k)} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}}_{\phi(j)}$$

$$\underbrace{\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}^2}_{\phi(i)^2} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^2}_{\phi(j)^2} = \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2}_{\phi(k)^2} = -\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\phi(e)}$$

Suppose for the sake of contradiction that $S_4 \cong \mathrm{SL}_2(\mathbb{F}_3)$ with isomorphism $\psi : S_4 \to \mathrm{SL}_2(\mathbb{F}_3)$. $D_8 \leq S_4$ and $H \leq \mathrm{SL}_2(\mathbb{F}_3)$ are both 2-Sylows in their respective groups. Thus, by Sylow II, $\psi(D_8)$ and H are conjugate to each other. But as discussed in class, the $Q \not\approx D_8$, a contradiction. ☐

3. Let G be a group, and let $N \subset G$ be the subgroup generated by the elements $xyx^{-1}y^{-1}$ for all pairs $x, y \in G$. Prove that N is a normal subgroup, and that G/N is abelian.

Proof. To prove that N is normal, it will suffice to show that for all $z \in N$ and $g \in G$, $gzg^{-1} \in N$. Let $x^{-1}y^{-1}xy \in N$ and $g \in G$ be arbitrary. Then

$$\begin{aligned} gx^{-1}y^{-1}xyg^{-1} &= gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} \\ &= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\ &\in N \end{aligned}$$

as desired.

To prove that G/N is abelian, it will suffice to show that $gN * hN = hN * gN$ for all $g, h \in G$. To do so, we can show that $ghN = hgN$, or that $g^{-1}h^{-1}ghN = N$. But since an element of the form $g^{-1}h^{-1}gh \in N$ by definition, we have the desired result. □

4. Compute the order of the following groups as well as a set of generators.

   (a) The centralizer of (12345) in A_7.

   (b) The centralizer of ((12), (123)) in $S_5 \times S_5$.

   Proof. Order: We have that $|\{(12)\}| = 10$ in S_5 and $|\{(123)\}| = 20$ in S_5. Thus, $|\{(12), (123)\}| = 10 \cdot 20 = 200$ in S_5^2. It follows that

$$|S_5^2| = |\{(12), (123)\}| \cdot |C_G(((12), (123)))|$$
$$5!^2 = 200|C_G(((12), (123)))|$$
$$\boxed{|C_G(((12), (123)))| = 72}$$

□

   (c) The normalizer of $H = \langle (12), (34), (56), (78) \rangle$ in S_8.

   Proof. We observe: Image of (12) under conjugation by an element of $N_{S_8}(H)$ must be (12), (34), (56), or (78). Conjugation preserves cycle structure. These are the only 2-cycles in H, so conjugation on H needs to take them to each other. Main point: The set of generators needs to go to the set of generators. Think about what sorts of relabelings will do these kinds of things and which will be possible in the normalizer. □

5. **Projective Linear Groups Over Finite Fields.** Let p be prime, and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Note that one can add and multiply elements of $\mathbb{F}_p$. Let $\mathrm{GL}_2(\mathbb{F}_p)$ be the group of 2×2 invertible matrices over $\mathbb{F}_p$, and let $\mathrm{SL}_2(\mathbb{F}_p) \subset \mathrm{GL}_2(\mathbb{F}_p)$ denote the subgroup of matrices of determinant one.

   (a) There are $p^2 - 1$ non-zero vectors $v \in \mathbb{F}_p^2$. Let a "line" $\ell = [v] \subset \mathbb{F}_p^2$ denote the scalar multiples λv of a non-zero vector v. Prove that the set X of lines has cardinality $|X| = p + 1$.

   Proof. Let $\mathbb{F}_p \circlearrowright \mathbb{F}_p^2$. □

   (b) Prove that $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{GL}_2(\mathbb{F}_p)$ act naturally on X by $g \cdot [v] = [g \cdot v]$.

