**Abstract Algebra**
**Day 15 Class Work Solutions**

1. It's possible that the domain and codomain of a function are the same. For instance, consider $f : U_{35} \to U_{35}$ where $f(x) = 3x$ for all $x \in U_{35}$.

   (a) Let $a$, $b \in U_{35}$ (domain) where $a = 8$ and $b = 22$. Compute $f(a)$ and $f(b)$. Then verify that $f(a)$, $f(b) \in U_{35}$ (codomain) and that $f(a) \neq f(b)$.

   ← How do we know that $a$ and $b$ are in $U_{35}$?

   **Solution.** We have $f(a) = 24$ and $f(b) = 31$, which are in $U_{35}$ and are different.

   (b) Choose another pair of elements $a$, $b \in U_{35}$ with $a \neq b$. Then repeat part (a).

   **Note:** Make sure that $a$ and $b$ are in $U_{35}$, not just in $\mathbb{Z}_{35}$.

   (c) **Prove:** If $a \neq b$ in the domain, then $f(a) \neq f(b)$ in the codomain.

   **Hint:** Think contrapositive.

   Proof. We will prove the contrapositive, namely: If $f(a) = f(b)$, then $a = b$.

   Assume $f(a) = f(b)$, where $a$, $b \in U_{35}$. Then $3a = 3b$ in $U_{35}$. The multiplicative inverse of 3 is 12, where $3 \cdot 12 = 1$ and $12 \cdot 3 = 1$ modulo 35. Multiplying both sides of the equation $3a = 3b$ by 12, we obtain $12 \cdot (3a) = 12 \cdot (3b)$. Thus $(12 \cdot 3) \cdot a = (12 \cdot 3) \cdot b$, which implies $1 \cdot a = 1 \cdot b$. Therefore, $a = b$. ■

   (d) Anita wonders, "How can we be sure that $f(x)$ actually is in the codomain $U_{35}$ and not just in $\mathbb{Z}_{35}$ for all inputs $x \in U_{35}$?" How would you respond to her?

   ← If $x \in U_{35}$, why must $f(x)$ also be in $U_{35}$?

   **Solution.** Let $x \in U_{35}$. Since 3 is also in $U_{35}$, we know that $3x \in U_{35}$, as $U_{35}$ is closed under multiplication. Thus, $f(x) = 3x$ is actually in the codomain $U_{35}$.

2. Consider again $f : U_{35} \to U_{35}$ where $f(x) = 3x$ for all $x \in U_{35}$.

   (a) Let $y = 11 \in U_{35}$ (codomain). Then find $x \in U_{35}$ (domain) such that $f(x) = y$.

   **Solution.** We claim that $x = 27$. Then $f(27) = 3 \cdot 27 = 81 = 11$ as desired.

   (b) Repeat part (a) with another $y \in U_{35}$.

   **Note:** First choose the $y$ value (in the codomain). Then find the $x$ (in the domain).

   (c) **Prove:** Let $y \in U_{35}$. Then there exists $x \in U_{35}$ such that $f(x) = y$.

   ← $x$ will depend on $y$.

   Proof. Let $y \in U_{35}$ (the codomain). The multiplicative inverse of 3 is 12, where $3 \cdot 12 = 1$ and $12 \cdot 3 = 1$ modulo 35. Then let $x = 12y$, which is an element of $U_{35}$ (the domain), since 12, $y \in U_{35}$ and $U_{35}$ is closed under multiplication. We now verify that $f(x) = y$. We have $f(x) = f(12y) = 3 \cdot (12y) = (3 \cdot 12) \cdot y = 1 \cdot y = y$, so that $f(x) = y$ as desired. ■

   (d) Elizabeth wonders, "Today's Class Work problems so far remind me of the Sudoku property for $U_{35}$." What might she mean?

---

**Definitions:** Let $f : S \to T$ be a function from domain $S$ to codomain $T$.

- We say $f$ is *one-to-one* when it satisfies: if $a \neq b$, then $f(a) \neq f(b)$ for all $a$, $b \in S$.
- We say $f$ is *onto* when for every $t \in T$, there exists $s \in S$ such that $f(s) = t$.

