1. Let $n > 0$. Find a formula for $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n$.

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}
\]

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}
\]

\[
\vdots
\]

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{n(n+1)}{2} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{n(n+1)}{2} \\ 0 & 1 \end{bmatrix}
\]

**Answer**

\[
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & \frac{n(n+1)}{2} \\ 0 & 1 \end{bmatrix}
\]
2.a. \[ RS = p \left[ \begin{array}{c} \vdots \end{array} \right] \cdot \left[ \begin{array}{c} \vdots \end{array} \right] q = p \left[ \begin{array}{c} \vdots \end{array} \right] \] each entry in \( RS \) is found by adding \( q \) numbers together, each being a multiplication of two numbers.

Therefore, \( RS \) requires \( pqr \) multiplications.

2.b. By 2.a. \( RS \) requires \( pqr \) multiplications, and then \( (RS)^T \)

requires \( prs \) multiplications.

Therefore \( (RS)^T \) requires \( pqr + prs \) multiplications.

2.c. By 2.a. \( ST \) requires \( qrs \) multiplications, and then \( R(ST) \)

requires \( qrs \) multiplications.

Therefore \( R(ST) \) requires \( qrs + qrs \) multiplications.

2.d. \( (RS)^T \) requires \( pqr + prs = (23)(14)(11) + (23)(11)(21) \)

\[ = 10120 \text{ multiplications.} \]

\( R(ST) \) requires \( qrs + qrs = (19)(11)(23) + (23)(19)(21) \)

\[ = 102,566 \text{ multiplications.} \]

\( (RS)^T \) requires fewer.
\[ A'' = \begin{bmatrix} -2 & 3 & 9 \\ -1 & -10 & 2 \\ -5 & 7 & 21 \end{bmatrix} \]

3.b. Using \( A'' \) from 3.a, we have:
\[ \lambda = -2x' + 8y' - 5z' \]
\[ \gamma = 3x' - 11y' + 7z' \]
\[ z = 9x' - 34y' + 21z' \]

4. \( A \sim \begin{bmatrix} 1 & -1 \\ 3 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \)

\[ E_{R_1 + R_2} E_{R_3 - R_2} E_{R_3 + R_2} A = I \]

\[ A'' = E_{R_1 + R_2} E_{R_3 - R_2} E_{R_3 + R_2} \]

\[ A = (E_{R_1 + R_2})^{-1} (E_{R_3 - R_2})^{-1} (E_{R_3 + R_2})^{-1} \]

\[ A = E_{R_1 + R_2} E_{R_3 - R_2} E_{R_3 + R_2} \]

\[ A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} \]

(There are many answers depending on the operation that you use.)
5. Let $C$ be the matrix $B^tA^t$.

Notice that $C(AB) = B^tA^tAB = B^t(A^tA)B = B^tIB = B^tB = I$.

Therefore $B^tA^t$ is the inverse matrix of $AB$.

\[ \therefore (AB)^{-1} = B^tA^t. \]

6. Let $C$ be the matrix $(A^t)^t$.

Notice that $C = A^t(A^t)^tA^t = (AA^t)^t = I^t = I$.

\[ \text{using the property} \quad (AB)^t = B^tA^t \]

\[ \text{the identity matrix is self-transpose.} \]

Therefore $(A^t)^t$ is the inverse matrix of $A^t$.

\[ \therefore (A^t)^{-1} = (A^t)^t. \]

In question 3a, we have $\begin{bmatrix} 3 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{bmatrix}^{-1} = \begin{bmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -14 & 1 \end{bmatrix}$.

By our work in question 6, we have $\begin{bmatrix} 7 & 0 & -3 \\ 2 & 3 & 4 \\ 1 & -1 & 2 \end{bmatrix}^t = \begin{bmatrix} -2 & 3 & 9 \\ 8 & -1 & -34 \end{bmatrix}$.
7. 

\[ A^t A = I \]

\[ \rightarrow \text{taking the determinant of this equation yields} \]

\[ \det(A^t A) = 1 \]

\[ \det(A^t) \det(A) = 1 \quad \text{(using the property } \det(AB) = \det(A) \det(B)) \]

\[ \det(A^t) = k = 1 \]

\[ \det(A^t) = \frac{1}{k} \]

8. \( \Rightarrow \) Show that \( \det(A) = \det(B) \Rightarrow \text{implies that } \det(AB^t) = 1 \)

\[ \text{Suppose that } \det(A) = \det(B). \]

\[ \text{Then we have, } \det(A) \cdot \frac{1}{\det(B)} = 1 \]