   Proof. Let $G = \mathrm{GL}_2(\mathbb{F}_p)$. Define $G \circlearrowright X$ by left multiplication. To confirm that this is a group action, it will suffice to show that for all $g, h \in G$ and $[v] \in X$, $g \cdot (h \cdot [v]) = gh \cdot [v]$ and for all $[v] \in X$, $e \cdot [v] = [v]$. With respect to the first statement, we have since g, h are linear that

$$g \cdot (h \cdot [v]) = g \cdot [hv] = [ghv] = gh \cdot [v]$$

   With respect to the latter statement,

$$e \cdot [v] = [ev] = [v]$$

   as desired.

   An analogous argument can treat the $\mathrm{SL}_2(\mathbb{F}_p)$ case. □

   (c) Prove that this action is transitive for both $\mathrm{GL}_2(\mathbb{F}_p)$ and $\mathrm{SL}_2(\mathbb{F}_p)$.

   Proof. Suppose $gu = v$, then $g = vu^{-1}$. □

   (d) Prove that the kernel of the action consists precisely of the scalar matrices λI in either $\mathrm{SL}_2(\mathbb{F}_p)$ or $\mathrm{GL}_2(\mathbb{F}_p)$.

Proof. Let λI be a scalar matrix. Then

$$\lambda I \cdot [v] = [\lambda v] = [v]$$

Similarly, if $g \cdot [v] = [v]$ and $g \cdot [u] = [u]$ for $u \neq v \in \mathbb{F}_p$, then $gv = \lambda v$ for some λ and $gu = \lambda u$ as well, i.e., $g = \lambda I$. $\square$

(e) Let $\mathrm{PGL}_2(\mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$ denote the quotient of G and H by the subgroup of scalar matrices. Prove that $|\mathrm{PGL}_2(\mathbb{F}_p)| = (p^2-1)p$ and $|\mathrm{PSL}_2(\mathbb{F}_p)| = 6$ if $p = 2$ and $\frac{1}{2}(p^2-1)p$ otherwise.

Proof. We know from HW3 Q6 that $|G| = (p^2-1)(p^2-p)$. Additionally, since there are $p-1$ scalar matrices (λI for $\lambda = 1, \dots, p-1$), we have by the corollary from Lecture 3.3 that

$$|\mathrm{PGL}_2(\mathbb{F}_p)| = \frac{|G|}{|\lambda I|} = \frac{(p^2-1)p(p-1)}{p-1} = (p^2-1)p$$

$\square$

(f) Prove that $\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) = S_3$.

(g) Prove that $\mathrm{PGL}_2(\mathbb{F}_3) = S_4$ and $\mathrm{PSL}_2(\mathbb{F}_3) = A_4$. (Compare with Question 2.)

(h) Prove that $\mathrm{PSL}_2(\mathbb{F}_5) = A_5$ and $\mathrm{PGL}_2(\mathbb{F}_5) = S_5$. (Hint: Using that A_6 is simple, prove that any index 6 subgroup of A_6 or S_6 is A_5 or S_5, respectively.)

Proof. Any index 6 subgroup of A_6 or S_6 is A_5 or S_5, respectively. Let $H \subset A_6$ be such that $[A_6 : H] = 6$. Then A_6/H has 6 elements. Let $H \circlearrowright A_6/H$ by left multiplication. This is transitive because we can always sent the identity coset H to any other coset. Recall that any group action on n elements induces a homomorphism from the group to S_n. Thus, we have a homomorphism from A_6 to S_6 (since A_6/H has 6 elements). This is not necessarily the usual injection; it could be very different. Let's call this map $\varphi : A_6 \to S_6$. A priori, φ need not be injective. Injectivity iff $A_6 \circlearrowright A_6/H$ is faithful. But in this case, φ is injective! Since A_6 is simple, $\ker\varphi = A_6$ or $\ker\varphi = \{e\}$. But it's not A_6 (stuff is being moved around??), so it's e. Therefore, $A_6 \circlearrowright A_6/H$ is faithful and φ gives an injection of A_6 in S_6. Restrict attention to $h \subset A_6$. $\varphi|_H : H \to S_6$ is injective. $H \circlearrowright A_6/H$, H fixes the identity coset. Therefore, H permutes the other five (nonidentity) cosets. But this gives an action of H on *five* elements. Indeed, the image $\varphi|_H(H) = S_5$. $\varphi|_H : H \to S_5$ is injective. Recap: H acts on 6 elements, but since every element of H fixes one of the six elements, then its really permuting five elements. The action $H \circlearrowright A_6/H \setminus \{H\}$ is faithful (fixes non-identity cosets implies fixes all cosets). When did we argue that $H \circlearrowright A_6/H$ faithfully? Recall that $A_6 \circlearrowright A_6/H$ faithfully because of simplicity. Now we look at the restriction $H \circlearrowright A_6/H$ to the subgroup $H \leq A_6$. This will also naturally be faithful. Lastly, $H \circlearrowright A_6/H \setminus \{H\}$ is faithful since if $h \in H$ fixes all five nonidentity cosets, then we already know h fixes H (identity coset), so h fixes all six cosets A_6/H since $H \circlearrowright A_6/H$ is faithful. So since $\psi : H \to S_5$ is injective, we have

