1. An isomorphism from a group G to itself is called an *automorphism*. Let $\mathrm{Aut}(G)$ denote the set of automorphisms of a group G.

(a) Let $f\colon G_1 \to G_2$ and $g\colon G_2 \to G_3$ be group homomorphisms. Prove that the composition $g \circ f\colon G_1 \to G_3$ is a group homomorphism.

(b) Let $f\colon G \to H$ be a group isomorphism. Prove that the inverse function $f^{-1}\colon H \to G$ is also a group isomorphism.

(c) Prove that $\mathrm{Aut}(G)$ is a group with operation given by composition.

(d) Prove that $\mathrm{Aut}(\mathbb{Z}_2) \cong \mathbb{Z}_2$.

(e) Prove that $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

(a) $\forall a, b \in G_1$, then

$g\circ f(a) *_3 g\circ f(b)$

$= g(f(a) *_2 f(b))$ since g is group homomorphism

$= g(f(a *_1 b))$ since f is group homomorphism

$= g \circ f(a *_1 b)$

So $g\circ f$ is a group homomorphism

(b) Select arbitrary $A, B \in H$

Since f is surjective, $\exists\, a, b \in G$ s.t. $f(a) = A$, $f(b) = B$

So $f(a+b) = A+B$, $f^{-1}(B) = b$, $f^{-1}(A) = a$

So $f^{-1}(A+B) = a+b = f^{-1}(B) + f^{-1}(A)$

Therefore f^{-1} is a group homomorphism

And f^{-1} is an isomorphism since f, f^{-1} is bijective

(c) ① Operation is associative.

$\forall f, g \in Aut(G)$

By (a), $f \circ g$ is also an homomorphism

and is isomorphism since the composition

of bijective functions is bijective.

② has an identity element : the identity map

$e: G \to G$ sending

$g \to g$

$\forall f \in Aut(G)$, $f \circ g = g \circ f = f$.

③ Every element has an inverse, proved by (b)

Since $\forall f \in Aut(G)$, $f^{-1} \in Aut(G)$ and

$f \circ f^{-1} = f^{-1} \circ f = e$, so f^{-1} is its inverse in $Aut(G)$

(d) There are two elements in $Aut(\mathbb{Z}_2)$

$(0\ 1)$ and (0)

And there are two elements in $\mathbb{Z}_2$: $0, 1$

So $|Aut(\mathbb{Z}_2)| = |\mathbb{Z}_2| = 2$

Since all groups of order 2 are isomorphic as

we have proved, $Aut(\mathbb{Z}_2) \cong \mathbb{Z}_2$

(e) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

There are 3 non-identity elements: $(0,1)$, $(1,0)$ and $(1,1)$. Denote them by A, B, C respectively.

Since $\forall$ isomorphism $f: \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$, f is homomorphism and thus $f((0,0)) = (0,0)$

So the elements of $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is the ways to rearrange A, B, C, which is by definition S_3.

To build an isomorphism $\varphi: S_3 \longrightarrow \mathrm{Auto}(\mathbb{Z}_2 \times \mathbb{Z}_2)$

Consider sending

$$
\begin{aligned}
(1) &\longmapsto (A) \\
(1,2) &\longmapsto (A, B) \\
(1,3) &\longmapsto (A, C) \\
(2,3) &\longmapsto (B, C) \\
(1,2,3) &\longmapsto (A, B, C) \\
(1,3,2) &\longmapsto (A, C, B)
\end{aligned}
$$

2. Let G be a group. The **center** of G is the set $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$.

1. Prove that $Z(G)$ is an abelian subgroup of G.
2. Compute the center of D_4.
3. Compute the center of S_3.
4. Compute the center of $GL_2(\mathbb{R})$.

1. Pf. ① $e \in Z(G)$

since $\forall h \in G$, $eh = he$.