Then by question 7, \( \det(A) \det(B^t) = 1 \)

Then using the property \( \det(CD) = \det(C) \det(D) \)

we have: \( \det(AB^t) = 1. \)

\( \Leftarrow \) \( \Rightarrow \) Show that \( \det(AB^t) = 1 \) implies that \( \det(A) = \det(B) \)

\[ \text{Suppose that } \det(AB^t) = 1. \]

\[ \text{Then we have } \det(A) \det(B^t) = 1. \]

By question 7, \( \det(A) \cdot \frac{1}{\det(B)} = 1 \)

Therefore \( \det(A) = \det(B). \)
1. The outcome is the same in either order.

\[ A \xrightarrow{\text{row op}} EA \xrightarrow{\text{col. op}} (EA)F \xrightarrow{\text{row op}} E(AF) \]

Thus are equal!

2.a. If \( E = E_{R_i \leftrightarrow R_j} \) then \( E^t = E \), and \( \det(E^t) = \det(E) = -1 \)

If \( E = E_{aR_i} \) then \( E^t = E \), and \( \det(E^t) = \det(E) = a \)

If \( E = E_{R_i + bR_j} \) then \( E^t = E_{R_j + bR_i} \), and \( \det(E^t) = \det(E) = 1 \).

2.b. If \( A \) is not invertible, then neither is \( A^t \), and therefore:

\[ \det(A) = \det(A^t) = 0 \]

If \( A \) is invertible, it is a product of elementary matrices: \( A = E_k E_{k-1} \cdots E_2 E_1 \).

\[ \det(A^t) = \det(E_1^t E_2^t \cdots E_k^t) = \det(E_1^t) \cdots \det(E_k^t) = \det(E_1) \cdots \det(E_k) \]

\[ = \det(A). \]

\( (\det(E^t) = \det(E)) \) for each \( E \).
3.a. $(1\ 6\ 5\ 4\ 3\ 2)$ cycle type: $(6)$.

3.b. $(1\ 2)(3)(4\ 5) = (1\ 2)(4\ 5)$ cycle type: $(2,2,1)$

3.c. $(1\ 4\ 2)(3) = (1\ 4\ 2)$ cycle type: $(3,1)$

4.a. $(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$ or $(2\ 1)(2\ 6)(2\ 5)(2\ 4)(2\ 3)$ or...

4.b. $(3\ 5)(3\ 4)(1\ 6)(1\ 2)$

5.a. 

5.b. 

$(1\ 3\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(1\ 2)$

$(1\ 4)(2\ 5) = (2\ 3)(3\ 4)(4\ 5)(2\ 3)(1\ 2)(2\ 3)(3\ 4)(2\ 3)$
6.a. \[ A_p = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \sigma(p) = (-1)^3 = 1 \]

6.b. \[ A_p = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \sigma(p) = (-1) \cdot (-1) \cdot (-1) = (-1)^3 = -1 \]

\[ (1 2 4 3) = (1 3)(1 4)(1 2) \]

7. Write \( p \in S_n \) as a product of transpositions: \( p = t_{k_1} \cdots t_{k_i} \).

Then \( A_p = A_{t_{k_1}} \cdots A_{t_{k_i}} \).

\[ A_p^t = A_{t_{k_i}}^t \cdots A_{t_{k_1}}^t \quad A_p^t = A_{t_{k_i}}^t \cdots A_{t_{k_1}}^t \]

\( A_p^t = A_{t_{k_i}}^t \cdots A_{t_{k_1}}^t \) (since the \( A_{t_i} \) are row-swap elements, their transposes are themselves.)

\[ (A_p)^{-1} = A_{t_{k_i}}^{-1} \cdots A_{t_{k_1}}^{-1} \]

\( (A_p)^{-1} = A_{t_{k_i}}^{-1} \cdots A_{t_{k_1}}^{-1} \) (since \( A_{t_i}^{-1} = A_{t_i} \) because they are row-swap elements.)

