Question 1. Show that multiplication is well defined in $\mathbb{Z}/m$, i.e. if $x \equiv x'$ and $y \equiv y'$ then $xy \equiv x'y'$. 

Proof. Suppose $x \equiv x'$ and $y \equiv y'$ modulo $m$. Then there exist $a, b \in \mathbb{Z}$ such that $x' = x + am$ and $y' = y + bm$. Hence,

$$x'y' - xy = (x + am)(y + bm) - xy = xbm + yam + abm^2 = (xb + ya + abm) \cdot m \equiv 0 \pmod{m},$$

which implies that $x'y' \equiv xy$ modulo $m$. $\square$

Question 2. Let $G$ be a group and $X$ a subset of $G$. Let $\langle X \rangle$ be the intersection of all subgroups of $G$ that contain $X$. Show that $\langle X \rangle$ is in fact a subgroup, called subgroup generated by $X$. If $G = GL_n(\mathbb{R})$ and $X$ is the set of all elementary matrices, what subgroup is $\langle X \rangle$?

Proof. First note symbolically we can write

$$\langle X \rangle = \bigcap_{X \subset H \leq G} H.$$

We would like to show $\langle X \rangle$ is a subgroup of $G$. (Note: In fact, a more general fact holds: an intersection of collection of subgroups of a group is again a subgroup. The proof is essentially the same as below.)

- (Identity) $1_G \in \langle X \rangle$ since $1_G = 1_H \in H$ for every subgroup $H \supset X$ of $G$.
- (Inverse) Also, for any $a \in \langle X \rangle$ we have that $a \in H$ for every $H \supset X$. Since $H$ itself is a subgroup, $a^{-1} \in H$ for every $H \supset X$. Hence, $a^{-1} \in \langle X \rangle$.
- (Closure) Similarly, for any $a, b \in \langle X \rangle$, it follows that $ab \in H$ for every subgroup $H \supset X$, proving $ab \in \langle X \rangle$.

These prove $\langle X \rangle$ is indeed a subgroup of $H$.

Now set $G = GL_n(\mathbb{R})$, and $X$ to be the set of all elementary matrices. We claim $\langle X \rangle$ is in fact the whole group $GL_n(\mathbb{R})$. We have $\langle X \rangle \subset GL_n(\mathbb{R})$ by definition, so it suffices to prove $\langle X \rangle \supset GL_n(\mathbb{R})$. For this, pick $A \in GL_n(\mathbb{R})$. Since an invertible matrix is a product of elementary matrices (Theorem 1.2.16), it follows that $A \in \langle X \rangle$, concluding the proof. $\square$

Question 3 (Artin 2.2.4). In which of the following cases is $H$ a subgroup of $G$?

(a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.
(b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.
(c) $G = \mathbb{Z}^+$ and $H$ is the set of positive integers.
(d) $G = \mathbb{R}^\times$ and $H$ is the set of positive reals.
(e) $G = GL_2(\mathbb{R})$ and $H$ is the set of matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$. 

1
Solution. (a,b,d) \( H \leq G \).
(c) \( H \not\leq G \). Note \( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin H \). Also \( H \not\leq G \) either, as \( \det \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = 0 \). //

**Question 4** (Artin 2.4.7). Let \( x \) and \( y \) be elements of a group \( G \). Assume that each of the elements \( x, y, \) and \( xy \) has order 2. Prove that the set \( H = \{1, x, y, xy\} \) is a subgroup of \( G \), and that it has order 4.

**Proof.** To show \( H \leq G \), first note \( 1 \in H \). Also, it is closed under taking inverses: \( x^{-1} = x, \ y^{-1} = y, \ (xy)^{-1} = xy \),

because \( x, y \) and \( xy \) are all of order 2. One way to see \( H \) is closed under multiplication is to draw the multiplication table(See Section 2.1 of Artin) for \( H \): Here note that since \( xyxy = 1, \)

\[
\begin{array}{c|cccc}
 & 1 & x & y & xy \\
\hline
1 & 1 & x & y & xy \\
x & x & 1 & y & x \\
y & y & yx & 1 & yxy \\
xy & xy & xyx & x & 1 \\
\end{array}
\]

it follows that \( xyx = y^{-1} = y \) and \( yxy = x^{-1} = x \). Also \( yx = x^{-1}y^{-1} = xy \). Hence after substituting these in the table, \( H \) is closed under the multiplication, showing \( H \leq G \).

