NAME:
Exercise 1  We recall that $GL_2(\mathbb{R})$ denotes the group of invertible $2 \times 2$ matrices with real coefficients. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a $2 \times 2$ matrix, we recall that the transpose of $A$, denoted by $A^T$ is the matrix $A^T := \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, and that $(AB)^T = B^T A^T$. The identity matrix is denoted by $I_2$.

We let $O_2(\mathbb{R})$ be the subset of $GL_2(\mathbb{R})$ defined by

$$O_2(\mathbb{R}) := \{ A \in GL_2(\mathbb{R}), A^T A = I_2 \}.$$ 

**Question 1.** Show that $O_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

- We have $I_2^T \cdot I_2 = I_2 \cdot I_2 = I_2$ hence $I_2 \in O_2(\mathbb{R})$.
- Let $A$ be in $O_2(\mathbb{R})$, by definition $A^T A = I_2$ hence $A^T = A^{-1}$. We also have $A \cdot A^{-1} = A^{-1} \cdot A = I_2$, in particular $A \cdot A^T = I_2$, but $A = (A^T)^T$, so $(A^T)^T \cdot A^T = I_2$, which means $A^T \in O_2(\mathbb{R})$, and thus $A^{-1} \in O_2(\mathbb{R})$.

- Let $A, B$ be in $O_2(\mathbb{R})$. Let us compute

\[(AB)^T AB = B^T A^T A B \quad \text{(by the formula recalled above)} \]
\[= B^T B \quad \text{(because $A \in O_2(\mathbb{R})$) \]
\[= I_2 \quad \text{(because $B \in O_2(\mathbb{R})$)} \]

hence $AB \in O_2(\mathbb{R})$.

In conclusion, $O_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

For any $A$ in $O_2(\mathbb{R})$, we define the commutator of $A$ as the subset

$$\text{Comm}(A) := \{ B \in O_2(\mathbb{R}), AB = BA \}.$$ 

In plain words, $\text{Comm}(A)$ is the set of all matrices in $O_2(\mathbb{R})$ that commute with $A$.

**Question 2.** Compute $\text{Comm}(I_2)$.

By definition, $\text{Comm}(I_2) = \{ B \in O_2(\mathbb{R}), I_2 B = B \cdot I_2 \}$

\[= \{ B \in O_2(\mathbb{R}), B = B \} \]

So $\text{Comm}(I_2) = O_2(\mathbb{R})$. 
Question 3. For all $A$ in $O_2(\mathbb{R})$, show that $\text{Comm}(A)$ is a subgroup of $O_2(\mathbb{R})$. Let $A \in O_2(\mathbb{R})$

- We have $I_2 \cdot A = A \cdot I_2 = A$, so $I_2 \in \text{Comm}(A)$.
- If $B \in \text{Comm}(A)$ we have $AB = BA$, so $B^{-1}A = AB^{-1}$ and $B \in \text{Comm}(A)$.
- If $B, C$ are in $\text{Comm}(A)$, we have $ABC = BAC = BCA$ thus $BC \in \text{Comm}(A)$ because $AB = BA$ because $AC = CA$

In conclusion, $\text{Comm}(A)$ is a subgroup of $O_2(\mathbb{R})$

Question 4. Let $A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Show that $A$ is in $O_2(\mathbb{R})$, compute its order and describe its commutator.

- We have $A^T = A$, and $A \cdot A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $A \in O_2(\mathbb{R})$.
- Since $A^T = A$, we have $A^2 = I_2$, so $A$ has order 2.
- $A \cdot A = I_2$.
- Let us describe its commutator. Let $B \in O_2(\mathbb{R})$, let us write $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

We have $B \in \text{Comm}(A) \iff BA = AB \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

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

so $B \in \text{Comm}(A) \iff B$ is in $O_2(\mathbb{R})$ and can be written as $\begin{pmatrix} a & c \\ c & a \end{pmatrix}$ for some $a, c$ in $\mathbb{R}$

This is an acceptable answer:

- $B = \begin{pmatrix} a & c \\ c & a \end{pmatrix}$ where $a^2 + c^2 = 1$
- $ac = 0$
- $B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.
Exercise 2. We recall that a group $G$ is said to be cyclic if there exists an element $g$ in $G$ such that the subgroup $\langle g \rangle$ generated by $g$ is equal to $G$ itself.