From this we see that \( (A_p)^t = (A_p)^{-1} \).
ma 312
ps 3 solutions

1.a. (in pencil)

<table>
<thead>
<tr>
<th></th>
<th>$\cdot$</th>
<th>$x$</th>
<th>$x^2$</th>
<th>$y$</th>
<th>$xy$</th>
<th>$x^2y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>(1 3)</td>
<td>(3 1)</td>
<td>(1 2)</td>
<td>(3 2)</td>
<td>(2 3)</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>(1 2 3)</td>
<td>(3 2 1)</td>
<td>(1 2)</td>
<td>(1 3)</td>
<td>(2 3)</td>
</tr>
</tbody>
</table>

1.b. (in red pen)

<table>
<thead>
<tr>
<th></th>
<th>$\cdot$</th>
<th>$x$</th>
<th>$x^2$</th>
<th>$y$</th>
<th>$xy$</th>
<th>$x^2y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1 3)</td>
<td>(1 2 3)</td>
<td>(3 2 1)</td>
<td>1</td>
<td>(1 2)</td>
<td>(1 3)</td>
</tr>
<tr>
<td>2</td>
<td>$x$</td>
<td>$x^2$</td>
<td>$y$</td>
<td>$xy$</td>
<td>$x^2y$</td>
<td>$y$</td>
</tr>
<tr>
<td>3</td>
<td>(3 2 1)</td>
<td>(3 2 1)</td>
<td>1</td>
<td>(1 2 3)</td>
<td>(2 3)</td>
<td>(1 2)</td>
</tr>
</tbody>
</table>

Sample calculation:

$xy(x^2y) = x(xy)x(y) = x(x^2y)y$

$= x^3(yx)y$

$= (1)(x^2y)y$

$= x^2y^2$

$= x^2(1)$

$= x^2$
1. c. Possible answers include:

\[ S_3 = \langle a, b \mid a^2 = 1, b^2 = 1, (ab)^3 = 1 \rangle \]

\[ S_3 = \langle a, b \mid a^2 = 1, b^2 = 1, ababa = 1 \rangle \]

\[ S_3 = \langle a, b \mid a^2 = 1, b^2 = 1, aba = bba \rangle \]

1. d. \( S_3 = \left\{ 1, ab, ba, a, aba, b \right\} \) (list of elements relative to \( a, b \) presentation)

\[
\begin{array}{cccccc}
\hline
 & i & ab & ba & a & aba & b \\
\hline
1 & 1 & ab & ba & a & aba & b \\
ab & ab & ba & 1 & aba & b & a \\
ba & ba & 1 & ab & b & a & aba \\
a & a & b & aba & 1 & ba & ab \\
aba & aba & a & \boxed{b} & ab & 1 & ba \\
b & b & aba & a & ba & ab & 1 \\
\hline
\end{array}
\]

Sample calculation: \( aba(ba) = ab(aba) = ab(bab) = a b^2 a b = a^3 b = b \).
2.a. Think about the composition $e \cdot e'$ in two ways.

on one hand, $e \cdot e' = e'$.

on the other hand, $e \cdot e' = e$.

Therefore $e = e'$.

2.b. $a = a \cdot e = a(geb) = (ag)b = e \cdot b = b$.

Thus shown that $a = b$.

3.a. $H \subseteq G$ is a subgroup.

* $1 \in H$ since $1 = 1^2$ and $1 \in \mathbb{Q}^x$.
* $x, y \in H \Rightarrow xy \in H$, since if $x = r^2$ and $y = s^2$, then $xy = (rs)^2$.
* $x \in H \Rightarrow x^{-1} \in H$, since if $x = r^2$ then $x^{-1} = \frac{1}{x} = \left(\frac{1}{r}\right)^2$.

3.b. $H \subseteq G$ is not a subgroup.

One way to see this is to look at the counterexample:

$\begin{align*}
(123) & \cdot (234) = (12)(34) \\
\text{E} H \text{ since cycle type} & \text{ E} H \text{ since cycle type} \quad \& H \text{ since cycle type} \\
(3,1,1) & \quad (3,1,1) \quad (3,2,1)
\end{align*}$
3. c. \( H \leq G \) is a subgroup.

\[
\begin{bmatrix}
0 & 1 \\
-1 & 0
\end{bmatrix}
\in \text{GL}_2(\mathbb{Z}), \text{ since } I \text{ has integer entries and } \det(I) = 1.
\]

\[
A, B \in \text{GL}_n(\mathbb{Z}) \implies AB \in \text{GL}_n(\mathbb{Z}), \text{ since if } A, B \text{ have integer entries and } \det \text{ of } \pm 1, \text{ then } AB \text{ has integer entries and } \det(AB) = \det(A) \det(B) = (\pm 1)(\pm 1) = \pm 1.
\]

\[
A \in \text{GL}_n(\mathbb{Z}) \implies A^{-1} \in \text{GL}_n(\mathbb{Z}), \text{ since if } A \text{ has integer entries and } \det \text{ of } \pm 1, \text{ then } \det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{(\pm 1)} = \pm 1.
\]

To justify that \( A^{-1} \) would have integer entries one could appeal to the adjoint formula for the inverse matrix.