② $Z(G)$ is closed under operation on G

Take $x, y \in Z(G)$, we have $\forall g \in G$,

$xg = gx$, $yg = gy$

So $xyg = x(yg) = (xg)y = g(xy)$

Therefore $xy \in Z(G)$

③ $Z(G)$ is closed under inverse

Take $g \in Z(G)$

For arbitrary $x \in G$, $gx = xg$

$\xrightarrow{\cdot g^{-1} \text{ on left}} x = g^{-1}xg$

$\xrightarrow{\cdot g^{-1} \text{ on right}} xg^{-1} = g^{-1}x \implies g^{-1} \in Z(G)$

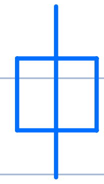
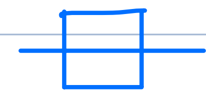
④ $Z(G)$ is commutative

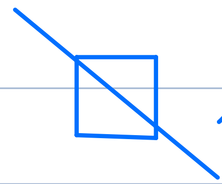
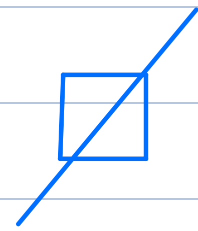
$\forall x, y \in Z(G)$ $xy = yx$ by definition

By ①②③④, $Z(G)$ is an abelian subgroup of G.

2. $D_4 = \{r_0, r_{90}, r_{180}, r_{-90}, f_1, f_2, f_3, f_4\}$

where r is clockwise and

f_1 denotes , f_2 denotes 

f_3 denotes , f_4 denotes 

$r_0 \in G(D_4)$ since $\forall a \in D_4$ $a r_0 = r_0 a = a$

$r_{180} \in G(D_4)$ through calculation

$r_{90} f_1 \neq f_1 r_{90}$, $r_{-90} f_2 \neq f_2 r_{-90}$

$f_3 r_{90} \neq r_{90} f_3$, $f_4 r_{90} \neq r_{90} f_4$

So $\underbrace{Z(D_4) = \{r_0, r_{180}\}}$

3. $S_3 = \{(1)\,(12)\,(13)\,(23)\,(123)\,(132)\}$

$(1) \in G(S_3)$ since it is the identity

$(12)(23) \neq (23)(12)$
$= (123) \qquad = (321)$

$(123)(13) \neq (13)(123)$
$= (23) \qquad = (12)$

$(132)(13) \neq (13)(132)$
$= (12) \qquad = (23)$

So $Z(S_3) = \{(1)\}$

4. let $\begin{pmatrix} m & n \\ p & q \end{pmatrix} \in Z(GL_2(\mathbb{R}))$

$\forall a, b, c, d \in \mathbb{R}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} m & n \\ p & q \end{pmatrix} = \begin{pmatrix} am+bp & an+bq \\ cm+dp & cn+dq \end{pmatrix}$$

$$= \begin{pmatrix} m & n \\ p & q \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} am+cn & bm+dn \\ ap+cq & bp+dq \end{pmatrix}$$

$\Longrightarrow bp = cn \Longrightarrow \underline{p = n = 0}$

$an+bq = bm+dn \Longrightarrow bq = bm \Rightarrow q = m$

$cm+dp = ap+cq \Longrightarrow cm = cq$ (always true

So $Z(GL_2(\mathbb{R})) = \left\{ k\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \middle| k \in \mathbb{R} \right\}$

3. Consider the symmetric group S_n, with $n \geq 3$. The goal of this problem is to prove that S_n can be generated by only two elements.

(a) Let $\tau \in S_n$ be a permutation, and $(\,a\,b\,)$ be a transposition. Show that $\tau(\,a\,b\,)\tau^{-1} = (\,\tau(a)\,\tau(b)\,)$, the transposition changing $\tau(a)$ and $\tau(b)$.

(b) Show that $(\,i\,j\,) = (\,1\,i\,)(\,1\,j\,)(\,1\,i\,)$. Conclude that every element of S_n is the product of transpositions of the form $(\,1\,i\,)$.

(c) Let σ be the $(n-1)$-cycle $(\,2\,3\,\cdots\,n\,)$. Show that $(\,1\,i\,) = \sigma^{i-2}(\,1\,2\,)(\sigma^{-1})^{i-2}$ for all $i = 2, \ldots, n$. Conclude that $S_n = \langle (\,1\,2\,), (\,2\,3\,\cdots\,n\,) \rangle$.