$$|H| = \frac{|A_6|}{6} = \frac{6!/2}{6} = \frac{360}{6} = 60$$

Then $[S_5 : \psi(H)] = 2$, so $\psi(H) = A_5$ and $H \cong A_5$. What about $S_5 \subset S_6$? Idea: Can do a similar strategy, except "kernel is e or A_6" should be replaced with "kernel is e, A_6, or S_6." What Abhijit means by similar strategy: Suppose $[S_6 : H] = 6$. Then $S_6 \circlearrowright S_6/H$. Use the simplicity of A_6 even in the S_6 case.

Look at the action on the lines faithfully. Something with a group action and counting can help. Prove something is always a normal subgroup. Circumvents the hint. $\square$

8 p-Sylows and Simple Groups

12/2: 1. Show that the 2-Sylow subgroups of S_4 and S_5 are isomorphic to D_8, and the 2-Sylow subgroups of A_4 and A_5 are isomorphic to the Klein 4-group.

Proof. Conjugate subgroups are isomorphic, so we need only find one representative 2-Sylow of S_4, S_5, A_4, A_5 and work with each of them. Let's begin.

For S_4, we have $4! = 24 = 2^3 \cdot 3$, and for S_5, we have $5! = 120 = 2^3 \cdot 15$. Thus, in both cases, we're looking for a subgroup of order 8, and the following will suffice.

$$H = \{e, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (4321)\}$$

Noting that $H = \langle (1234), (13) \rangle$ and $D_8 = \langle r, s \rangle$, where $|(1234)| = |r| = 4$ and $|(13)| = |s| = 2$, we can define our isomorphism $\varphi : H \to D_8$ by

$$(1234) \mapsto r \qquad\qquad (13) \mapsto s$$

Everything else follows homomorphically.

Similarly, for A_4, we have $12 = 2^2 \cdot 3$ and for A_5, we have $60 = 2^2 \cdot 15$. Thus, we're looking for a subgroup of order 4 this time, and the following will suffice.

$$H = \{e, (12)(34), (13)(24), (14)(23)\}$$

Here, we define our isomorphism by

$$e \mapsto e \qquad (12)(34) \mapsto (1, 0) \qquad (13)(24) \mapsto (0, 1) \qquad (14)(23) \mapsto (1, 1)$$

□

2. Let H be the subset of $\mathrm{GL}_3(\mathbb{F}_p)$ of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

(a) Prove that H is a p-Sylow subgroup of $\mathrm{GL}_3(\mathbb{F}_p)$.

Proof. We know from Dummit and Foote (2004, p. 35) that

$$\begin{aligned} |\mathrm{GL}_3(\mathbb{F}_p)| &= (p^3 - 1)(p^3 - p)(p^3 - p^2) \\ &= p^9 - p^8 - p^7 + p^5 + p^4 - p^3 \\ &= p^3 \cdot (p^6 - p^5 - p^4 + p^2 + p - 1) \end{aligned}$$

Additionally, each variable x, y, z in the prototypical element of H can take on all p possible values without affecting the status of that matrix as an element of $\mathrm{GL}_3(\mathbb{F}_p)$. This is because that (upper triangular) matrix's determinant will always be the product of its unchanging diagonal entries. Therefore, $|H| = p^3$. It follows by the definition of p-Sylows that H is a p-Sylow of $\mathrm{GL}_3(\mathbb{F}_p)$, as desired. □

(b) Prove that H is not normal.

