Abstract Algebra
Day 14 Class Work Solutions

1. Determine if each of these groups is cyclic. ← Two of them are cyclic.

   (a) Additive group $\mathbb{Z}_{12}$.

   Solution. Yes, since $\mathbb{Z}_{12} = \langle 1 \rangle$.

   (b) Multiplicative group U_{13}.

   Solution. Yes, since $U_{13} = \langle 2 \rangle$. ← Day 13 Class Work, #6.

   (c) Multiplicative group $\mathbb{R}^*$.

   Solution. Not cyclic. Suppose for contradiction that $\mathbb{R}^*$ is cyclic, so that $\mathbb{R}^* = \langle g \rangle$ for some generator g. Thus every element of $\mathbb{R}^*$ is a power of g. In particular, -1 is in $\mathbb{R}^*$, so we have $g^k = -1$ for some $k \in \mathbb{Z}$. Since g is a real number, we must have $g = -1$ (and k must be odd). But that implies $\mathbb{R}^* = \langle -1 \rangle$, which is a contradiction—i.e., the powers of -1 cannot generate all of $\mathbb{R}^*$. Thus, $\mathbb{R}^*$ is *not* cyclic.

2. (a) Find all generators of $\mathbb{Z}_{12}$.

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

   (b) **(Review)** Recall that 2 is a generator of U_{13}, where ← and $2^{12} = 2^0 = 1$.

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

   - Find $9 + 7$ in $\mathbb{Z}_{12}$; and find k (with $0 \le k \le 11$) such that $2^9 \cdot 2^7 = 2^k$ in U_{13}.
   - Solve $4 + \boxed{?} = 0$ in $\mathbb{Z}_{12}$; and find k such that $2^4 \cdot 2^k = 1$ in U_{13}.

   Solution. In $\mathbb{Z}_{12}$, we have $9 + 7 = 4$ and $4 + 8 = 0$. In U_{13}, we have $2^9 \cdot 2^7 = 2^4$ and $2^4 \cdot 2^8 = 1$. Notice how $k \in \mathbb{Z}_{12}$ corresponds to $2^k \in U_{13}$.

   (c) Use your results from parts (a) and (b) to find all other generators of U_{13}. **Ans:** 6, 11, 7.

   Solution. From part (a), the generators of $\mathbb{Z}_{12}$ are 1, 5, 7, 11. Using the correspondence from part (b), the generators of U_{13} are $2^1 = 2,\ 2^5 = 6,\ 2^7 = 11,\ 2^{11} = 7$.

3. (a) Find all subgroups of $\mathbb{Z}_{12}$. Are they cyclic, too? ← There are six of them.

   Solution. The subgroups, which are all cyclic, are shown below.

$$\begin{aligned} \mathbb{Z}_{12} &= \langle 1 \rangle \\ \{0,\ 2,\ 4,\ 6,\ 8,\ 10\} &= \langle 2 \rangle \\ \{0,\ 3,\ 6,\ 9\} &= \langle 3 \rangle \\ \{0,\ 4,\ 8\} &= \langle 4 \rangle \\ \{0,\ 6\} &= \langle 6 \rangle \\ \{0\} &= \langle 0 \rangle \end{aligned}$$

   (b) Same as part (a), but with U_{13}.

Solution. The subgroups, which are all cyclic, are shown below.

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

(c) What conjecture do you have?

Solution. Let G be a cyclic group, and H a subgroup of G. Then H is also cyclic.

← This is Theorem 14.12 in the textbook.

4. We've seen that the *additive* group $\mathbb{Z}_{12}$ is cyclic, since $\mathbb{Z}_{12} = \langle 1 \rangle$. Our friends are discussing the meaning of $\langle 1 \rangle$ when the operation is addition:

Elizabeth: I think $\langle 1 \rangle$ means $\{1^k \mid k \in \mathbb{Z}\}$.

Anita: I disagree. I think $\langle 1 \rangle$ means $\{k \cdot 1 \mid k \in \mathbb{Z}\}$.

With whom do you agree? Explain.

Solution. Recall that 1 is a generator of the *additive* group $\mathbb{Z}_{12}$, because:

$$1 = 1, \quad 1+1 = 2, \quad 1+1+1 = 3, \quad 1+1+1+1 = 4, \quad \ldots, \quad \underbrace{1+1+\cdots+1}_{12 \text{ terms}} = 0.$$

But we can also write this more succinctly as

$$1 \cdot 1 = 1, \quad 2 \cdot 1 = 2, \quad 3 \cdot 1 = 3, \quad 4 \cdot 1, \quad \ldots, \quad 12 \cdot 1 = 0,$$

which gives us the definition $\langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\}$. Thus, we agree with Anita.