(a)
$$\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(a) & \cdots & \tau(b) & \cdots & \tau(n) \\ 1 & 2 & \cdots & a & \cdots & b & \cdots & n \end{pmatrix}$$

$$\Rightarrow (ab)\circ\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(a) & \cdots & \tau(b) & \cdots & \tau(n) \\ 1 & 2 & \cdots & b & \cdots & a & \cdots & n \end{pmatrix}$$

$$\Rightarrow \tau\circ(ab)\circ\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \cdots & \tau(a) & \cdots & \tau(n) \\ \tau(1) & \tau(2) & \cdots & \tau(b) & & \tau(n) \end{pmatrix}$$

$$= (\tau(a), \tau(b))$$

(b)
$$(1\ i) = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ i & 2 & \cdots & 1 & \cdots & j & \cdots & n \end{pmatrix}$$

$$\Rightarrow (1\ j)(1\ i) = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ i & 2 & \cdots & j & \cdots & 1 & \cdots & n \end{pmatrix}$$

$$\Rightarrow (1\ i)(1\ j)(1\ i) = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix} = (i\ j)$$

Conclusion: Every element of S_n is the product of transpositions of the form $(1\ i)$

(c) $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$

$\sigma^{i-2} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & i & i+1 & \cdots & i-1 & i-2 \end{pmatrix}$

By (a), $\sigma^{i-2}(1\,2)(\sigma^{-1})^{i-2} = (\sigma^{i-2}(1), \sigma^{i-2}(2))$

$\underbrace{= (1, i)}$

Therefore $S_n = \langle (1,2), \sigma \rangle$ since by Thm 7.26, $\forall s \in S_n$ is product of some transpositions and every transposition $\langle ij \rangle$ is product of transpositions of the form $(1\, i)$ and $(1\, i) = \sigma^{i-2}(1\,2)(\sigma^{-1})^{i-2}$

4. Consider the alternating group A_n, that is, the subgroup of S_n consisting of all the even permutations of S_n, for $n \geq 3$. Let $i, j, k, l \in \{1, 2, \ldots, n\}$, with $i \neq j$ and $k \neq l$.

(a) Suppose that $(i\,j)$ and $(k\,l)$ are not disjoint cycles. Show that $(i\,j)(k\,l)$ is either the identity or a 3-cycle.

(b) Suppose that $(i\,j)$ and $(k\,l)$ are disjoint cycles. Show that $(i\,j)(k\,l)$ is the product of two 3-cycles.

(c) Prove that A_n is generated by the set of all 3-cycles of S_n.

(a) Case 1: each of k, l equal to one of i, j

So $(ij) = (kl)$,

Since $|(ij)| = 2$, $\underline{(ij)(kl) = (1)}$

Case 2: only one of k, l equal to one of i, j

WLOG suppose $i=k$

So $(ij)(kl) = (ij)(il) = (li)(ij)$

$= (lij)$

Therefore we can conclude: $(ij)(kl)$ is either the identity or a 3-cycle.

(b) $(ij)(kl) = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & k & \cdots & l & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & l & \cdots & k & \cdots & n \end{pmatrix}$

$= (ij)(1)(kl)$

$= (ij)(jk)(jk)(kl)$

$= \underline{(ijk)(jkl)}$

So $(ij)(kl)$ is the product of two cycles.

(c) $\forall a \in A_n$, so $a = a_1 a_2 \cdots a_{2k}$ where $k \in \mathbb{Z}^+$ for some transpositions $a_1, \ldots, a_{2k}$

Then $a = \prod_{i=1}^{k} a_i a_{i+1}$

By (a)(b), $a_i a_{i+1} = (1)$ or a 3-cycle or a product of 3-cycle

note that $\underline{(1) = (12)(21)}$

$= (12)(23)(32)(21) = (123)(321)$

is also a product of two 3-cycles

Therefore a is a product of 3-cycles.

So A_n is generated by the set of all 3-cycles of S_n.