Now to show \( H \) is of order 4, it suffices to show \( 1, x, y \) and \( xy \) are distinct. First, \( x, y \) and \( xy \) are distinct from \( 1 \) as they are of order 2. Next, we see \( x, y \) are different from \( xy \), otherwise we get \( x = 1 \) or \( y = 1 \). Finally, \( x \neq y \), otherwise \( xy = x^2 = 1 \) contradicting the order of \( xy \) is 2. Therefore, \( H \) has order 4. \( \square \)

**Question 5** (Artin 2.4.9). How many elements of order 2 does the symmetric group \( S_4 \) contain?

**Solution.** The order 2 elements in \( S_4 \) are exactly 2-cycles and \((2,2)\)-cycles. (See Section 1.5 of Artin.) The number of 2-cycles is \( \binom{4}{2} = 6 \) and that of \((2,2)\)-cycles is \( \binom{4}{2}/2 = 3 \). Therefore, the total number of order 2 elements is \( 6 + 3 = 9 \). //

**Question 6** (Artin 2.9.7). Determine the order of each of the matrices \( A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \) and \( B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \) when the matrix entries are interpreted modulo 3.

**Solution.** One can check that \( A^n = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \), so \( A \) is of order 3 in \( GL_2(\mathbb{Z}/3) \), the set of invertible matrices with entries in \( \mathbb{Z}/3 \).

On the other hand, \( B^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \) where \( F_n \) is the \( n \)-th term of the Fibonacci sequence defined as \( F_n = F_{n-1} + F_{n-2} \) for \( n \geq 2 \) and \( F_0 = 0, F_1 = 1 \). Using this, one can compute that \( B^8 = \begin{bmatrix} 34 & 21 \\ 21 & 13 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}/3) \), and \( B^m \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}/3) \) for \( m < 8 \), proving \( B \) is of order 8. //
**Question 7 (Bonus question).** Construct a group $G$ and elements of $x, y \in G$ of order 2 such that $xy$ has order $n$ for a given integer $n \geq 1$.

**Proof.** A typical order 2 element to think of is a reflection. The key idea is to observe that *the composition of two parallel reflections is a translation.* (Two non-parallel reflections compose into a rotation.) Using this, we can construct such $G$. Namely, first consider a real line $\mathbb{R}$. Let $x$ be the reflection at the point $\frac{1}{4}$, and $y$ be the reflection at the point $-\frac{1}{4}$. Then we claim that $xy$ is a translation by $+1$. (Here we follow the function composition notation; first apply $y$, and then $x$.) Indeed, for any $r \in \mathbb{R}$, we have

$$xy(r) = x(-\frac{1}{2} - r) = \frac{1}{2} - (-\frac{1}{2} - r) = 1 + r.$$  

Hence, if the order of $xy$ is given to be infinity, we can just let $x, y$ as such reflections on $\mathbb{R}$. (In this case $\langle x, y \rangle \cong D_\infty$, called the *infinite dihedral group*.)

However, if $n$ is a finite positive integer, we can make $\mathbb{R}$ into a circle $\mathbb{R}/\sim$ by declaring the equivalence relation $r \sim r + n$ for all $r \in \mathbb{R}$. Then $\mathbb{R}/\sim$ becomes a circle with circumference $n$, so the $n$ times of $+1$-translation becomes the identity. Now we achieved to find the elements $x, y$ of order 2 such that $xy$ is of order $n$, we declare $G = \langle x, y \rangle$, the group generated by $x$ and $y$. (See Question 2). In fact, in this case $G \cong D_{2n}$, the dihedral group of order $2n$. □