Proof. To prove that H is not normal, it will suffice to find $h \in H$ and $g \in G$ such that $ghg^{-1} \notin H$. Indeed, if we take

$$h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad\qquad g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

then

$$\underbrace{\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}}_{g}\underbrace{\begin{pmatrix}1&0&0\\0&1&2\\0&0&1\end{pmatrix}}_{h}\underbrace{\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}}_{g^{-1}}=\begin{pmatrix}1&0&0\\0&1&0\\0&2&1\end{pmatrix}\notin H$$

as desired. □

(c) Determine the number n_p of p-Sylow subgroups of $\mathrm{GL}_3(\mathbb{F}_p)$.

Proof. Prove 2d and then by Sylow III, take

$$n_p = [G : N_G(H)]$$

From

$$N_G(H) = \left\{ \begin{pmatrix}*&*&*\\0&*&*\\0&0&*\end{pmatrix} |\in \mathrm{GL}_3(\mathbb{F}_p) \right\}$$

That $|N_G(H)| = (p-1)^3p^3$, $|G| = |\mathrm{GL}_3(\mathbb{F}_p)|$. Recall that elements of $\mathrm{GL}_3(\mathbb{F}_p)$ lives in three columns. Treat the columns one by one. The number of choices for the first are p^3-1. The number of choices for the second are p multiples of the first column in $\mathbb{F}_p^3$, p^3-p chosen for the second column. There will be p^3-p^2 choices for the third column. Thus, there are $(p^3-1)(p^3-p)(p^3-p^2)$ ways to choose the columns; this is the order of $|\mathrm{GL}_3(\mathbb{F}_p)|$. Implies that the order

$$\begin{aligned}n_p &= [G : N_G(H)]\\ &= \frac{|G|}{|N_G(H)|}\\ &= \frac{(p-1)^3p^3(p^2+p+1)(p+1)}{(p-1)^3p^3}\\ &= (p^2+p+1)(p+1)\end{aligned}$$

This is a very important computation and Abhijit wants to make sure we really understand it! Write something about it in my OH notes.

If we ever learn Rep theory, we'll learn a different proof of this idea. Denote by U the set of upper triangular matrices. Our proposition 1 is that $N_H(G) = U$. Proposition 2 is $N_U(G) = U$. Why does 2 imply 1? It turns out that $H \triangleleft U$. This is rather subtle. We want to show that $N_G(H) = U$, where H is the **Heisenberg group of matrices**. Check $U \subset N_G(H)$. Approach 1: "Do it" with matrix multiplication and cogue that the diagonal of ghg^{-1} is all ones if $g \in U$. Approach 2: Conjugation in matrix groups is a change of basis. Conjugating by BmB^{-1} is a change of basis from $\{e_1, \dots, e_n\} \mapsto \{Be_1, \dots, Be_n\}$. This does not change how the operator/matrix acts on subspaces. Recall that much of linear algebra can be done in a basis-free sense. □

(d) Determine the normalizer of H.

3. Suppose that P is a normal p-Sylow subgroup of G. Suppose that H is a subgroup of G. Prove that $P \cap H$ is the unique p-Sylow subgroup of H. (Exercise 4.5.33 of Dummit and Foote (2004).)

Proof. To prove that $P \cap H$ is the unique p-Sylow of H, we must show that $P \cap H$ is a p-Sylow of H and that $P \cap H \triangleleft H$. Let's begin.

Since P is a normal p-Sylow, Sylow II implies that P is the only p-Sylow in G. Thus, all p-groups in G are subgroups of P. In particular, since $P \cap H \leq P$, $P \cap H$ is a p-group and, moreover, it must be the maximal p-group (or p-Sylow) in H since any larger p-group would by definition necessarily have elements lying outside of H.

