Abstract Algebra
Day 11 Class Work Solutions

1. Recall that $H = \{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8$ under addition. Find *all* subgroups of $\mathbb{Z}_8$. ← How do you know that you've found them all?

   Solution. $\{0\}$, $\{0, 4\}$, $\{0, 2, 4, 6\}$, $\mathbb{Z}_8$ itself.

2. Recall that

   - $M(\mathbb{Z}_{10})$ = the set of 2×2 matrices with entries in $\mathbb{Z}_{10}$.
   - $G(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \alpha \text{ has a multiplicative inverse}\}$.

   (a) $M(\mathbb{Z}_{10})$ is a group under what operation?

   (b) $G(\mathbb{Z}_{10})$ is a group under what operation?

   (c) Is $G(\mathbb{Z}_{10})$ a subgroup of $M(\mathbb{Z}_{10})$? Why or why not? **Ans:** It's not. (Why not?)

   Solution. $M(\mathbb{Z}_{10})$ is a group under addition and $G(\mathbb{Z}_{10})$ is a group under multiplication. Even though $G(\mathbb{Z}_{10})$ is a subset of $M(\mathbb{Z}_{10})$, because their group operations are different, $G(\mathbb{Z}_{10})$ is *not* a subgroup of $M(\mathbb{Z}_{10})$.

3. Recall the set $S(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \det \alpha = 1\}$.

   (a) Write down a few elements of $S(\mathbb{Z}_{10})$.

   Solution. Examples include $\left[\begin{smallmatrix} 3 & 2 \\ 4 & 3 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 7 & 2 \\ 5 & 3 \end{smallmatrix}\right]$, since each has determinant of 1.

   (b) Find the multiplicative inverse of each matrix in part (a). Verify that these inverses are also in $S(\mathbb{Z}_{10})$. **Recall:** α^{-1} is given by $(\det \alpha)^{-1} \cdot \left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right]$.

   Solution.

$$\begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}^{-1} = 1^{-1} \cdot \begin{bmatrix} 3 & -2 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 3 & 8 \\ 6 & 3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 7 & 2 \\ 5 & 3 \end{bmatrix}^{-1} = 1^{-1} \cdot \begin{bmatrix} 3 & -2 \\ -5 & 7 \end{bmatrix} = \begin{bmatrix} 3 & 8 \\ 5 & 7 \end{bmatrix}.$$

   The inverses have determinants $3 \cdot 3 - 8 \cdot 6 = 1 \pmod{10}$ and $3 \cdot 7 - 8 \cdot 5 = 1 \pmod{10}$. Therefore, the inverses are also in $S(\mathbb{Z}_{10})$.

   (c) Prove that $S(\mathbb{Z}_{10})$ is a subset of $G(\mathbb{Z}_{10})$.

   Hint: Let $\alpha \in S(\mathbb{Z}_{10})$. Why does α have a multiplicative inverse?

   Proof. Let $\alpha \in S(\mathbb{Z}_{10})$. We have $\det \alpha = 1 \in U_{10}$. Thus, $\alpha \in G(\mathbb{Z}_{10})$. ∎

   (d) Prove that $S(\mathbb{Z}_{10})$ is a sub*group* of $G(\mathbb{Z}_{10})$ under multiplication. ← This should be useful: $\det(\alpha\beta) = \det \alpha \cdot \det \beta$.

   Note: You may assume that matrix multiplication is associative.

   Proof. We will first show that $S(\mathbb{Z}_{10})$ is closed under matrix multiplication. Assume $\alpha, \beta \in S(\mathbb{Z}_{10})$. Then $\det \alpha = 1$ and $\det \beta = 1$. Thus,

$$\det(\alpha\beta) = (\det \alpha)(\det \beta) = 1 \cdot 1 = 1.$$

   Hence, $\det(\alpha\beta) = 1$ and so $\alpha\beta \in S(\mathbb{Z}_{10})$.
   Next, note that $\det \varepsilon = 1$ and thus $\varepsilon \in S(\mathbb{Z}_{10})$. Lastly, suppose $\gamma \in S(\mathbb{Z}_{10})$. Then $\det \gamma = 1$. Note that $\det(\gamma^{-1}) = (\det \gamma)^{-1} = 1^{-1} = 1$. Thus $\gamma^{-1} \in S(\mathbb{Z}_{10})$. ∎

4. Find *all* subgroups of the (additive) group $\mathbb{Z}$. ← Again, how do you know you've found them all?

   Hint: The two extreme cases are $\{0\}$ and $\mathbb{Z}$ itself.

   Solution. They are of the form $m\mathbb{Z}$ where $m \in \mathbb{Z}$.

5. Given a group G, define its subset $H = \{g \in G \mid g^2 = \varepsilon\}$.

   Note: By default, assume that the operation is multiplication.

   (a) Find H if $G = U_{16}$. (Start by listing the elements of U_{16}.) **Ans:** $H = \{1, 7, 9, 15\}$.

   Solution. $H = \{1, 7, 9, 15\}$.

   (b) With G and H as in part (a), construct a multiplication table for H and verify that it's a subgroup of G.

   Solution. The multiplication table of H is given by:

$\cdot$	1	7	9	15
1	1	7	9	15
7	7	1	15	9
9	9	15	1	7
15	15	9	7	1

   Note how (1) the set H is closed, (2) multiplication is associative (or observe that H inherits the associative operation from U_{16}), (3) $\varepsilon = 1$ is contained in H, and (4) every element of H has an inverse in H; in this case, the definition of H implies that every element of H is a self inverse. Thus, H is a subgroup of U_{16}.

   (c) **Prove:** If G is commutative, then H is a subgroup of G.

   PROOF. We will first show that H is closed. Assume $a, b \in H$. Then $a^2 = \varepsilon$ and $b^2 = \varepsilon$. Since G is commutative, we have $(ab)^2 = a^2b^2 = \varepsilon \cdot \varepsilon = \varepsilon$. Hence, $(ab)^2 = \varepsilon$ and so $ab \in H$.

   Next, note that $\varepsilon^2 = \varepsilon$ and thus $\varepsilon \in H$. Lastly, suppose $c \in H$. Then $c^2 = \varepsilon$. Note that $(c^{-1})^2 = (c^2)^{-1} = \varepsilon^{-1} = \varepsilon$. Thus $(c^{-1})^2 = \varepsilon$ so that $c^{-1} \in H$. ■

   (d) Using a counterexample, show that the statement in part (c) is false when the group G is non-commutative.

   Solution. Let $G = D_4$. Then $H = \{\varepsilon, r_{180}, h, v, d, d'\}$. But H is not closed, since $h \circ d = r_{90}$, which is not in H. Thus, H is not a subgroup of G.

6. Consider the subsets $H = \{0, 6\}$ and $K = \{0, 4, 8\}$ of the additive group $\mathbb{Z}_{12}$.

   (a) Verify that H is a subgroup of $\mathbb{Z}_{12}$. Do likewise for K.

   (b) With H and K as above, compute the set $H + K = \{h + k \mid h \in H, k \in K\}$. ← $H + K$ has 6 elements.

   (c) Verify that the set $H + K$ you found in part (b) is a subgroup of $\mathbb{Z}_{12}$.

   (d) **Generalize:** Let H and K be subgroups of an additive group G. Define

$$H + K = \{h + k \mid h \in H, k \in K\}.$$

   Prove that $H + K$ is a subgroup of G.

7. **(Challenge)** Find all subgroups of $D_4 = \{\varepsilon, r_{90}, r_{180}, r_{270}, h, v, d, d'\}$. ← i.e., the group of symmetries of a square.