4. a. \[\begin{align*}
765 &= 567 + 198 \\
567 &= (2)(198) + 171 \\
198 &= 171 + 27 \\
171 &= (6)(27) + 9 \\
27 &= (3)(9) + 0
\end{align*}\]

\[\gcd(765, 567) = 9\]
4.6. Since \( \gcd(567, 765) = 9 \), the hour hand can reach 9:00, and that is the smallest hour value it can reach. Overall, therefore, it can reach all hours that are multiples of 9; \((0:00, 9:00, 18:00, 27:00, 36:00, \ldots, 75:00)\).

Multiplying our solution to \( 765x + 567y = 9 \) by 3 we obtain:

\[
765(-60) + 567(81) = 27
\]

In other words,

\[
567(81) = 27 + 765(60)
\]
4. \, want \ minimal \, n \, such \, that \, \((a^{567})^n = 1 = (a^{765})^k\)

\[567 \, n = 765 \, k\]

(divide out by \(\gcd(567, 765) = 9\))

\[63 \, n = 85 \, k\]

since 63 and 85 have no common factors, we see that \(n = 85\)

is the minimal solution.

Therefore \(\text{ord} \, (a^{567}) = 85\).

5. \(\text{ord} \, (p) = \text{lcm} \, (l_1, \ldots, l_k)\) if \(p\) has cycle type \((l_1, \ldots, l_k)\).

Therefore the elements of \(S_6\) having order 6 must have cycle type:

\[
\begin{array}{ccc}
\times & (6) & \text{How Many?} \\
& (a \, b \, c \, d \, e \, f) & \\
& \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{6} & = 120 \\
\end{array}
\]

120 elements of cycle type (6).

we divided by six because of equality of cyclic rotations:

\[
(1 \, 2 \, 3 \, 4 \, 5 \, 6) = (2 \, 3 \, 4 \, 5 \, 6 \, 1) = (3 \, 4 \, 5 \, 6 \, 1 \, 2) = (4 \, 5 \, 6 \, 1 \, 2 \, 3) = (5 \, 6 \, 1 \, 2 \, 3 \, 4) = (6 \, 1 \, 2 \, 3 \, 4 \, 5)
\]

\[
\begin{array}{ccc}
\times & (3,2) & \text{How Many?} \\
& (a \, b \, c)(d \, e)(f) & \\
& \frac{(6 \cdot 5 \cdot 4)(3 \cdot 2)}{3} \cdot \frac{1}{2} & = 40 \cdot 3 = 120 \\
\end{array}
\]

120 elements of cycle type (3,2).

240 total elements of order 6 in \(S_6\).
Bonus.

\[ A_{\Phi} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \]

\[ \sigma(\Phi) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases} \]

Cycle type of \( \Phi \): \((2, 2, \ldots, 2)\) if \( n \) is even,
\[ \frac{n}{2} \]
\((2, 2, \ldots, 2, 1)\) if \( n \) is odd,
\[ \frac{n-1}{2} \]

Bonus.

\[
\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \sim \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}
\]

Therefore

\[
\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.
\]

Using the logic of the 2x2 example above we have:

\[
E_{R_i \leftrightarrow R_j} = E_{-R_i} E_{R_j + R_i} E_{R_i - R_j} E_{R_j + R_i}
\]
The two expressions \( \Phi \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \) and \( \Phi \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Phi \begin{bmatrix} e & f \\ g & h \end{bmatrix} \) are equal.

Therefore \( \Phi : \text{GL}_2(\mathbb{Q}) \to G \) is a homomorphism.
1.b. \( v(v(x)) = v\left(\frac{1}{x}\right) = \frac{1}{\left(\frac{1}{x}\right)} = x \). Therefore \( v^2 = I \) (where \( I(x) = x \) is the identity function).

\[ \therefore \text{ord}(v) = 2. \]

\[ u(u(x)) = u\left(\frac{x-1}{x}\right) = \frac{\left(\frac{x-1}{x}\right) - 1}{\left(\frac{x-1}{x}\right)} = \frac{\frac{x-1 - x}{x}}{\left(\frac{x-1}{x}\right)} = \frac{-1}{x} \cdot \frac{x}{x-1} = \frac{-1}{x-1}. \]

\[ u(u(u(x))) = u\left(\frac{-1}{x-1}\right) = \frac{\left(-\frac{1}{x-1}\right) - 1}{\left(-\frac{1}{x-1}\right)} = \frac{-1 - (x-1)}{x-1} \cdot \frac{x-1}{-1} = -\frac{x}{-1} = x. \]