For example, the function that we saw in Problems #1 and #2 is both one-to-one and onto.

---

3. Consider the function $\gamma : \mathbb{Z}_{12} \to \mathbb{Z}_{18}$ where $\gamma(a) = 6a$ for all $a \in \mathbb{Z}_{12}$.

   (a) Is $\gamma$ one-to-one? Why or why not? **Ans to (a):** No.

   **Solution.** We have $\gamma(5) = 12$ and $\gamma(8) = 12$. Thus, different inputs $5, 8 \in \mathbb{Z}_{12}$ both map to the same element 12 in the codomain $\mathbb{Z}_{18}$. Hence, $\gamma$ is *not* one-to-one.

   (b) Is $\gamma$ onto? Why or why not?

   **Solution.** We have

   $$\gamma(0) = 0,\ \gamma(1) = 6,\ \gamma(2) = 12,\ \gamma(3) = 0,\ \gamma(4) = 6,\ \gamma(5) = 12, \ldots,$$

   so that the only possible outputs of $\gamma$ are 0, 6, and 12 (in $\mathbb{Z}_{18}$). Thus, there is no element $a \in \mathbb{Z}_{12}$ such that $\gamma(a) = 1$. Hence, $\gamma$ is *not* onto.

   (c) Anita says, "I can tell right away that $\gamma$ isn't onto, because its codomain is larger than its domain." What might she mean?

   **Solution.** The possible outputs of $\gamma$ are $\gamma(0)$, $\gamma(1)$, $\gamma(2)$, …, $\gamma(11)$. Thus, there are at most 12 different outputs of $\gamma$. (In fact, we saw in part (b) that there are actually only 3 different outputs.) Since the codomain $\mathbb{Z}_{18}$ contains 18 elements, there are some elements of $\mathbb{Z}_{18}$ that are *not* "hit" by the function $\gamma$. Hence, $\gamma$ cannot be onto.

4. Consider the function $\varphi : \mathbb{Z} \to \mathbb{Z}_5$ where $\varphi(a) = a \pmod 5$ for all $a \in \mathbb{Z}$.

   (a) Find $\varphi(43)$ and $\varphi(-14)$. **Ans:** $\varphi(-14) = 1$.

   **Solution.** We have $\varphi(43) = 3$ and $\varphi(-14) = 1$.

   (b) Is $\varphi$ one-to-one? Why or why not?

   **Solution.** We have $\varphi(6) = 1$ and $\varphi(-14) = 1$. Thus, different inputs $6, -14 \in \mathbb{Z}$ both map to the same element 1 in the codomain $\mathbb{Z}_5$. Hence, $\varphi$ is *not* one-to-one.

   (c) Is $\varphi$ onto? Why or why not?

   **Solution.** Every element of $\mathbb{Z}_5$ (codomain) is "hit" by the function $\varphi$, since $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(2) = 2$, $\varphi(3) = 3$, and $\varphi(4) = 4$. Hence, $\varphi$ is onto.

5. Let $f : \mathbb{Z} \to \mathbb{Z}$ where $f(a) = 2a$ for all $a \in \mathbb{Z}$. Explain why $f$ is one-to-one, but not onto.

   **Solution.** To show that $f$ is one-to-one, assume $f(a) = f(b)$, where $a, b \in \mathbb{Z}$. Then $2a = 2b$, so that $a = b$. Hence, $f$ is one-to-one. However, $f$ is *not* onto, because the only elements of the codomain $\mathbb{Z}$ that are "hit" by $f$ are the even integers.

6. Describe a function $f : \mathbb{Z} \to \mathbb{Z}$ that is onto, but not one-to-one.

7. Let $g$ be a group element with $\operatorname{ord}(g) = 18$. Define $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$, i.e., the set of all integer powers of $g$. Consider $\theta : \mathbb{Z}_{18} \to \langle g \rangle$ where $\theta(a) = g^a$ for all $a \in \mathbb{Z}_{18}$.