To prove that $P \cap H \triangleleft H$, it will suffice to show that $P \cap H \subset H$ and if $h \in H$ and $x \in P \cap H$, $hxh^{-1} \in P \cap H$. The first claim clearly follows from the set theoretic definition of the intersection. For the second claim, we know that $x \in P$ since $x \in P \cap H$. Thus, since P is normal in G and $h \in H \subset G$, $hxh^{-1} \in P$. Additionally, since $x, h \in H$ and H is a subgroup, we know that the product $hxh^{-1} \in H$. But if $hxh^{-1} \in P, H$, then $hxh^{-1} \in P \cap H$, as desired. □

4. Prove that if $n < p^2$, the p-Sylow subgroup of S_n is abelian. Prove that if $n \geq p^2$, the p-Sylow subgroup of S_n is *not* abelian.

   Proof. Groups of order p^2 and groups of order p are abelian, always?? Counterexample: $p = 3$, S_9 has abelian p-Sylow
   $$\langle (1,2,3,4,5,6,7,8,9) \rangle$$
   □

5. Let N be a normal subgroup of G, and suppose that the largest power of p dividing $|N|$ is equal to the largest power of p dividing $|G|$. Prove that the p-Sylow subgroups of G are precisely the p-Sylow subgroups of N.

   Proof. Every p-Sylow of N is a p-Sylow of G. Suppose for the sake of contradiction that there exists a p-Sylow $Q \subset G$ such that $Q \not\subset N$. Let P be a p-Sylow of N (guaranteed to exist by Sylow I). Sylow II: There exists $g \in G$ such that $gPg^{-1} = Q$. In particular, let $q \in Q$ be such that $q \notin N$. Then $q = gpg^{-1}$ for some $p \in P \subset N$. But this implies that not all $p \in N$ satisfy $gpg^{-1} \in N$, a contradiction. □

6. Prove that there do not exist any simple groups of order p^2q for distinct primes p, q. (*Hint*: Consider the congruence restrictions from Sylow III.)

   Proof. Let G be a group of order $|G| = p^2q$ for p, q distinct primes. Suppose for the sake of contradiction that G is simple. We divide into two cases ($p > q$ and $p < q$).

   First, let $p > q$. Sylow III: $n_p \equiv 1 \bmod p$ and $n_p \mid q$. Thus, $n_p \in \{1, q\}$. If $n_p = 1$, we are done. If $n_p = q$, then $n_p \not\equiv 1 \bmod p$, a contradiction.

   Second, let $p < q$. Sylow III: $n_q \equiv 1 \bmod q$ and $n_q \mid p^2$. Thus, $n_q \in \{1, p, p^2\}$. If $n_q = 1$, we are done. If $n_q = p$, then $n_q \not\equiv 1 \bmod q$. If $n_q = p^2$, then the total number of elements of order q is $n_q(q-1) = p^2(q-1) = p^2q - p^2$. Thus, only p^2 elements of G do not have order q. But since by Sylow I there must exist a p-Sylow of order p^2 in G, these remaining elements will be used up by that p-Sylow. Since there are no more element of G, there is only one p-Sylow in G, which is necessarily normal, a contradiction. □

7. Prove that there do not exist any simple groups of the following orders. (Warning: Not in order of difficulty.)

   (a) (*) 336.

   (b) 1176.

   Proof. $1176 = 2^3 \cdot 3 \cdot 7^2$. We have $n_7 \equiv 1 \bmod 7$ and $n_7 | 24$. Thus, $n_7 = 1, 8$. If $n_7 = 1$, we are done. Now suppose $n_7 = 8$. □

   (c) 2907.

   Proof. $2907 = 3^2 \cdot 17 \cdot 19$. □

   (d) 6545.

   Proof. $6545 = 5 \cdot 7 \cdot 11 \cdot 17$. □

9 Final Exam

12/8: **1.** ($40 = 20 + 20$ points) **For this question: no working required**

Compute the orders of the following sets:

1. The centralizer of $(123)(456)(789) \in S_9$.

Proof. Let $g = (123)(456)(789)$, and let $\{g\}$ denote the conjugacy class of g in S_n. We build up to applying the orbit-stabilizer theorem.