Therefore \( u^3 = I \).

\[ \text{ord}(u) = 3. \]

1.c. we need to show that \( uv = u^2 v \).

\[ v(u(x)) = v\left(\frac{x-1}{x}\right) = \frac{1}{\left(\frac{x-1}{x}\right)} = \frac{x}{x-1}. \]

\[ u(u(v(x))) = u\left(u\left(\frac{1}{x}\right)\right) = u\left(\frac{\left(\frac{1}{x}\right)-1}{\left(\frac{1}{x}\right)}\right) = u\left(1 - x\right) = \frac{(1-x)-1}{1-x} = \frac{-x}{1-x} = \frac{x}{x-1}. \]

Therefore \( uv = u^2 v \).

Therefore \( H \cong \langle u, v \mid u^3 = 1, v^2 = 1, uv = u^2 v \rangle \cong S_3. \)
2.a. Let $a^i, a^j$ be two elements in $C_{10}$.

Then $f(a^i \cdot a^j) = (a^{i+j})^6 = a^{6i+6j} = a^i \cdot a^j = (a^i)^6 (a^j)^6$

$= f(a^i)f(a^j)$.

Thus $f$ is a homomorphism.

$\ker(f) = \{ 1, a^5 \}$

$\text{im}(f) = \{ 1, a, a^2, a^3, a^4, a^8 \}$

2.b. $g$ is a homomorphism by reasoning in 2a.

since $3 \cdot 7 = 1 \cdot 2 \cdot 10$ we have that $X \to X^3$

is the inverse function.

$$X \xrightarrow{g} X^7 \xrightarrow{(. )^3} X^{21} = X$$

$g$ is an invertible homomorphism $\iff g$ is an isomorphism.

2.c. Let $X, Y$ be elements of $C_n$.

$$(X \cdot Y)^k = X^k \cdot Y^k$$ shows that the function is a homomorphism.

If $\gcd(k,n) \neq 1$, this function cannot be an isomorphism since it cannot be one-to-one. Suppose $d = \gcd(k,n) \neq 1$.

$$a \xrightarrow{k} a^d \xrightarrow{1} a^d \xrightarrow{a^d} 1$$

$$\text{gcd}(12,18) = 3$$
Now suppose that $\gcd(k,n) = 1$.

By the Euclidean Algorithm, $kX + nY = 1$ has a solution for $X, Y \in \mathbb{Z}$.

Let $(X_0, Y_0)$ be a particular integer solution.

Then $kX_0 = 1 + n(-Y_0)$ shows that the function $X \rightarrow kX_0$

is an inverse of the function $X \rightarrow X^k$:

$$X \rightarrow X^k \rightarrow X^k = X^{1+n(-Y_0)} = X$$

Therefore $X \rightarrow X^k$ is an isomorphism $C_n \rightarrow C_n$ exactly when $\gcd(k,n) = 1$.

2.d. $23, 5, 3, 2, 1, 0$

$23 = 4(5) + 3$
$5 = 3 + 2$ $\iff 3 - 2 = 1$
$3 = 2 + 1$
$2 = 2(1) + 0$

$2(3) - 5 = 1$
$2(23 - 4(5)) - 5 = 1$
$2(23) - 9(5) = 1$
$(-9)(5) = 1 + 23(-2)$

$$X \rightarrow X^5 \rightarrow X^{-45} = X^{1+23(-2)} = X \cdot (X^{23})^{-2} = X$$

The inverse function is $X \rightarrow X^{-9}$ or equivalently, $X \rightarrow X^{14}$.
(a b)(b c) = (a b c)

(a b)(c d) = (a b c)(b c d)

Let \( p \in A_n \). Then \( p = \tau_{2k} \tau_{2k-1} \cdots \tau_3 \tau_2 \tau_1 \) is a product of an even number of transpositions. The permutation is therefore a product of a number of pairs of transpositions \( p = (\tau_{2k} \tau_{2k-1}) \cdots (\tau_2 \tau_1) \).

We know that each pair is either a single 3-cycle or a product of two 3-cycles. Therefore \( p \) is a product of 3-cycles.

Therefore \( A_n = \langle 3\text{-cycles} \rangle \).

\[(1 2 3 4 5) = (1 5)(1 4)(1 3)(1 2) = (5 1)(1 4)(3 1)(1 2) = (5 1 4)(3 1 2).\]
Claim. \( \text{Ker}(\phi) = \{1\} \subseteq S_4 \). (The kernel has the identity of \( S_4 \) only.)