Question 1. Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic, but that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not.

Let us consider $\langle (1,1) \rangle$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$. The successive powers of $(1,1)$ are $(1,1)$, $(0,2)$, $(1,0)$, $(0,1)$, $(1,2)$, $(0,0)$, so $\langle (1,1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ is thus cyclic.

In $\mathbb{Z}_2 \times \mathbb{Z}_2$ we have

$\langle (0,0) \rangle = \langle (0,0) \rangle$
$\langle (1,0) \rangle = \langle (0,0), (1,0) \rangle$
$\langle (0,1) \rangle = \langle (0,0), (0,1) \rangle$
$\langle (1,1) \rangle = \langle (0,0), (1,1) \rangle$

None of these are $\mathbb{Z}_2 \times \mathbb{Z}_2$, so there is no generation.

$\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Question 2. Let $G, H$ be two groups. Assume that $G$ is cyclic and that there exists an isomorphism from $G$ to $H$. Prove that $H$ is cyclic.

Done in class.
Question 3. Let $G$ be a group, and let $g$ be in $G$. Someone tells you that there is at most one element of $G$ not included in $\langle g \rangle$. Show that $G$ is cyclic.

- If there is no element not included in $\langle g \rangle$, then $G$ is cyclic and $g$ is a generator.

- Let us assume there is exactly one element in $G$ and not in $\langle g \rangle$, let us denote it by $h$. Consider $g \cdot h$.

  * Either $g \cdot h = h$, which means $g = e$. Then $\langle g \rangle = \langle e \rangle$, and thus $G = \langle e \rangle$, $h \not\in \langle g \rangle$ is isomorphic to $\mathbb{Z}_2$, and is thus cyclic.

  * Or $g \cdot h \neq h$. Since $h$ is the only element not in $\langle g \rangle$, we must have $g \cdot h \in \langle g \rangle$, but since $ge \not\in \langle g \rangle$ we have $h \not\in \langle g \rangle$, which is absurd.
The signature morphism. Let \( n \geq 2 \). We recall that the "signature" or "parity" of a permutation \( \sigma \) in \( S_n \) is defined as

\[
\varepsilon(\sigma) := \prod_{1 \leq i < j \leq n} \text{Sign} \left( \sigma(j) - \sigma(i) \right),
\]

where \( \text{Sign} \) denotes the sign (+1 or -1).

We have proven the following facts: \( \varepsilon(\text{Id}) = 1 \), and if \( \tau \) is a transposition, \( \varepsilon(\tau) = -1 \). The goal of this exercise is to prove that \( \varepsilon \) is a morphism, namely that for all permutations \( \sigma_1, \sigma_2 \), we have

\[
\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2).
\]

**Question 1.** Show that

\[
(13) = (23)(12)(23) \quad \text{and} \quad (23) = (12)(23)
\]

\[
= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (13) = (23)(12)(23)
\]

**Question 2.** For \( i = 1, \ldots, n - 1 \), we let \( \tau_i \) be the transposition

\[
\tau_i := (i(i+1)),
\]

that switches two "neighbors" in \( \{1, \ldots, n\} \). Prove that any transposition can be written as a product of these transpositions \( \tau_i \).

You may argue by induction on the "distance" between the elements of the transposition, and let yourself be inspired by Question 2.

Let us prove that for any \( \tau \geq 1 \), for any

\[
i \neq 0, 1, \ldots, n - \tau \}
\]

the transposition \( (i(i+\tau)) \) can be written as a product of the \( \tau_i \)s.