Since the conjugacy class of g is the set of all elements with the same cycle shape, and we have a formula for calculating the number of elements in the symmetric group of order n given a certain cycle shape, we apply the formula to learn that

$$|\{g\}| = \frac{n!}{\prod_{i=1}^{k} p_i^{c_i} \cdot c_i!} = \frac{9!}{3^3 \cdot 3!} = 2240$$

Let $S_9 \circlearrowright S_9$ by conjugation. Then $\text{Orb}(g) = \{g\}$ and $\text{Stab}(g) = C_{S_9}(g)$, so we have by the orbit-stabilizer theorem and the above that

$$\begin{aligned} |\text{Orb}(g)| \cdot |\text{Stab}(g)| &= |S_9| \\ |C_{S_9}(g)| &= \frac{9!}{2240} \\ \boxed{|C_{S_9}(g)| = 162} \end{aligned}$$

$\square$

2. The normalizer of $H = \langle (12345) \rangle \subset S_6$.

Proof. Let X be the set of subgroups of S_6 of order 5. Every subgroup in X is generated by a 5-cycle. In particular, there are

$$\binom{6}{5} \cdot (5-1)! = 144$$

5-cycles in S_6. Additionally, each such subgroup contains 4 distinct 5-cycles and e, so

$$|X| = \frac{144}{4} = 36$$

Let $S_6 \circlearrowright X$ by conjugation. Since all 5-cycles are conjugate in S_6, the action is transitive. By the definition of the stabilizer and normalizer, we have that

$$\text{Stab}(H) = \{\sigma \in S_6 \mid \sigma \cdot H = H\} = \{\sigma \in S_6 \mid \sigma H \sigma^{-1} = H\} = N_{S_6}(H)$$

It follows by the orbit-stabilizer theorem that

$$\begin{aligned} |\text{Orb}(H)| \cdot |\text{Stab}(H)| &= |S_6| \\ |N_{S_6}(H)| &= \frac{6!}{36} \\ \boxed{|N_{S_6}(H)| = 20} \end{aligned}$$

$\square$

2. ($40 = 20 + 20$ points) For each of the following groups G, find the smallest n such that G is isomorphic to a subgroup of S_n. Justify your answers.

1. The group $G = S_5 \times \mathbb{Z}/4\mathbb{Z}$.

Proof. We know that

$$C_{S_n}((1,\dots,k)) \cong S_{n-k} \times \mathbb{Z}/k\mathbb{Z}$$

Thus, solving $k = 4$ and $n - k = 5$, we find

$$\boxed{n = 9}$$

□

2. The dihedral group D_{72} of order 72.

   Proof. We know that D_{72} contains an element of order $72/2 = 36$. The order of an element of S_n is equal to the least common multiple of its constituent cycle lengths. Thus, we know that the product of a disjoint 4-cycle and 9-cycle in S_{13} satisfies

   $$|(1,2,3,4)(5,6,7,8,9,10,11,12,13)| = 36$$

   and that S_{13} is the smallest symmetric group to contain such an element. Thus, we can map

   $$r \mapsto (1,2,3,4)(5,6,7,8,9,10,11,12,13)$$

   Additionally, we can geometrically picture separate rotations of a 4-gon and a 9-gon to motivate choosing the following as a reflection element.

   $$s \mapsto (2,4)(6,13)(7,12)(8,11)(9,10)$$

   Together, these elements satisfy the relations

   $$r^{36} = s^2 = e \qquad\qquad rs = sr^{-1}$$

   which characterize D_{72}. Therefore, we take

   $$\boxed{n = 13}$$

   □

3. Let A be a finite abelian group. Suppose that A acts transitively and faithfully on a set X. Prove that $|A| = |X|$.

Proof. We approach this proof from the perspective of the Orbit-Stabilizer Theorem. According to it,

$$|A| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$$

for all $x \in X$. Since $A \circlearrowright X$ is transitive, $\operatorname{Orb}(x) = X$, and we can further refine the above to

$$|A| = |X| \cdot |\operatorname{Stab}(x)|$$

Thus, to prove that $|A| = |X|$, it will suffice to show that $|\operatorname{Stab}(x)| = 1$ for all $x \in X$. To do so, we will show that $\operatorname{Stab}(x) = \operatorname{Stab}(y)$ for all $x, y \in X$, from which it will follow by the faithfulness of the action that

$$\operatorname{Stab}(x) = \bigcap_{y \in X} \operatorname{Stab}(y) = \ker = \{e\}$$

for all $x \in X$, as desired. Let $x, y \in X$ be arbitrary. Since A acts transitively, there exists $g \in A$ such that $g \cdot x = y$. Now suppose $h \in \operatorname{Stab}(y)$. Then since A is abelian,

$$\begin{aligned} g \cdot x &= y \\ &= h \cdot y \\ &= h \cdot (g \cdot x) \\ &= hg \cdot x \\ &= gh \cdot x \\ &= g \cdot (h \cdot x) \end{aligned}$$