Proof. Let \( p \in \text{Ker}(\phi) \). Consider \( \phi(p) \) mapping \( \{1, 2\} \rightarrow \{1, 2\} \) and \( \{1, 3\} \rightarrow \{1, 3\} \).

(This is because \( \phi(p) \) is the identity permutation of \( S_6 \).)

\( \{1, 2\} \rightarrow \{1, 2\} \) implies that \( p(1) = 1 \) or \( p(1) = 2 \). But \( p(1) = 2 \) would contradict the fact that \( \{1, 3\} \rightarrow \{1, 3\} \). Therefore \( p(1) = 1 \). Similar reasoning shows that \( p(i) = i \) for all \( i = 1, 2, 3, 4 \). \( \square \)

Claim. \( \text{Im}(\phi) \subseteq A_6 \).

Proof. Since \( S_4 \) is generated by simple transpositions, it is enough to show that \( \phi(1 2) \), \( \phi(2 3) \), and \( \phi(3 4) \) are elements of \( S_6 \).

(Why? Let \( p \in S_4 \). Write \( p = t_{k_1} t_{k_2} \ldots t_{k_l} \) as a product of simple transpositions.)

Then \( \phi(p) = \phi(t_{k_1}) \cdot \phi(t_{k_2}) \cdot \ldots \cdot \phi(t_{k_l}) \in A_6 \).

\[
\phi(1 2) = (2 4)(3 5) \in A_6
\]

\[
\phi(2 3) = (1 2)(5 6) \in A_6
\]

\[
\phi(3 4) = (2 3)(4 5) \in A_6
\]
Let \( x = (1 \, 2 \, 3 \, 4) \) and \( y = (1 \, 3) \). Then \( x^4 = 1 \), \( y^2 = 1 \), and \( yx = x^3y \).

Therefore, \( G \cong \langle x, y \mid x^4 = 1, y^2 = 1, yx = x^3y \rangle \).
2. Label the four pairs of opposite vertices of the cube. We obtain a homomorphism:

\[ G_c \xrightarrow{\phi} S_4 \]

(Identity)

- \( 90^\circ \) rotation:
  \[ (a b c d) \] all cycle type (4) obtained this way.

- \( 180^\circ \) rotation:
  \[ (a b)(c d) \] all cycle type (2,2) obtained this way.

- \( 120^\circ \) rotation:
  \[ (a b c)(d) \] all cycle type (3,1) obtained this way.

- \( 180^\circ \) rotation:
  \[ (a b)(c)(d) \] all cycle type (2,1,1) obtained this way.

\( \phi \) is a one-to-one and onto homomorphism, thus an isomorphism.

\[ G_c \cong S_4. \]
Label the four pairs of opposite faces

We obtain a homomorphism:

\[ G_0 \xrightarrow{\phi} S_4 \]

(Identity)

\[ \rightarrow (1)(2)(3)(4) \]

\[ \rightarrow (a b c d) \quad \text{all cycle type (4) are obtained this way.} \]

\[ \rightarrow (a b)(c d) \quad \text{all cycle type (2,2) are obtained this way.} \]

\[ \rightarrow (a b c)(d) \quad \text{all cycle type (3,1) are obtained this way.} \]

\[ \rightarrow (ab)(c)(d) \quad \text{all cycle type (2,1,1) are obtained this way.} \]

\( \phi \) is a one-to-one and onto homomorphism, thus an isomorphism.

\[ G_0 \cong S_4 \]
4.a. $X = \{ \text{colorings of } \Box \text{ relative to an ordering of the faces} \}$

$G_o \subseteq X$
$G_o = \{ \text{rotational symmetries of the cube} \} \approx S_4$

$$|X/S_4| = \frac{1}{|S_4|} \left( |X^{(1,1,1)}| + 6|X^{(3,1,1)}| + 8|X^{(3,3,1)}| + 3|X^{(3,3,3)}| + 6|X^{(4,1)}| \right)$$

$$= \frac{1}{24} \left( 3^6 + 6 \cdot 3^3 + 8 \cdot 3^3 + 3 \cdot 3^4 + 6 \cdot 3^4 \right)$$

$$= 3^4 \left( 3^2 + 6 \cdot 3 + 8 + 3^2 + 6 \cdot 3 \right)$$

$$= 3^2 \left( 27 + 44 \right)$$

$$= 3 \left( \frac{71}{2} \right)$$

$$= 3 \left( 36 \frac{1}{2} \right)$$

$$= 3 \left( 19 \right)$$

$$= 57 \text{ ways!}$$

4.b. $X = \{ \text{labellings of } \Box \text{ with } \{1, 2, \ldots , 8\} \}$

$G_o \subseteq X$
$G_o = \{ \text{rotational symmetries of the octahedron} \} \approx S_4$