* If \( \tau = 1 \), it is one of the \( \tau_i \)'s!

* Assume it's true for some \( \tau > 1 \), and consider \( (i(i+\tau+2)) \).

We write, as in question 1:

\[
(i(i+\tau+2)) = (i(i+\tau+2)(i+\tau+1)) (i(i+\tau+2)) \quad \text{by induction hypothesis}
\]

so \( (i(i+\tau+2)) \) can be written as a product of the \( \tau_i \)s.
**Question 3.** Deduce that every permutation in $S_n$ can be written as product of the transpositions $\tau_i$.

We know by a result from class that every permutation can be written as a product of transpositions. From Question 2, we know every transposition is a product of the $\tau_i$'s. Thus every permutation is a product of the $\tau_i$'s.

(hence the whole result boils down to this very easy computation that you can do at home.)

**Question 4.** Show that, in order to prove that $\varepsilon$ is a group morphism, it is enough to prove that for any permutation $\sigma$ and for any $i \in \{1,\ldots,n-1\}$, we have

$$\varepsilon(\sigma \circ \tau_i) = -\varepsilon(\sigma). \quad \text{(*)}$$

We prove the following: for any permutation $\sigma_1$, for any $k \geq 1$, if $\sigma_2$ is a product of $k$ transpositions $\tau$, then $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \varepsilon(\sigma_2)$

* $k = 1$ follows from (*)

* Assume it is true for $k \geq 1$. Write $\sigma_2$ as $\sigma_2' \circ \tau$, where $\sigma_2'$ is the product of at most $k$ transpositions $\tau$, and $\tau$ is one of them.

We have

$$\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1 \circ \sigma_2' \circ \tau) = \varepsilon(\sigma_1 \circ \sigma_2') \circ \tau$$

$$= \varepsilon(\sigma_1 \circ \sigma_2') \varepsilon(\tau) \quad \text{(by *)}$$

$$= \varepsilon(\sigma_1) \varepsilon(\sigma_2') \varepsilon(\tau) = \varepsilon(\sigma_1) \varepsilon(\sigma_2) \quad \text{(by induction hypothesis)}$$

Since, by Question 3, every $\sigma_2$ is a product of the $\tau_i$'s, we have proven the result.
Question 5. Compute (with minimal justification) the parity of the following permutations:

1. \((123)(456)(123456)\)
2. \((12)(234)^{-1}(12345)(34)^{-1}\)
3. \((123456789)\).

Parity of a cycle of length \(L = \) parity of \(L-1\)
Parity of \(\sigma = \) parity of \(\sigma^{-1}\). Hence

1) \(1 \cdot 1 \cdot (-1) = -1\)
2) \((-1) \cdot 1 \cdot (1) \cdot (-1) = 1\)
3) \(1\).

Bonus question: compute the center of \(S_n\) for \(n \geq 3\).

It is trivial. Let \(\sigma \in S_n\) be different from the identity. Let \(a \in \{1, \ldots, n\}\) such that \(\sigma(a) \neq a\); denote \(b = \sigma(a)\).

\[\cdots\]

* If \(\sigma(b) \neq a\), let \(\tau = (ab)\), \(\cdots\)
We have \(\sigma \circ \tau(a) = \sigma(b)\) and \(\tau \circ \sigma(a) = \tau(b) = a\)
   since \(\sigma(b) \neq a\), \(\sigma \circ \tau \neq \tau \circ \sigma\) so \(\sigma, \tau\) don't commute.

* If \(\sigma(b) = a\), since \(n \geq 3\) we can take \(c \neq a, b\).
   Let \(\tau = (ac)\). We have \(\sigma \circ \tau(b) = \sigma(c)\) \(\bullet \bullet \bullet = a\)
   \(\tau \circ \sigma(b) = \tau(a) = c\)
   hence \(\sigma \circ \tau \neq \tau \circ \sigma\) and \(\sigma, \tau\) don't commute.