Abstract Algebra
Day 13 Class Work Solutions

1. Compute the following in the additive group $\mathbb{Z}_{12}$.

   (a) $3 + 5$.

   Solution. $3 + 5 = 8$.

   (b) $9 + 7$.

   Solution. $9 + 7 = 4$.

   (c) The additive inverse of 4. ← i.e., $4 + k = 0$.

   Solution. $-4 = 8$.

2. The following are to be done in the multiplicative group U_{13}.

   (a) Find the smallest positive integer k such that $2^3 \cdot 2^5 = 2^k$.

   Solution. $k = 8$.

   (b) Same as above, but with: $2^9 \cdot 2^7 = 2^k$. **Hint:** Recall that $2^{12} = 1$.

   Solution. $k = 4$.

   (c) Find the smallest positive integer k such that $2^4 \cdot 2^k = 1$. **Ans to (c):** $k = 8$.

   Note: In other words, 2^k is the multiplicative inverse of 2^4.

   Solution. $k = 8$.

3. Our friends are having the following conversation.

   Elizabeth: The groups $\mathbb{Z}_{12}$ and U_{13} are the same. ← We'll formalize this notion of same-ness soon.

   Anita: Yeah, they have the same number of elements.

   Elizabeth: Well, their operations match up, too.

   What might Elizabeth mean? Describe as *precisely* as possible.

   Hint: Compare Problems #1(a) with #2(a); #1(b) with #2(b); and #1(c) with #2(c).

   Solution. Rather than writing $U_{13} = \{1, 2, 3, 4, \ldots, 12\}$, we write it as follows:

$$\begin{aligned} U_{13} &= \{\, 1,\ \ 2,\ \ 4,\ \ 8,\ \ 3,\ \ 6,\ \ 12,\ 11,\ \ 9,\ \ 5,\ \ 10,\ \ \ 7\ \ \} \\ &= \{\, 2^0,\, 2^1,\, 2^2,\, 2^3,\, 2^4,\, 2^5,\, 2^6,\, 2^7,\, 2^8,\, 2^9,\, 2^{10},\, 2^{11}\} \end{aligned}$$

   where $2^0 = 2^{12} = \varepsilon$. When we express the elements of U_{13} as powers of 2 (its generator), we highlight the correspondence between $\mathbb{Z}_{12}$ and U_{13}. For example, $5 \in \mathbb{Z}_{12}$ corresponds to $2^5 \in U_{13}$. More generally, $k \in \mathbb{Z}_{12}$ corresponds to $2^k \in U_{13}$.

   As Elizabeth points out, the operations of $\mathbb{Z}_{12}$ and U_{13} match up, too. For example, we saw that $9 + 7 = 4$ in $\mathbb{Z}_{12}$. The matching product in U_{13} is $2^9 \cdot 2^7 = 2^4$, which respects the $k \leftrightarrow 2^k$ correspondence. In general, if $a + b = c$ in $\mathbb{Z}_{12}$, then $2^a \cdot 2^b = 2^c$ in U_{13}.

4. Let g be an element of a multiplicative group with $\operatorname{ord}(g) = 12$.

   (a) Find the smallest positive integer k such that $g^{-1} = g^k$. **Ans to (a):** $k = 11$.

   Solution. $k = 11$. Note that $g \cdot g^{11} = g^{12} = \varepsilon$, so that the inverse of g is g^{11}.

   (b) Same as above, but with g^{-1} replaced by each of the following: g^{-3}, g^{197}, g^{-197}.

Solution. Noting that $g^{12} = \varepsilon$, we have

- $g^{-3} = g^{-3} \cdot \varepsilon = g^{-3} \cdot g^{12} = g^9$. $(k = 9.)$
- $g^{197} = g^{12 \cdot 16 + 5} = (g^{12})^{16} \cdot g^5 = \varepsilon^{16} \cdot g^5 = g^5$. $(k = 5.)$
- $g^{-197} = g^{-5} = g^{-5} \cdot \varepsilon = g^{-5} \cdot g^{12} = g^7$. $(k = 7.)$

(c) Is it possible that $g^8 = g^5$? Why or why not?

Ans: No. (Why not?)

Solution. No, it's not possible. See solution to Problem #5(b) below.

5. Again, let g be an element of a group G with $\text{ord}(g) = 12$. Define $H = \{g^k \mid k \in \mathbb{Z}\}$.

← H is a subset of G. Do you see why?

(a) Anita says that H has infinitely many elements, since it contains all integer powers of g. Do you agree or disagree with her?

Solution. Disagree. As seen in Problem #4, every element of H (i.e., a power of g) can be written as g^k where the exponent k is an integer between 0 and 11 (i.e., the elements of $\mathbb{Z}_{12}$). Thus, $H = \{g^0, g^1, g^2, g^3, \ldots, g^{11}\}$. (Note that $g^0 = \varepsilon$.)

(b) How many elements does H actually contain? Explain your reasoning.

Ans: 12 elements.

Solution. From part (a), H contains *at most* 12 elements. We also know that the elements $g^0, g^1, g^2, g^3, \ldots, g^{11}$ are distinct. For instance, it is *not* possible that, say, $g^8 = g^5$. If it were possible, then multiplying both sides by g^{-5} would yield $g^3 = \varepsilon$. However, $g^3 = \varepsilon$ is a contradiction; since $\text{ord}(g) = 12$, the smallest positive exponent n such that $g^n = \varepsilon$ is 12. Thus, H has exactly 12 elements.

(c) **Prove:** H is a subgroup of G.

PROOF. We will first prove that H is closed. Let $a, b \in H$ so that $a = g^k$ and $b = g^j$ for some $k, j \in \mathbb{Z}$. Then $a \cdot b = g^k \cdot g^j = g^{k+j}$, where $k + j \in \mathbb{Z}$. Thus $a \cdot b \in H$ so that H is closed. The identity ε is in H, because $\varepsilon = g^0$. Lastly, the inverse of a is $a^{-1} = (g^k)^{-1} = g^{-k}$ where $-k \in \mathbb{Z}$. Thus $a^{-1} \in H$ as desired. ■

6. Recall that 2 is a generator of the multiplicative group U_{13}. Find all generators of U_{13}.

Hint: What did Elizabeth say about $\mathbb{Z}_{12}$ and U_{13}?

Solution. The generators of $\mathbb{Z}_{12}$ are 1, 5, 7, 11. Thus, the generators of U_{13} are

$$2^1 = 2,\ 2^5 = 6,\ 2^7 = 11,\ \text{and } 2^{11} = 7.$$

7. Determine if each group below is cyclic (i.e., it has a generator):

(a) U_5 (b) U_{12} (c) U_{14} (d) D_4

Solution. U_5 and U_{14} are cyclic; but U_{12} and D_4 are not cyclic.

8. (a) Verify that 2 is a generator for U_{19}.

(b) Find all generators of U_{19}.

← There are six of them.

9. **Prove:** Let $a \in \mathbb{Z}_m$. Then a is a generator of $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

Example: The generators of $\mathbb{Z}_{12}$ are 1, 5, 7, 11.