$$|X/S_4| = \frac{1}{|S_4|} \left( |X^{(1,1,1)}| + 6(0) + 8(0) + 3(0) + 6(0) \right)$$

$$= \frac{|X|}{|S_4|}$$

$$= 8 \cdot 7 \cdot 6 \cdot 5$$

$$= 1680 \text{ distinct octahedral dice.}$$
4.c. Let $X = \{ \text{colorings of } \circ \text{ with } R, O, Y, G, B, V \text{ relative to that ordering} \}$

$G \subset X$

$G = \{ \text{symmetries of the hexagon} \}$

$G \cong \{ 1, (1\ 2\ 3\ 4\ 5\ 6), (6\ 5\ 4\ 3\ 2\ 1), (1\ 3\ 5)(2\ 4\ 6), (5\ 3\ 1)(6\ 4\ 2), \}

$0^\circ \quad 60^\circ \quad -60^\circ \quad 120^\circ \quad -120^\circ$

$(1\ 4)(2\ 5)(3\ 6), \quad (2\ 6)(3\ 5), \quad (1\ 2)(3\ 6)(4\ 5), \quad (1\ 3)(4\ 6), \quad (1\ 4)(2\ 3)(5\ 6), \quad (1\ 5)(2\ 4), \quad (1\ 6)(2\ 5)(3\ 4) \}$

$\ast (G \text{ is isomorphic to a twelve element subgroup of } S_6.)$

$|X/G| = \frac{1}{12} \left( |X^{(1,1,1,1,1,1)}| + 2|X^{(6)}| + 2|X^{(3,3)}| + 4|X^{(2,2,2,2)}| + 3|X^{(2,2,2,1,1,1)}| \right)$

$= \frac{1}{12} \left( (6^6) + 2(6^1) + 2(6^3) + 4(6^4) + 3(6^4) \right)$

$= 4291$
1. \( \phi(17) = 17 - 1 = 16 \) (since 17 is prime)

\[
\phi(n) = n \prod_{\text{prime } p | n} \left(1 - \frac{1}{p}\right)
\]

\( \phi(32) = \phi(2^5) = 2^5 \left(1 - \frac{1}{2}\right) = 2^4 = 16 \)

\( \phi(40) = \phi(2^3 \cdot 5) = 2^3 \cdot 5 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 2^3 \cdot 5 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) = 2^3 \cdot 4 = 40 \)

\( \phi(100) = \phi(2^2 \cdot 5^2) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 2^2 \cdot 5^2 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) = 2 \cdot 5 \cdot 4 = 40 \)

\[
\phi(17) = 16 \\
\phi(32) = 16 \\
\phi(40) = 16 \\
\phi(100) = 40
\]

2. \( \left( \mathbb{Z}/15\mathbb{Z} \right)^* = \{ 1, 2, 4, 7, 8, 11, 13, 14 \} \)
\[ 2^1 = 2 \quad 7^1 = 7 \quad 11^1 = 11 \quad 13^1 = 13 \quad 14^1 = 14 \]
\[ 2^2 = 4 \quad 7^2 = 4 \quad 11^2 = 1 \quad 13^2 = 4 \quad 14^2 = 1 \]
\[ 2^3 = 8 \quad 7^3 = 13 \quad 13^3 = 7 \]
\[ 2^4 = 1 \quad 7^4 = 1 \quad 13^4 = 1 \]

(we see that all elements of \((\mathbb{Z}/15\mathbb{Z})^*\) are either order 4, or order 2.)

\[
(\mathbb{Z}/15\mathbb{Z})^* = \langle 2, 11 \mid 2^4 = 1, 11^2 = 1, 2 \cdot 11 = 11 \cdot 2 \rangle = \langle a, b \mid a^4 = 1, b^2 = 1, ab = ba \rangle.
\]

let \(2 = a\)
\(11 = b\)

* you can take the first generator to be any of: 2, 7, 8, 13, since they have \(\text{ord} = 4\).

* you can take the other generator to be any of the elements of order 2 that are not the square of the other generator.