It follows by the faithfulness of the action that $h \cdot x = x$, i.e., $h \in \operatorname{Stab}(x)$. Having shown that an arbitrary element of one stabilizer is necessarily in another, we know that all stabilizers are equal, and thus have the desired result. □

4. (45 = 15 + 15 + 15 points) Determine whether the following statements are true or false. Justify your answer in each case.

1. There are finitely many groups up to isomorphism which act faithfully on 5 points.

   Proof. Let X be a set with $|X| = 5$, and let G be a group such that $G \circlearrowright X$ faithfully. This group action induces a homomorphism $\phi : G \to S_5$ which, due to the faithfulness of the action, must have $\ker \phi = \{e\}$. In other words, ϕ is an injection. Therefore, by the first isomorphism theorem, there exists a bijection
$$\tilde{\phi} : G \to \operatorname{im}\phi \leq S_5$$
   i.e., we must have that G is isomorphic to a subgroup of S_5. But since there are only finitely many subgroups of S_5 up to isomorphism, the statement is

$$\boxed{\text{True.}}$$

   $\square$

2. Any finite group is a subgroup of A_n for some integer n.

   Proof. Let G be an arbitrary finite group, and let $|G| = m$. By Cayley's theorem, we know that $G \leq S_m$. Thus, if we can prove that $S_m \leq A_n$ for some n, we are done. Let $n = m+2$, and define $\phi : S_m \to A_n$ by
$$\sigma \mapsto \begin{cases} \sigma & \sigma = \tau_1 \cdots \tau_{2k} \\ \sigma(n+1, n+2) & \sigma = \tau_1 \cdots \tau_{2k+1} \end{cases}$$
   Obviously, ϕ is well-defined and outputs only even permutations. To prove that ϕ is a homomorphism, it will suffice to show that $\phi(\sigma\sigma') = \phi(\sigma)\phi(\sigma')$ for all $\sigma, \sigma' \in S_m$. We divide into four cases (σ, σ' even, σ even & σ' odd, σ odd & σ' even, and σ, σ' odd). For case 1, we have that $\sigma\sigma'$ is even as well, and hence
$$\phi(\sigma\sigma') = \sigma\sigma' = \phi(\sigma)\phi(\sigma')$$
   For case 2, we have that $\sigma\sigma'$ is odd, and hence
$$\phi(\sigma\sigma') = \sigma\sigma'(n+1, n+2) = \phi(\sigma)\phi(\sigma')$$
   For case 3, we have that $\sigma\sigma'$ is odd, and hence
$$\phi(\sigma\sigma') = \sigma\sigma'(n+1, n+2) = \sigma(n+1, n+2)\sigma' = \phi(\sigma)\phi(\sigma')$$
   where we have used the fact that disjoint cycles commute in the next to last step (this is why it's important to go up by +2). Lastly, for case 4, we have that $\sigma\sigma'$ is even, and hence
$$\phi(\sigma\sigma') = \sigma\sigma' = \sigma\sigma'(n+1, n+2)^2 = \sigma(n+1, n+2)\sigma'(n+1, n+2) = \phi(\sigma)\phi(\sigma')$$
   Therefore, ϕ is a homomorphism.
   We can also see that ϕ is injective since distinct σ, σ' will map to distinct outputs σ, σ' (and the presence or absence of an appended disjoint cycle will not change the distinctness of the original permutations). Thus, $S_m \leq A_{m+2}$, as desired.
   Therefore, $G \leq A_{|G|+2}$, and we have proven that the statement is

$$\boxed{\text{True.}}$$

   $\square$

3. A group of order $2688 = 2^7 \cdot 3 \cdot 7$ has a transitive action on a set X with $|X| = 21$.

Proof. Leg G be a group of order $|G| = 2688$. By Sylow I, G has a 2-Sylow subgroup P. By Lagrange's theorem,

$$|G/P| = |G|/|P| = 21$$

We know that $G \circlearrowright G/P$ transitively for P a subgroup, so take $X = G/P$. Therefore, we have proven that the statement is

$$\boxed{\text{True.}}$$

□

5. (30 points) Let G be a simple group of order 168. Determine the number of elements of G of order 7.

