Abstract Algebra
Day 10 Class Work Solutions

1. **(Review)** Consider the set $U_{10} = \{1, 3, 7, 9\}$.

   (a) Complete its multiplication table below.

   Solution.

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

   (b) Use the table created to check the group properties for U_{10}.

   Solution.

   1. U_{10} is closed under multiplication. We can see this from the table above, since every entry in the table (i.e., all possible products) is an element of U_{10}.
   2. The associative law holds for multiplication.
   3. U_{10} contains the identity element 1.
   4. Every element in U_{10} has an inverse in U_{10}. Note that 3 and 7 are inverses of each other. Each of 1 and 9 is a self inverse.

2. More generally, consider

$$U_m = \{a \in \mathbb{Z}_m \mid a \text{ has a multiplicative inverse}\}.$$

Elizabeth claims that U_m is a group under multiplication. Help her justify each group property by answering the following questions.

   (a) Complete Elizabeth's proof below.

Claim: U_m is closed under multiplication.

Proof: Assume $\alpha, \beta \in U_m$.

Then α has a multiplicative inverse k

Such that ________ in $\mathbb{Z}_m$. **Ans:** $\alpha \cdot k = 1$.

Similarly, β has ________________

Such that ________________.

Hence, $(\alpha\beta)\cdot(\quad) = (\quad)\cdot(\quad) = 1 \cdot 1 = 1$ in $\mathbb{Z}_m$,

So that ____ is a multiplicative inverse of $\alpha\beta$.

Thus, ________ as desired.

   (b) You may assume that multiplication is associative. (Move onto part (c).)

(c) Use the definition of U_m above to explain why the multiplicative identity 1 is in U_m. ← Why is $1 \in U_m$?

Solution. The element 1 is the *multiplicative* identity, because $1 \cdot a = a$ and $a \cdot 1 = a$ for all $a \in U_m$. And 1 itself is in U_m, because it is a self inverse (so, in particular, 1 has a multiplicative inverse).

(d) Our friends are trying to prove: If $a \in U_m$, then a^{-1} is in U_m.

- **Elizabeth:** We start by assuming that $a \in U_m$.
- **Anita:** That means a has a multiplicative inverse. So, a^{-1} exists. We're done!
- **Elizabeth:** Not so fast. We have to show that a^{-1} is in U_m, too.
- **Anita:** Ok, but how do we know that a^{-1} has a multiplicative inverse? **Hint:** $a \cdot a^{-1} = 1$.

How would you respond to Anita?

Solution. Since a^{-1} is a multiplicative inverse of a, we have $a \cdot a^{-1} = 1$. This implies that a^{-1} also has a multiplicative inverse, namely a. Therefore, $a^{-1} \in U_m$.

3. Let $M(\mathbb{Z}_{10})$ be the set of 2×2 matrices with entries in $\mathbb{Z}_{10}$. For example, here are two matrices in $M(\mathbb{Z}_{10})$: $\alpha = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right]$ and $\beta = \left[\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right]$. Compute the sum $\alpha + \beta$ and product $\alpha \cdot \beta$. **Ans:** $\alpha \cdot \beta = \left[\begin{smallmatrix} 9 & 2 \\ 3 & 0 \end{smallmatrix}\right]$.

Solution. $\alpha + \gamma = \left[\begin{smallmatrix} 6 & 8 \\ 0 & 2 \end{smallmatrix}\right]$ and $\alpha \cdot \gamma = \left[\begin{smallmatrix} 9 & 2 \\ 3 & 0 \end{smallmatrix}\right]$.

4. Recall that $M(\mathbb{Z}_{10})$ is a group under addition. Now let's consider multiplication. ← i.e., just like $\mathbb{Z}_{10}$.

(a) Explain why $M(\mathbb{Z}_{10})$ is closed under multiplication.

Solution. Assume $\alpha, \beta \in M(\mathbb{Z}_{10})$. Thus $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and $\beta = \left[\begin{smallmatrix} w & x \\ y & z \end{smallmatrix}\right]$, where all the matrix entries are in $\mathbb{Z}_{10}$. Then

$$\alpha\beta = \begin{bmatrix} aw+by & ax+bz \\ cw+dy & cx+dz \end{bmatrix},$$

which is a 2×2 matrix. Moreover, $aw + by$, $ax + bz$, $cw + dy$, $cx + dz \in \mathbb{Z}_{10}$, because $\mathbb{Z}_{10}$ is closed under addition and multiplication. Therefore, $\alpha\beta \in M(\mathbb{Z}_{10})$.

(b) You may assume that matrix multiplication is associative. (Move onto part (c).) ← Do you see why?

(c) What is the *multiplicative* identity of $M(\mathbb{Z}_{10})$?

Solution. The element $\varepsilon = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is the multiplicative identity.

(d) **True or False:** Every $\alpha \in M(\mathbb{Z}_{10})$ has a multiplicative inverse in $M(\mathbb{Z}_{10})$. **Ans:** False. (Why?)