3. Work in \(\mathbb{Z}/100\mathbb{Z}\), we have that \(\phi(100) = 40\) \(\Leftrightarrow 3^{40} = 1\).

\[
127^{54} = 3^{40k + r} = (3^{40})^k 3^r = 3^r. \quad \text{So we need the remainder of } 127^{54} \text{ when divided by } 40.
\]

In \(\mathbb{Z}/40\mathbb{Z}\), we have \(127 = 7\), so \(127^{54} = 7^{54} = (7^6)^9 = 1^9 = 1\). Since \(1 \cdot 7^{16} = 1\) in \(\mathbb{Z}/40\mathbb{Z}\), \(1 = 81 \cdot 9\), \(1 \cdot 9 = 81\). Therefore \(127^{54} = 40k + 9\).

Putting things together:

in \(\mathbb{Z}/100\mathbb{Z}\)

\[
127^{54} = 3^{40k + 9} = (3^{40})^k 3^9 = 1^k 3^9 = 3^9 = (3^4)^2 3 = 81 \cdot 81 \cdot 3 = 61 \cdot 3 = 183 = 83
\]

\[
\frac{81}{81} = 81, 81 = 6561 = 61, \quad \frac{61}{183} = 83
\]

(last two digits: 83)
4. Figures could be something like...

\[ \begin{array}{ccc}
\text{D}_6 \text{ symmetry group} & \text{D}_6 \text{ symmetry group} & \text{D}_6 \text{ symmetry group} \\
\end{array} \]

But not something like...

\[ \begin{array}{cc}
\text{C}_6 \text{ symmetry group} & \text{D}_3 \text{ symmetry group} \\
\end{array} \]

5. \( \rho = \text{rotation by } 180^\circ \) (note: \( R_1 R_2 = \rho \), \( R_2 R_1 = \rho \) )

\[ W = \{ 1, R_1, R_2, \rho \} \]

\[ W = \langle R_1, R_2 \mid R_1^2 = 1, R_2^2 = 1, R_1 R_2 = R_2 R_1 \rangle \]

\( W \) is isomorphic to the Klein 4-group.
6. Let \( X = \{ \text{colorings of } 1 \to 2 \to 3 \text{ relative to ordering} \} \)

\[ |X| = 3^4. \]

\( \forall w \in X \cdot \)

\[ |X/w| = \frac{1}{|W|} \sum_{w \in W} |X^0| \]

\[ = \frac{1}{4} \left( |X^{1,1,1,1}| + |X^{2,2}| + 2 |X^{2,1,1,1}| \right) \]

\[ = \frac{1}{4} \left( 3^4 + 3^2 + 2 \cdot 3 \right) \]

\[ = \frac{3^2 \cdot 15}{4} \]

\[ = 36. \]

36 distinct rhombuses.
Rotational Symmetry

H \rotate[180]{180} \quad S \rotate[180]{180}
I \rotate[180]{180} \quad X \rotate[180]{180}
N \rotate[180]{180} \quad Z \rotate[180]{180}
O \rotate[180]{180}

Reflection Symmetry

A \quad B \quad C \quad D \quad E
H \quad I \quad K \quad M
O \quad T \quad U \quad V
W \quad X \quad Y

Both

H, I, O, X

Smallest symmetry group
G = \{1\}
F, G, J, P, Q, R.

Largest symmetry group
G \cong V \text{ Klein 4-group.}
H, I, O

There are aspects of this question that are "open to debate."
8. \( D_n = \langle p, R \mid p^n = 1, R^2 = 1, Rp = p^{-1} R \rangle \).

Since \( \phi \) is a homomorphism: \( \text{im}(\phi) \subseteq A_n \) precisely when \( \phi(p) \in A_n \) and \( \phi(R) \in A_n \).

\( \phi(p) \in A_n \) requires that the \( n \)-cycle \((1 \ 2 \ 3 \ \ldots \  n)\) be even.

\( \phi(p) \in A_n \iff n \text{ odd} \).

\( \phi(R) \in A_n \) requires that the cycle type \( (\underbrace{2,2,\ldots,2}_{\frac{n-1}{2}},1) \) be even.

\( \phi(R) \in A_n \iff \frac{n-1}{2} \text{ even} \).

Putting things together: \( \frac{n-1}{2} = 2k \iff n-1 = 4k \iff n = 4k+1 \).

**Bonus.** Reflections give rise to transpositions \((a \ b)\).

We see that the composition of two reflections gives a rotation of the tetrahedron.

The composition of three reflections \((3 \ 4)(2 \ 3)(1 \ 2) = (4 \ 3 \ 2 \ 1)\) gives 4-cycles: \( (1 \ 2 \ 3 \ 4) \) (which is an interesting "non-geometric" transformation).

Anyway, we see that \( \phi: G \to S_4 \) is an isomorphism.

\[ G \cong S_4 \]