Proof. Since 7 is a prime number (and one that only appears once in the prime factorization of 168), we know that the number of elements in G of order 7 will be equal to the number n_7 of 7-Sylows. By Sylow III, we know that $n_7 \equiv 1 \bmod 7$. Additionally, we have by Lagrange's theorem that $n_7 \mid 168$; in particular, since $168 = 24 \cdot 7$ and $n_7 \not\equiv 0 \bmod 7$, we know that $n_7 \nmid 7$ so it must be that $n_7 \mid 24$.

The only two natural numbers that are both congruent to 1 mod 7 and divide 24 are $n_7 \in \{1, 8\}$. But if $n_7 = 1$, then by Sylow II, the sole 7-Sylow is normal in G, contradicting its simplicity. Therefore, we must have that

$$\boxed{n_7 = 8}$$

□

6. (20 = 10 + 10 points) Let $n > 1$ be an integer and let G be a group of order n. The left action of G on itself induces an injective map $\psi : G \to S_n$.

1. Prove that if $g \in G$ has order 2, then n is even and the cycle decomposition of $\psi(g)$ consists of $n/2$ disjoint 2-cycles.

   Proof. Since g has order 2, Lagrange's theorem implies that $2 \mid |G|$, so n must be an even number, as desired.

   Let $G \circlearrowright G$ be the described left action. Let $h \in G$ be arbitrary. Since $|g| = 2$ and hence $g \neq e$, we have by the Sudoku lemma that $gh \neq h$. It follows by the group action axioms that

   $$g \cdot h = gh \qquad\qquad g \cdot gh = h$$

   Thus, to every $h \in G$, there corresponds a unique matching element gh. By the faithfulness of the group action, there is no overlap between the pairs h, gh and hence G can be partitioned into pairs of elements h, gh. Moreover, we have by the above that for any $h \in G$,

   $$\psi(g)(h) = g \cdot h = gh \qquad\qquad \psi(g)(gh) = g \cdot gh = h$$

   so every pair h, gh presents as a 2-cycle in the cycle decomposition of $\psi(g) \in S_G \cong S_n$, as desired. □

2. Prove that if $n \equiv 2 \bmod 4$ and $n > 2$, then G is not a simple group.

   Proof. Suppose for the sake of contradiction that G is a group of order n. An equivalent formulation to $n \equiv 2 \bmod 4$ is stating that $n = 2m$ where m is an odd number greater than or equal to 3. Since $|G| = 2 \cdot m$ where $m \nmid 2$, Sylow I implies that G contains a 2-Sylow of order 2. In particular, there exists $g \in G$ of order 2 (take the nontrivial element of the 2-Sylow).

   Applying part (1), we learn that $\psi(g) \in S_n$ consists of $n/2 = m$ (an odd number) of 2-cycles. Thus, $\psi(g) \notin A_n$.

   However, as a simple group with a transitive action on a set of $n \geq 2$ points, Lemma 11 asserts that either $G \hookrightarrow A_n$ or $|G| = 2$. By the above, we know that $G \not\hookrightarrow A_n$, but by hypothesis, $n \neq 2$ either, a contradiction. □

7. Let G be a subgroup of A_8 which is simple of order 504. Prove that the action of G is 2-transitive, that is, for any pairs $\{a, b\}$ and $\{c, d\}$ of two distinct elements of $\{1, 2, 3, \ldots, 8\}$, there is an element g such that

$$g(a) = c \qquad\qquad g(b) = d$$

Proof. $504 = 2^3 \cdot 3^2 \cdot 7$. $\square$

References

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