   **Example:** For $7 \in \mathbb{Z}_{18}$, we have $\theta(7) = g^7 \in \langle g \rangle$.

   (a) Let $y = g^{1001} \in \langle g \rangle$. Find $x \in \mathbb{Z}_{18}$ such that $\theta(x) = y$.

   **Solution.** Since $1001 = 18 \cdot 55 + 11$, we have

   $$g^{1001} = g^{18 \cdot 55 + 11} = (g^{18})^{55} \cdot g^{11} = \varepsilon^{55} \cdot g^{11} = g^{11},$$

   so that $g^{1001} = g^{11}$. With $x = 11 \in \mathbb{Z}_{18}$, we have $\theta(x) = \theta(11) = g^{11} = g^{1001} = y$.

   (b) **Prove:** $\theta$ is onto.

(c) **Prove:** $\theta$ is one-to-one. (**Hint:** Think contrapositive.)

PROOF. We will prove the contrapositive, namely: If $\theta(a) = \theta(b)$, then $a = b$.

Assume $\theta(a) = \theta(b)$, where $a, b \in \mathbb{Z}_{18}$. Then $g^a = g^b$, so that Theorem 13.12 implies that $18 \mid (a - b)$. Thus $a = b$ in $\mathbb{Z}_{18}$, from which we conclude that $\theta$ is one-to-one. ■

(d) Anita says that the sets $\mathbb{Z}_{18}$ and $\langle g \rangle$ match up completely. What might she mean?

**Solution.** We saw above that $\theta$ is both one-to-one and onto. Thus, each element of the domain $\mathbb{Z}_{18}$ corresponds exactly with one element of the codomain $\langle g \rangle$; and conversely, each element of the codomain corresponds with exactly with one element of the domain. This implies that $\langle g \rangle$ has 18 distinct elements just like $\mathbb{Z}_{18}$, so that the elements in $\mathbb{Z}_{18}$ and $\langle g \rangle$ "match up" as follows:

$$\mathbb{Z}_{18} = \{\, 0, \;\; 1, \;\; 2, \;\; 3, \;\; \ldots, \;\; 16, \;\; 17 \,\}$$
$$\langle g \rangle = \{g^0, g^1, g^2, g^3, \ldots, g^{16}, g^{17}\} \quad (\text{where } g^0 = \varepsilon)$$

(e) Write down the distinct elements of $\langle g \rangle$.

**Solution.** See the solution to part (d) above.

8. Again, let $g$ be a group element with $\operatorname{ord}(g) = 18$.

(a) Compute $12 + 15$ in $\mathbb{Z}_{18}$ and $g^{12} \cdot g^{15}$ in $\langle g \rangle$.

(b) Find the additive inverse of 12 in $\mathbb{Z}_{18}$ and the multiplicative inverse of $g^{12}$ in $\langle g \rangle$.

(c) Elizabeth says that $\mathbb{Z}_{18}$ and $\langle g \rangle$ behave in the same way. What might she mean?

9. **(Some Food for Thought)** Let $S = \{a, b, c, d, e\}$ and $T = \{x, y, z\}$.

(a) How many different functions are there with domain $S$ and codomain $T$? **Ans:** 243 functions.

(b) The tables below depict two functions $\alpha$ and $\beta$ with domain $S$ and codomain $T$. Which function is onto?

| $s$ | $\alpha(s)$ |
|---|---|
| $a$ | $y$ |
| $b$ | $x$ |
| $c$ | $x$ |
| $d$ | $z$ |
| $e$ | $y$ |

| $s$ | $\beta(s)$ |
|---|---|
| $a$ | $y$ |
| $b$ | $x$ |
| $c$ | $x$ |
| $d$ | $y$ |
| $e$ | $y$ |

(c) How many different *onto* functions are there with domain $S$ and codomain $T$?