Question 1. (4 points.) Give the definition of a group.

A group is a set \( G \) together with a law of composition \( \ast \), which satisfies the following properties:

1. The law \( \ast \) is associative: \( \forall x, y, z \in G, \ (x \ast y) \ast z = x \ast (y \ast z) \).
2. There exists an identity element for \( \ast \): \( \exists e \in G, \ \forall x \in G, \ x \ast e = e \ast x = x \).
3. Each element has an inverse in \( G \): \( \forall x \in G, \ \exists y \in G, \ x \ast y = y \ast x = e \).

Question 2. (4 points.) Let \( E = [0, 1] \) and let us define the following law on \( E \):

\[
\forall x, y \in E, \ x \ast y = x + y - xy
\]

Show that \( \ast \) is a law of composition. Is it associative? Commutative? Has it got an identity element?

Don’t forget the first part of the question! You must check that \( \ast : [0, 1] \times [0, 1] \rightarrow [0, 1] \) is a law of composition.

We can notice that for \( x, y \in [0, 1], \ x \ast y = 1 - (1 - x) \times (1 - y) \).

Since \( x, y \in [0, 1], \ (1 - x), (1 - y) \in [0, 1] \).

Then \( (1 - x) \times (1 - y) \in [0, 1] \).

This implies that \( x \ast y \in [0, 1] \) since \( x \ast y = 1 - (1 - x) \times (1 - y) \).

Therefore \( \ast \) is well defined, and it is a law of composition on \( E \).

It is associative, since for \( x, y, z \in [0, 1] \):

\[
x \ast (y \ast z) = x + y + z - x(y \ast z)
= x + (y + z - yz) - x(y + z - yz)
= x + y + z - yz - xy - xz + xwz
\]

And on the other hand:

\[
(x \ast y) \ast z = x \ast y + z - (x \ast y)z
= (x + y - xy) + z - (x + y - xy)z
= x + y + z - yz - xy - xz + xyz
\]

So \( x \ast (y \ast z) = (x \ast y) \ast z \).

\( \ast \) is commutative since for \( x, y \in [0, 1] \): \( x \ast y = x + y - xy = y + x - yx = y \ast x \).

0 is an identity element for \( \ast \) since for all \( x \in [0, 1] \): \( x \ast 0 = x + 0 - x \times 0 = x \). And you can prove \( 0 \ast x = x \) using the same calculation, or just by mentioning the commutativity of \( \ast \).
Problem 1. (6 points.) Is $B$ a subgroup of group $A$ in these examples? Justify.

1. $A = (GL_2(\mathbb{R}), \cdot)$ and $B = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \ a, b \in \mathbb{R}, \ a \neq 0 \right\}$.

   $B$ is a subset of $A$ since for $a, b \in \mathbb{R}, \ a \neq 0$, $\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 \neq 0$. So each matrix in $B$ has an inverse.

   However it is not stable by the matrix product since for $a, b, c, d \in \mathbb{R}, \ a, c \neq 0$:

   $$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \times \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}$$

   Nothing guarantees that $ac - bd \neq 0$ (a counter-example is $a = b = c = d = 1$). Therefore, $B$ is not a subgroup of $A$.

2. $A = (GL_2(\mathbb{R}), \cdot)$ and $B = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \ a \in \mathbb{R} \right\}$.

   1. $B$ is a subset of $A$ since for any $a \in \mathbb{R}$, $\det \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = 1 \neq 0$.

   2. The identity is in $B$, for a parameter $a$ equal to 0.

   3. $B$ is stable by matrix product, since for any $a, b \in \mathbb{R}$:

      $$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a + b & 0 \end{pmatrix} \in B$$

   4. $B$ is stable by inversion, since for $a \in \mathbb{R}$:

      $$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -a & 0 \end{pmatrix} \in B$$

   Therefore, $B$ is a subgroup of $A$.

3. $A = (\mathbb{Q}^*, \times)$ and $B = \{2^n, \ n \in \mathbb{Z}\}$.

   1. $B$ is a subset of $A$ since for any $n \in \mathbb{Z}$, $2^n = \frac{2^n}{1} \in \mathbb{Q}$.

   2. The identity is in $B$, since $1 = 2^0 \in B$.

   3. $B$ is stable by multiplication, since for any $m, n \in \mathbb{Z}$:

      $$2^n \times 2^m = 2^{m+n} \in B$$

   4. $B$ is stable by inversion, since for $n \in \mathbb{Z}$:

      $$(2^n)^{-1} = 2^{-n} \in B$$
Problem 2. (6 points.) Below is a partially completed Cayley table of a group. Fill in the missing parts of the table.

Here is the initial table:

\[
\begin{array}{c|cccc}
\ast & a & b & c & d \\
\hline 
a & b & d & \\
b & a & \\
c & b & \\
d & b & \\
\end{array}
\]

\(b \ast a = a\) tells us that \(b\) is the identity element. Therefore:

\[
\begin{array}{c|cccc}
\ast & a & b & c & d \\
\hline 
a & b & a & d & c \\
b & a & b & c & d \\
c & c & b & \\
d & d & b & \\
\end{array}
\]

Then, let us have a look to \(ad\):

1. It can’t be \(b\), because in that case \(aa = ad\) and that would imply \(a = d\).
2. It can’t be \(d\), because in that case \(ac = ad\) and that would imply \(c = d\).
3. It can’t be \(a\), because in that case \(ab = ad\) and that would imply \(b = d\).

Therefore, \(ad = c\).

\[
\begin{array}{c|cccc}
\ast & a & b & c & d \\
\hline 
a & b & a & d & c \\
b & a & b & c & d \\
c & c & b & \\
d & d & b & \\
\end{array}
\]

The same reasoning applies to fill each box of the table.

\[
\begin{array}{c|cccc}
\ast & a & b & c & d \\
\hline 
a & b & a & d & c \\
b & a & b & c & d \\
c & c & b & a \\
d & d & b & \\
\end{array}
\]

Then:

\[
\begin{array}{c|cccc}
\ast & a & b & c & d \\
\hline 
a & b & a & d & c \\
b & a & b & c & d \\
c & d & c & b & a \\
d & d & b & \\
\end{array}
\]

And finally:

\[
\begin{array}{c|cccc}
\ast & a & b & c & d \\
\hline 
a & b & a & d & c \\
b & a & b & c & d \\
c & d & c & b & a \\
d & c & d & a & b \\
\end{array}
\]