Abstract Algebra
Day 22 Class Work Solutions

Below, we'll consider the subgroup $H = \langle 10 \rangle$ of the (multiplicative) group U_{37}.

1. (a) Quick, how many elements are in U_{37}? ← Yes, 37 is prime.

   Solution. Since 37 is prime, $U_{37} = \{1, 2, 3, \ldots, 35, 36\}$. It has 36 elements.

   (b) Verify that $\langle 10 \rangle = \{1, 10, 26\}$ by computing the powers of 10 modulo 37.

   Solution. By definition, $\langle 10 \rangle = \{10^k \mid k \in \mathbb{Z}\}$, i.e., the set of all integer powers of 10. Reducing mod 37, we have $10^1 = 10$, $10^2 = 26$, $10^3 = 1$. Thus, $\langle 10 \rangle = \{1, 10, 26\}$.

   (c) How many distinct cosets of H are there? How do you know? **Ans:** 12 cosets.

   Solution. U_{37} and H have 36 and 3 elements, respectively. Thus, there are $36/3 = 12$ distinct cosets of H.

2. **Suggestion:** Use a calculator for parts (a) and (b) below.

   (a) Compute the cosets $4H$ and $11H$. **Ans:** $4H = \{4, 3, 30\}$.

   Solution. We have

   $$4H = \{4{\cdot}1,\ 4{\cdot}10,\ 4{\cdot}26\} = \{4, 3, 30\} \text{ and } 11H = \{11{\cdot}1,\ 11{\cdot}10,\ 11{\cdot}26\} = \{11, 36, 27\}.$$

   (b) Compute the coset product $4H \cdot 11H$ *without using the coset multiplication shortcut*, and verify that it is, indeed, equal to $44H$.

   Note: It might help to write $4H = \{4, 3, -7\}$ and $11H = \{11, -1, -10\}$. (Why?)

   Solution. Writing $4H$ and $11H$ as above allows us to work with numbers that are smaller in absolute value. We have...

   $$\begin{aligned} 4H \cdot 11H &= \{4, 3, -7\} \cdot \{11, -1, -10\} \\ &= \{4 \cdot 11,\ 4 \cdot (-1),\ 4 \cdot (-10),\ 3 \cdot 11,\ 3 \cdot (-1),\ 3 \cdot (-10),\ -7 \cdot 11,\ -7 \cdot (-1),\ -7 \cdot (-10)\} \\ &= \{7, 33, 34, 33, 34, 7, 34, 7, 33\} \\ &= \{7, 33, 34\} \end{aligned}$$

   And $44H = 7H = \{7 \cdot 1,\ 7 \cdot 10,\ 7 \cdot 26\} = \{7, 33, 34\}$ so that $4H \cdot 11H = 44H$.

> You may use the coset multiplication shortcut for the rest of the problems!

← i.e., $aH \cdot bH = (ab)H$.

3. Find the coset product $1H \cdot 11H$. (**Optional:** Compute this *without* using the shortcut.) What does this say about the role of $1H$ in U_{37}/H?

   Solution. We have $1H \cdot 11H = 11H$, so that $1H$ is the identity element in U_{37}/H.

4. (a) Anita claims that $2H$ and $19H$ in U_{37}/H are inverses of each other. Do you agree or disagree with her? Explain.

   Solution. Agree. Using the shortcut, we have $2H \cdot 19H = (2 \cdot 19)H = 1H$. Thus, the product of $2H$ and $19H$ is the identity element $1H$ so that $2H$ and $19H$ are indeed inverse of each other.

   (b) Find the inverse of $15H$ in U_{37}/H. How about the inverse of $28H$?

   Solution. We have $15 \cdot 5 = 1 \pmod{37}$. Thus, $15H \cdot 5H = (15 \cdot 5)H = 1H$, and $5H$ is the inverse of $15H$. Similarly, the inverse of $28H$ is $4H$, because $28H \cdot 4H = (28 \cdot 4)H = 1H$. Symbolically, we write $(28H)^{-1} = 4H$.

5. Verify that U_{37}/H with coset multiplication satisfies the group properties. Note that...
   - Since U_{37} is commutative, the shortcut $aH \cdot bH = (ab)H$ holds in U_{37}/H.
   - You may assume that coset multiplication is associative. ← Proved in Chapter 21.

   Solution. Below is a proof outline. (See Chapter 22 reading for a complete proof.)

   Since U_{37}/H satisfies the coset multiplication shortcut...
   - U_{37}/H is closed under coset multiplication, i.e., $aH \cdot bH = (ab)H \in U_{37}/H$.
   - Coset multiplication is associative. (See Chapter 21 reading.)
   - U_{37}/H contains an identity element $1H$ such that $1H \cdot aH = (1 \cdot a)H = aH$.
   - Each $aH \in U_{37}/H$ has an inverse $(aH)^{-1} = a^{-1}H \in U_{37}/H$ where

     $$aH \cdot (aH)^{-1} = aH \cdot a^{-1}H = (a \cdot a^{-1})H = 1H.$$

     Here, a^{-1} is the inverse of a in U_{37}.

6. (a) Find all $a \in U_{37}$ such that $aH = 1H$.

   Solution. We have $H = \{1, 10, 26\}$. Thus, $1H = 10H = 26H$.

   (b) Find the order of $6H$ in U_{37}/H. **Ans:** $\text{ord}(6H) = 4$.

   Note: Feel free to use the shortcut to compute the powers of $6H$.