5. Explain why the additive group $\mathbb{Z}$ is cyclic. Find all of its generators.

← There are two generators.

Solution. Using the notation from Problem #4, we have

$$\mathbb{Z} = \{k \cdot 1 \mid k \in \mathbb{Z}\} = \langle 1 \rangle \quad \text{and} \quad \mathbb{Z} = \{k \cdot (-1) \mid k \in \mathbb{Z}\} = \langle -1 \rangle.$$

Thus, $\mathbb{Z}$ is cyclic with generators 1 and -1.

6. (a) Verify that 4 and 10 are multiplicative inverses of each other in U_{13}. Then compute the cyclic subgroups $\langle 4 \rangle$ and $\langle 10 \rangle$. How do they compare?

Solution. We have $\langle 4 \rangle = \langle 10 \rangle$, where both are equal to $\{1, 3, 4, 9, 10, 12\}$.

(b) Recall again the subgroup $\langle 3 \rangle \subseteq \mathbb{R}^*$. Now consider the cyclic subgroup $\left\langle \frac{1}{3} \right\rangle \subseteq \mathbb{R}^*$. In particular, how do $\langle 3 \rangle$ and $\left\langle \frac{1}{3} \right\rangle$ compare? Explain your reasoning.

← So, $\left\langle \frac{1}{3} \right\rangle$ is the set of all integer powers of $\frac{1}{3}$.

Solution. We have $\langle 3 \rangle = \left\langle \frac{1}{3} \right\rangle$, where both contain *all* integer powers of 3.

(c) Let g be a group element. Prove that $\langle g \rangle = \langle g^{-1} \rangle$.

Note: This is a set equality. So you must show $\langle g \rangle \subseteq \langle g^{-1} \rangle$ and $\langle g^{-1} \rangle \subseteq \langle g \rangle$.

Proof. Suppose $x \in \langle g \rangle$. Then $x = g^k$ for some $k \in \mathbb{Z}$. Thus, $x = g^k = (g^{-1})^{-k}$, where $-k \in \mathbb{Z}$. Hence, $x \in \langle g^{-1} \rangle$ so that $\langle g \rangle \subseteq \langle g^{-1} \rangle$. Now suppose $y \in \langle g^{-1} \rangle$. Then $y = (g^{-1})^j$ for some $j \in \mathbb{Z}$. Thus, $y = (g^{-1})^j = g^{-j}$ where $-j \in \mathbb{Z}$. Therefore, $y \in \langle g \rangle$ so that $\langle g^{-1} \rangle \subseteq \langle g \rangle$. Thus, $\langle g \rangle = \langle g^{-1} \rangle$. ■

7. Recall the subgroup $\langle 3 \rangle$ of the multiplicative group $\mathbb{R}^*$.

   (a) Find $k \in \mathbb{Z}$ such that $3^{17} \cdot 3^{25} = 3^k$ in $\langle 3 \rangle$.

   Solution. $3^{17} \cdot 3^{25} = 3^{17+25} = 3^{42}$ in $\langle 3 \rangle$, just like $17 + 25 = 42$ in $\mathbb{Z}$. ($k = 42$.)

   (b) Find $k \in \mathbb{Z}$ such that 3^k is the multiplicative identity of $\langle 3 \rangle$.

   Solution. The multiplicative identity of $\langle 3 \rangle$ is $3^0 = 1$, just like how the additive identity of $\mathbb{Z}$ is 0. ($k = 0$.)

   (c) Find $k \in \mathbb{Z}$ such that 3^k is the multiplicative inverse of 3^{17} in $\langle 3 \rangle$.

   Solution. The multiplicative inverse of 3^{17} is 3^{-17} in $\langle 3 \rangle$, just like how the additive inverse of 17 is -17 in $\mathbb{Z}$. ($k = -17$.)

   (d) Elizabeth says that $\langle 3 \rangle$ behaves just like the additive group $\mathbb{Z}$. What might she mean? Be as precise as possible.

   Solution. As shown in the calculations in parts (a), (b), and (c), there is a correspondence $k \leftrightarrow 3^k$ between $\mathbb{Z}$ and $\langle 3 \rangle$. Soon, we'll formalize what it means for $\langle 3 \rangle$ to behave "just like" $\mathbb{Z}$.

8. (a) Find all subgroups of $\mathbb{Z}_{18}$.

   (b) Find all subgroups of U_{19}. (**Hint:** Find its generator first.)

9. Consider the additive group $\mathbb{Z}_{40}$.

   (a) Find a subgroup H of $\mathbb{Z}_{40}$ containing 10 elements.

   (b) Verify that H is cyclic by finding a generator.

   (c) Find *all* generators of H.

10. **Prove:** Let G be a cyclic group, and H a subgroup of G. Then H is also cyclic.