Solution. False. For example, the matrix $\left[\begin{smallmatrix} 2 & 3 \\ 0 & 0 \end{smallmatrix}\right] \in M(\mathbb{Z}_{10})$ does *not* have a multiplicative inverse. There is no matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ such that $\left[\begin{smallmatrix} 2 & 3 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, because

$$\begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2a+3c & 2b+3d \\ 0 & 0 \end{bmatrix}.$$

Since its bottom row contains 0's only, the product cannot equal $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

5. Is $M(\mathbb{Z}_{10})$ a group under multiplication? Why or why not?

Solution. No. It's true that $M(\mathbb{Z}_{10})$ is closed under multiplication, matrix multiplication is associative, and $\varepsilon = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is the multiplicative identity. But not every element of $M(\mathbb{Z}_{10})$ has a multiplicative inverse, as we saw in Problem #4(d).

Define the subset $G(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \alpha \text{ has a multiplicative inverse}\}$. ← Analogous to U_{10}.

6. Here are some matrices in $M(\mathbb{Z}_{10})$: $\alpha = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 7 \end{smallmatrix}\right]$, $\beta = \left[\begin{smallmatrix} 1 & 2 \\ 3 & 8 \end{smallmatrix}\right]$, $\gamma = \left[\begin{smallmatrix} 4 & 1 \\ 3 & 5 \end{smallmatrix}\right]$, $\delta = \left[\begin{smallmatrix} 2 & 4 \\ 1 & 5 \end{smallmatrix}\right]$.

   (a) Compute the determinant of each of these matrices.

   Recall: The *determinant* of a matrix in $M(\mathbb{Z}_{10})$ is given by $\det\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = ad - bc$.

   Solution. We have $\det\alpha = 1$, $\det\beta = 2$, $\det\gamma = 7$, $\det\delta = 6$.

   (b) For each matrix, find its multiplicative inverse or explain why one doesn't exist.

   Solution. Since $\det\alpha = 1$ and $\det\gamma = 7$ have multiplicative inverses in $\mathbb{Z}_{10}$, we conclude that α and γ have multiplicative inverses in $M(\mathbb{Z}_{10})$.

   - We have $\det\alpha = 1$ so that $(\det\alpha)^{-1} = 1$. Thus, $\alpha^{-1} = \left[\begin{smallmatrix} 7 & -2 \\ -3 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 7 & 8 \\ 7 & 1 \end{smallmatrix}\right]$.
   - We have $\det\gamma = 7$ so that $(\det\gamma)^{-1} = 3$. Thus, $\gamma^{-1} = 3 \cdot \left[\begin{smallmatrix} 5 & -1 \\ -3 & 4 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 5 & 7 \\ 1 & 2 \end{smallmatrix}\right]$.

   Meanwhile, $\det\beta = 2$ and $\det\delta = 6$ do *not* have multiplicative inverses in $\mathbb{Z}_{10}$. Thus, β and δ do *not* have multiplicative inverses in $M(\mathbb{Z}_{10})$.

   (c) Which of these are in $G(\mathbb{Z}_{10})$? **Ans:** α and γ.

   Solution. α and γ.

   (d) Fill in the blank below:

   Solution. Theorem. Let $\alpha \in M(\mathbb{Z}_{10})$. Then $\alpha \in G(\mathbb{Z}_{10})$ if and only if $\det\alpha \in U_{10}$.

7. Explain why $G(\mathbb{Z}_{10})$ is a group under multiplication. Be sure to verify each group property.

   Solution. See the explanation in Section 10.2 in the textbook.

> Define the subset $S(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \det\alpha = 1\}$.

8. (a) Consider the matrices in Problem #6. Determine which of those are in $S(\mathbb{Z}_{10})$. **Ans:** α only.

   Solution. α only.

   (b) Explain why $S(\mathbb{Z}_{10}) \subseteq G(\mathbb{Z}_{10})$.

   PROOF. Assume $\alpha \in S(\mathbb{Z}_{10})$. Then $\det\alpha = 1$, which has a multiplicative inverse in $\mathbb{Z}_{10}$, namely itself. Therefore, α has a multiplicative inverse in $M(\mathbb{Z}_{10})$, which implies that $\alpha \in G(\mathbb{Z}_{10})$. Thus, $S(\mathbb{Z}_{10}) \subseteq G(\mathbb{Z}_{10})$. ∎

   (c) Explain why $S(\mathbb{Z}_{10})$ is a group under multiplication. Verify each group property.

   Solution. See the explanation in Section 10.3 in the textbook.

9. **(Socks-Shoes Revisited)** In $M(\mathbb{Z}_{10})$, let $\alpha = \left[\begin{smallmatrix} 3 & 4 \\ 5 & 1 \end{smallmatrix}\right]$ and $\beta = \left[\begin{smallmatrix} 7 & 1 \\ 0 & 3 \end{smallmatrix}\right]$.

   (a) Verify that α and β are in $G(\mathbb{Z}_{10})$.

   (b) Verify that $(\alpha\beta)^{-1} \neq \alpha^{-1}\beta^{-1}$, but $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

10. **(Some Food for Thought)** U_{10} is a subset of $\mathbb{Z}_{10}$, and both are groups. Should U_{10} be called a *subgroup* of $\mathbb{Z}_{10}$? Why or why not? **Ans:** No. (Why not?)

11. **(More Food for Thought)**

    (a) Without listing them, find the number of elements in U_{35}.

    (b) Repeat part (a), but with U_{39}; with U_{55}; with U_{91}.

    (c) Repeat part (a), but with U_{pq} where p and q are distinct odd primes.