   Solution. We have...

   $$\begin{aligned} (6H)^1 &= 6^1H \neq 1H \\ (6H)^2 &= 6^2H = 36H \neq 1H \\ (6H)^3 &= 6^3H = 31H \neq 1H \\ (6H)^4 &= 6^4H = 1H \end{aligned}$$

   Thus, $n = 4$ is the smallest positive exponent with $(6H)^n = 1H$. Hence, $\text{ord}(6H) = 4$.

   (c) Verify that $\text{ord}(34H) = 3$ in U_{37}/H. It might help to write $34H = (-3)H$.

   Solution. We have...

   $$\begin{aligned} (34H)^1 &= 34^1H \neq 1H \\ (34H)^2 &= 34^2H = 9H \neq 1H \\ (34H)^3 &= 34^3H = 10H = 1H \end{aligned}$$

   Therefore, $\text{ord}(34H) = 3$.

   (d) Find the order of $4H$ in U_{37}/H. **Ans:** $\text{ord}(4H) = 6$.

   Solution. $\text{ord}(4H) = 6$. Proceed as in parts (b) and (c).

   (e) In U_{37}, it turns out that: $\text{ord}(6) = 4$, $\text{ord}(34) = 9$, $\text{ord}(4) = 18$. Any conjectures?

   Solution. See Problem #7 below.

7. (a) Let $a \in U_{37}$ with $\text{ord}(a) = 12$. Show that $(aH)^{12} = 1H$. What does this say about the order of aH in U_{37}/H?

   Solution. Since $\text{ord}(a) = 12$, we have $a^{12} = 1$ in U_{37}. Now in U_{37}/H, we have

   $$(aH)^{12} = a^{12}H = 1H.$$

   This doesn't mean that the order of aH is equal to 12. But it does mean that $\text{ord}(aH)$ is a divisor of 12.

(b) **Prove:** $\text{ord}(aH)$ in U_{37}/H is a divisor of $\text{ord}(a)$ in U_{37} for all $a \in U_{37}$.

PROOF. Let $n = \text{ord}(a)$. Then in U_{37}, we have $a^n = 1$. Now in U_{37}/H, we have

$$(aH)^n = a^n H = 1H.$$

Thus, $\text{ord}(aH)$ is a divisor of n, as desired. ∎

8. Recall that U_{13} is cyclic with generator 2, i.e., $U_{13} = \langle 2 \rangle$. With the subgroup $H = \{1, 3, 9\}$ of U_{13}, verify that U_{13}/H is cyclic with generator $2H$.

PROOF. Let $aH \in U_{13}/H$ where $a \in U_{13}$. Since $U_{13} = \langle 2 \rangle$, we have $a = 2^n$ for some $n \in \mathbb{Z}$. Then $aH = 2^n H = (2H)^n$, so that aH can be written as an integer power of $2H$. Hence, U_{13}/H is cyclic with generator $2H$. ∎

9. Note that $\mathbb{Z}_{12}$ is cyclic with generator 1, i.e., $\mathbb{Z}_{12} = \langle 1 \rangle$. With the subgroup $H = \{0, 4, 8\}$ of $\mathbb{Z}_{12}$, verify that $\mathbb{Z}_{12}/H$ is cyclic with generator $1 + H$.

Solution. I'll leave it to you to rewrite the proof in Problem #8 for an additive group.

10. Consider the subgroup $H = \{1, 7\}$ of U_{16}.

(a) Quick, how many distinct cosets of H are there? Explain how you know.

(b) Find the quotient group U_{16}/H.

(c) Create the table for U_{16}/H and verify that it's a group under coset multiplication.

(d) Find the order of each $aH \in U_{16}/H$. Is the group cyclic?

11. Consider the subgroup $H = \{1, 9\}$ of U_{16}.

(a) Find the quotient group U_{16}/H and determine if it's cyclic.

(b) Compare your work in part (a) with Problem #10. Are you surprised by the results?

(c) U_{16} has another 2-element subgroup K. Find it and determine if U_{16}/K is cyclic.

12. **(An Important Proof)** Let G be a commutative group, H its subgroup, and $a, b \in G$. Define the coset product by ← i.e., The shortcut holds when G is commutative.

$$aH \cdot bH = \{\alpha \cdot \beta \mid \alpha \in aH,\ \beta \in bH\}.$$

Then show that $aH \cdot bH = (ab)H$.

PROOF. First, we will show that $(ab)H \subseteq aH \cdot bH$. Let $g \in (ab)H$ so that $g = (ab)h$ for some $h \in H$. Then, $g = (ab)h = (a\varepsilon)(bh) \in aH \cdot bH$. Thus, $(ab)H \subseteq aH \cdot bH$.

Next, we will show that $aH \cdot bH \subseteq (ab)H$. Let $\alpha \cdot \beta \in aH \cdot bH$, where $\alpha \in aH$ and $\beta \in bH$. Thus, $\alpha = ah$ and $\beta = bk$ for some $h, k \in H$. Since G is commutative,

$$\alpha \cdot \beta = (ah)(bk) = a(hb)k = a(bh)k = (ab)(hk),$$

where $hk \in H$ as H is closed. Thus $\alpha \cdot \beta \in (ab)H$, so that $aH \cdot bH \subseteq (ab)H$. Combined with $(ab)H \subseteq aH \cdot bH$, we conclude that $aH \cdot bH = (ab)H$. ∎

13. **(Some Food for Thought)** What about non-commutative groups? In Chapter 21 Exercises, we considered these subgroups of D_4: $Z = \{\varepsilon, r_{180}\}$ and $H = \{\varepsilon, v\}$. We found that D_4/Z satisfied the shortcut, but D_4/H did not. Can you explain what's going on?